ΑΣΦΆΛΕΙΑ
ΣΤΟΝ ΨΗΦΙΑΚΌ ΚΌΣΜΟ

Εκπαιδευτικό πρόγραμμα με σενάρια εργαστηρίων και υλικό για εκπαιδευτικούς σχετικά με την κυβερνοασφάλεια ηλικιωμένων

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1. Εισαγωγή

Το «Cyber Safe Senior» είναι ένα πρόγραμμα που χρηματοδοτείται από την Ευρωπαϊκή Ένωση και στοχεύει στη βελτίωση της ψηφιακής παιδείας, της ασφάλειας στο διαδίκτυο και της γενικής ψηφιακής ενδυνάμωσης των ατόμων ηλικίας 65 ετών και άνω. Στον σημερινό όλο και πιο ψηφιακό κόσμο, οι ηλικιωμένοι αντιμετωπίζουν ειδικά εμπόδια κατά την πλοήγησή τους στο διαδίκτυο, καθώς συχνά δεν είναι εξοικειωμένοι με τις νέες τεχνολογίες, τους κινδύνους του διαδικτύου και τις ασφαλείς ψηφιακές συμπεριφορές. Αναγνωρίζοντας αυτό το γεγονός, η πρωτοβουλία Cyber Safe Senior στοχεύει να καλύψει κρίσιμα κενά στις ψηφιακές γνώσεις και ικανότητες χρησιμοποιώντας μια οργανωμένη, προσβάσιμη και πολυδιάστατη προσέγγιση.

Το πρόγραμμα περιλαμβάνει τη δημιουργία ενός ενημερωτικού ηλεκτρονικού βιβλίου που περιλαμβάνει πραγματικές μελέτες περιπτώσεων εγκλημάτων στο διαδίκτυο, πρακτικές συμβουλές ασφάλειας και αναλυτικές οδηγίες για ασφαλή συμπεριφορά στο διαδίκτυο. Επιπλέον, η πρωτοβουλία προσφέρει εικονικές διαλέξεις, διαδραστικές ασκήσεις βασισμένες σε σενάρια και πιλοτικές εκπαιδευτικές συνεδρίες που είναι ειδικά προσαρμοσμένες στους μαθησιακούς στόχους και τις προτιμήσεις των ηλικιωμένων συμμετεχόντων. Το Cyber Safe Senior στοχεύει στην εξάλειψη του ψηφιακού αποκλεισμού, στη βελτίωση της εμπιστοσύνης στη χρήση της τεχνολογίας και στην ενδυνάμωση των ηλικιωμένων ώστε να μπορούν να συμμετέχουν ανεξάρτητα και με ασφάλεια σε ψηφιακά περιβάλλοντα, εστιάζοντας σε ηλικιωμένους που έχουν κάποια βασική ψηφιακή εμπειρία αλλά δεν έχουν επαρκή γνώση της ασφάλειας στο διαδίκτυο.

Το εκπαιδευτικό πρόγραμμα του έργου για εκπαιδευτικούς και εκπαιδευτές τους παρέχει τις πληροφορίες, τη μεθοδολογία και τα πρακτικά εργαλεία που χρειάζονται για να προσφέρουν υψηλής ποιότητας εκπαίδευση σε θέματα ασφάλειας στο διαδίκτυο στους ηλικιωμένους. Οι εκπαιδευτές προετοιμάζονται όχι μόνο για να διδάξουν βασικές έννοιες της ασφάλειας στον κυβερνοχώρο, αλλά και για να εμπλέξουν τους μαθητές σε διαδραστικές δραστηριότητες, σενάρια της πραγματικής ζωής και ασκήσεις που αναδεικνύουν τα μοναδικά προβλήματα που μπορεί να αντιμετωπίσουν οι ηλικιωμένοι στον ψηφιακό κόσμο. Αυτό εγγυάται ότι η εκπαίδευση είναι πρακτική και άμεσα σχετική με την καθημερινή ζωή των συμμετεχόντων.

Το πρόγραμμα υλοποιείται από μια κοινοπραξία εταίρων από την Πολωνία, τη Σλοβενία, την Τουρκία και την Ελλάδα, οι οποίοι συγκεντρώνουν γνώσεις από εκπαιδευτικά ιδρύματα, κοινοτικές οργανώσεις, βιβλιοθήκες, πολιτιστικά κέντρα και κοινότητες ηλικιωμένων. Χρησιμοποιώντας αυτά τα τοπικά δίκτυα, το Cyber Safe Senior μπορεί να προσεγγίσει ηλικιωμένους τόσο σε αστικές όσο και σε αγροτικές περιοχές, εξασφαλίζοντας δίκαιη πρόσβαση σε υλικό ψηφιακής παιδείας και υποστήριξη.

Εκπαιδεύοντας τους ηλικιωμένους να χρησιμοποιούν με αυτοπεποίθηση τις διαδικτυακές πλατφόρμες, να προστατεύουν τα προσωπικά τους δεδομένα, να αναγνωρίζουν τους κινδύνους του διαδικτύου και να συμμετέχουν ενεργά στην ψηφιακή κοινωνία, το πρόγραμμα στοχεύει στη δημιουργία ενός πιο ασφαλούς και φιλόξενου ψηφιακού περιβάλλοντος. Τελικά, το Cyber Safe Senior συνδυάζει εκπαιδευτικό υλικό, πρακτικές δραστηριότητες και συμμετοχή της κοινότητας για να δημιουργήσει ένα περιβάλλον όπου οι ηλικιωμένοι διαθέτουν τις πληροφορίες, τις ικανότητες και την αυτοπεποίθηση που χρειάζονται για να χρησιμοποιούν τα ψηφιακά εργαλεία με ασφάλεια, ανεξαρτησία και παραγωγικότητα.

Ένα βασικό συμπληρωματικό στοιχείο του εκπαιδευτικού προγράμματος Cyber Safe Senior είναι η σειρά διαδραστικών περιπτωσιολογικών μελετών Improve που αναπτύχθηκαν με τη χρήση του Genially. Αυτές οι περιπτώσεις που βασίζονται σε σενάρια είναι πλήρως ευθυγραμμισμένες με τα θέματα κάθε εκπαιδευτικής ενότητας και έχουν σχεδιαστεί για να προσομοιώνουν πραγματικές ψηφιακές καταστάσεις που αντιμετωπίζουν συνήθως οι ηλικιωμένοι. Μέσω καθοδηγούμενης λήψης

αποφάσεων, πρακτικών εργασιών και οπτικής αλληλεπίδρασης, οι περιπτώσεις Improve ενισχύουν τις θεωρητικές γνώσεις και υποστηρίζουν τη βιωματική μάθηση, καθιστώντας τις πολύπλοκες έννοιες της ασφάλειας στο διαδίκτυο πιο προσιτές και ελκυστικές για τους ηλικιωμένους μαθητές.

Κάθε εκπαιδευτική ενότητα ακολουθεί μια δομημένη μορφή που είναι συνεπής με τη διεπαφή της ενότητας, συμπεριλαμβανομένων των μαθησιακών στόχων, του προγραμματισμού των συνεδριών, των πρόσθετων πόρων, της αυτοανασκόπησης του εκπαιδευτή και των στοιχείων αξιολόγησης. Προκαταρκτικές και τελικές εξετάσεις πραγματοποιούνται στην αρχή και στο τέλος κάθε ενότητας για τη μέτρηση της απόκτησης γνώσεων και της προόδου της μάθησης. Επιπλέον, χρησιμοποιούνται ερωτηματολόγια αξιολόγησης για τη συλλογή σχολίων από τους συμμετέχοντες και τους εκπαιδευτές, υποστηρίζοντας τη διασφάλιση της ποιότητας και τη συνεχή βελτίωση του εκπαιδευτικού προγράμματος.

1.1 Στόχος του εκπαιδευτικού προγράμματος

Το πρόγραμμα εκπαίδευσης Cyber Safe Senior έχει αναπτυχθεί για να καλύψει την αυξανόμενη ανάγκη για ψηφιακή παιδεία και ασφάλεια στο διαδίκτυο μεταξύ των ηλικιωμένων άνω των 65 ετών. Οι ηλικιωμένοι αντιμετωπίζουν δυσκολίες στην πλοήγηση στο διαδίκτυο στον σημερινό ψηφιακό κόσμο, επειδή συνήθως έχουν ελάχιστες γνώσεις σχετικά με τις πιθανές απειλές, τα μέτρα ασφάλειας στο διαδίκτυο και τις ασφαλείς ψηφιακές συνήθειες. Ο στόχος αυτού του εκπαιδευτικού προγράμματος είναι να καλύψει αυτά τα κενά, παρέχοντας στους ηλικιωμένους τα εργαλεία που χρειάζονται για να χρησιμοποιούν τις ψηφιακές τεχνολογίες με ασφάλεια και αυτοπεποίθηση σε ένα αποτελεσματικό, πρακτικό και ενδιαφέρον μαθησιακό περιβάλλον.

Στόχοι του είναι να αυξήσει τις γνώσεις των ηλικιωμένων σχετικά με την ασφάλεια στο διαδίκτυο, να τους παρέχει τις απαραίτητες δεξιότητες και να ενθαρρύνει την αυτοπεποίθησή τους στη χρήση των ψηφιακών τεχνολογιών με ασφάλεια. Εκτός από πρακτικά μέτρα για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής, το εκπαιδευτικό πρόγραμμα προσφέρει σαφή ενημέρωση σχετικά με τις διαδεδομένες απειλές στο διαδίκτυο και τον τρόπο αναγνώρισής τους, συμβουλές για ασφαλείς συμπεριφορές στο διαδίκτυο και πληροφορίες για πραγματικά σενάρια που απεικονίζουν πιθανές απειλές και λύσεις. Με πέντε εκτενή μαθήματα διάρκειας τεσσάρων ωρών το καθένα και δέκα διαδραστικές περιπτώσεις IMPROVE που προσομοιώνουν ad hoc αντιδράσεις σε διαδικτυακές απειλές, το πρόγραμμα δίνει μεγάλη έμφαση στην πρακτική μάθηση, εξετάζοντας πραγματικά παραδείγματα κινδύνων για την ασφάλεια στον κυβερνοχώρο. Το περιεχόμενο, οι διεξοδικές ασκήσεις με οδηγίες, καθώς και τα εργαλεία και οι πόροι που απαιτούνται για την παροχή αυτού του εκπαιδευτικού προγράμματος περιλαμβάνονται σε κάθε συνεδρία.

Αυτοί οι πόροι παρέχουν στους εκπαιδευτικούς χρήσιμες δραστηριότητες, υλικά και μεθόδους για να προσελκύσουν το ενδιαφέρον των ηλικιωμένων και να τους εμπλέξουν στην διαδραστική μάθηση. Οι εκπαιδευτικοί που ολοκληρώνουν με επιτυχία αυτό το πρόγραμμα θα είναι σε θέση να βοηθήσουν τους ηλικιωμένους να αναπτύξουν τις ψηφιακές τους δεξιότητες και την αυτοπεποίθησή τους.

1.2.1 Βασικοί στόχοι του προγράμματος

Ευαισθητοποίηση των ηλικιωμένων σχετικά με τις διαδικτυακές απειλές
Θα αποκτήσουν μια ολοκληρωμένη κατανόηση των πιο διαδεδομένων διαδικτυακών απειλών, όπως κακόβουλο λογισμικό, ηλεκτρονικό ψάρεμα, απάτες, κλοπή ταυτότητας και επικίνδυνες ιστοσελίδες. Το πρόγραμμα διδάσκει στους συμμετέχοντες πώς να αναγνωρίζουν τα προειδοποιητικά σημάδια και απεικονίζει πιθανούς κινδύνους χρησιμοποιώντας παραδείγματα από τον πραγματικό κόσμο.

Ανάπτυξη πρακτικών ψηφιακών δεξιοτήτων
Οι συμμετέχοντες θα αποκτήσουν μια ολοκληρωμένη κατανόηση του πώς να εκτελούν σωστά τυπικές εργασίες στο διαδίκτυο, όπως η χρήση των κοινωνικών μέσων, οι ηλεκτρονικές τραπεζικές συναλλαγές, οι αγορές και η περιήγηση. Δίνεται έμφαση στην ασφαλή διαχείριση δεδομένων, στην επαλήθευση δύο παραγόντων και στα ισχυρά κωδικά πρόσβασης.

Προώθηση ασφαλούς συμπεριφοράς στο διαδίκτυο
Το πρόγραμμα δίνει έμφαση στην υιοθέτηση βέλτιστων πρακτικών για την προστασία της ιδιωτικής ζωής, την ασφαλή επικοινωνία και την ηθική ψηφιακή συμμετοχή. Οι ηλικιωμένοι θα κατανοήσουν πώς να διαχειρίζονται τα προσωπικά τους στοιχεία, να αναγνωρίζουν τα δόλια μηνύματα και να ανταποκρίνονται κατάλληλα σε ύποπτες δραστηριότητες.

Εξοπλισμός των εκπαιδευτών με εξειδικευμένες γνώσεις
Η εκπαίδευση των εκπαιδευτικών και των διαμεσολαβητών αποτελεί θεμελιώδες μέρος του προγράμματος. Οι εκπαιδευτές θα αποκτήσουν τις δεξιότητες, τους πόρους και τις τεχνικές που απαιτούνται για την παροχή εκπαίδευσης σε θέματα ασφάλειας στο διαδίκτυο με έμφαση στους ηλικιωμένους. Αυτό περιλαμβάνει συμβουλές για τη διαχείριση της δυναμικής της ομάδας, τη μάθηση με βάση σενάρια και τις διαδραστικές τεχνικές διδασκαλίας.

Μείωση του ψηφιακού αποκλεισμού
Το πρόγραμμα στοχεύει στη μείωση της κοινωνικής και τεχνολογικής απομόνωσης των ηλικιωμένων, ειδικά εκείνων που ζουν εκτός αστικών περιοχών, ενισχύοντας την ψηφιακή παιδεία και τις γνώσεις τους σχετικά με την ασφάλεια στο διαδίκτυο. Στον σημερινό ψηφιακό κόσμο , οι συμμετέχοντες θα νιώθουν πιο άνετα να χρησιμοποιούν μόνοι τους τις ψηφιακές συσκευές, προωθώντας έτσι την ένταξη.

1.2.2 Αναμενόμενα αποτελέσματα

- Οι ηλικιωμένοι θα αποκτήσουν τις γνώσεις και τις πρακτικές δεξιότητες που απαιτούνται για την ασφαλή πλοήγηση στο διαδίκτυο.
- Οι εκπαιδευτές θα είναι καλά προετοιμασμένοι για να παρέχουν στους ηλικιωμένους ενδιαφέρουσες και χρήσιμες οδηγίες για την ασφάλεια στον κυβερνοχώρο.
- Οι ηλικιωμένοι με ψηφιακή ενδυνάμωση που μπορούν να συμμετέχουν σε διαδικτυακές δραστηριότητες και υπηρεσίες με ασφαλή τρόπο θα ωφελήσουν τις κοινότητές τους.

Το εκπαιδευτικό πρόγραμμα συνδυάζει τη θεωρία με διαδραστικές ασκήσεις βασισμένες σε σενάρια, μελέτες περιπτώσεων και ομαδικές δραστηριότητες, ώστε να διασφαλιστεί ότι οι μαθητές μαθαίνουν μέσω της πράξης. Κάθε ενότητα περιέχει δομημένες πληροφορίες, πρακτικές ασκήσεις και ευκαιρίες για συζήτηση, επιτρέποντας στους ηλικιωμένους να χρησιμοποιούν άμεσα τις γνώσεις τους και να αποκτήσουν αυτοπεποίθηση σε πραγματικές καταστάσεις. Το πρόγραμμα περιλαμβάνει επίσης στοιχεία αξιολόγησης και αναστοχασμού, τα οποία διασφαλίζουν την επίτευξη των μαθησιακών αποτελεσμάτων, ενώ παράλληλα προσφέρουν ανατροφοδότηση τόσο στους εκπαιδευτές όσο και στους συμμετέχοντες, ώστε να εξελίσσονται συνεχώς.

1.2.3 Βελτίωση περιπτώσεων

Οι περιπτώσεις IMPROVE είναι διαδραστικές, βασισμένες σε σενάρια μαθησιακές δραστηριότητες που έχουν ως στόχο να συμπληρώσουν τα εκπαιδευτικά modules του Cyber Safe Senior. Αυτά τα σενάρια σχετίζονται άμεσα με τα Modules I-V και παρουσιάζουν πραγματικές καταστάσεις στο διαδίκτυο που μπορεί να συναντήσουν οι ηλικιωμένοι στις καθημερινές τους ψηφιακές αλληλεπιδράσεις, όπως ηλεκτρονικά μηνύματα phishing, απάτες σε ηλεκτρονικές αγορές, επικίνδυνη χρήση δημόσιων δικτύων Wi-Fi και απάτες με επενδύσεις. Τα σενάρια, τα οποία παρέχονται μέσω διαδραστικού περιεχομένου Genially, επιτρέπουν στους συμμετέχοντες να αναγνωρίσουν πιθανές απειλές, να λάβουν τεκμηριωμένες αποφάσεις και να κατανοήσουν τις επιπτώσεις των επικίνδυνων διαδικτυακών δραστηριοτήτων. Οι περιπτώσεις IMPROVE ενθαρρύνουν τη βιωματική μάθηση, αναπαράγοντας πραγματικές ψηφιακές απειλές, επιτρέποντας στους ηλικιωμένους να αναπτύξουν πρακτικές δεξιότητες για ασφαλέστερη χρήση του διαδικτύου.

Οι περιπτώσεις Improve είναι ευθυγραμμισμένες με τις ενότητες εκπαίδευσης ανάλογα με το θεματικό τους επίκεντρο και τους μαθησιακούς στόχους του προγράμματος

- **Ενότητα I – Βασικές αρχές της ασφάλειας στον κυβερνοχώρο: Προστασία του υπολογιστή, του ηλεκτρονικού ταχυδρομείου και των προσωπικών δεδομένων σας:** Smishing; Το δίλημμα του δημόσιου Wi-Fi.
- **Ενότητα II – Συνηθισμένες διαδικτυακές απάτες που στοχεύουν ηλικιωμένους:** Απάτη των παππούδων; Η παγίδα της απάτης για φιλανθρωπικούς σκοπούς.
- **Ενότητα III – Ασφάλεια στις ηλεκτρονικές τραπεζικές συναλλαγές και τις αγορές:** Απάτες στις ηλεκτρονικές αγορές, απάτες ηλεκτρονικού ταχυδρομείου (phishing), η ψευδαίσθηση του κρυπτονομίσματος: η ψευδαίσθηση του άμεσου πλουτισμού, χρυσές αποδόσεις – το τίμημα της εμπιστοσύνης.
- **Ενότητα IV – Ασφαλής και υπεύθυνη χρήση των μέσων κοινωνικής δικτύωσης για ηλικιωμένους:** Απάτη Deepfake. Απάτη τύπου υπηρεσίας στο διαδίκτυο.
- **Ενότητα V – Ασφαλής ψηφιοποίηση των ηλικιωμένων:** Καλύπτεται εγκάρσια μέσω του συνολικού περιεχομένου και των δραστηριοτήτων της εκπαίδευσης.

Πρόσβαση σε περιπτώσεις βελτίωσης:

- Crypto Mirage: Η ψευδαίσθηση του άμεσου πλουτισμού
- Απάτες σε διαδικτυακές αγορές
- Η παγίδα της φιλανθρωπικής απάτης
- Smishing
- Το δίλημμα του δημόσιου Wi-Fi
- Απάτη ηλεκτρονικού ψαρέματος
- Απάτη με τους παππούδες
- Απάτη τύπου διαδικτυακής υπηρεσίας
- Απάτη με deepfake
- Χρυσές αποδόσεις – Το τίμημα της εμπιστοσύνης: Μια υπόθεση επενδυτικής απάτης

ΕΝΟΤΗΤΑ Ι

Βασικά στοιχεία κυβερνοασφάλειας που προστατεύουν τους υπολογιστές, το email και τα προσωπικά σας δεδομένα

2. Ενότητα Ι - Βασικές αρχές της κυβερνοασφάλειας: προστασία των υπολογιστών, του ηλεκτρονικού ταχυδρομείου και των προσωπικών δεδομένων

Το μάθημα «Βασικές αρχές της ασφάλειας στον κυβερνοχώρο» προσφέρει μια πλήρη επισκόπηση της ψηφιακής ασφάλειας, συνδυάζοντας θεωρητικές γνώσεις με πρακτικές εφαρμογές. Οι συμμετέχοντες θα αποκτήσουν μια βαθιά κατανόηση των βασικών αρχών της ασφάλειας των υπολογιστών, της ιδιωτικότητας του ηλεκτρονικού ταχυδρομείου και της προστασίας των προσωπικών δεδομένων. Η ενότητα καλύπτει σημαντικά υποθέματα, όπως η ασφάλεια των υπολογιστών και η διαχείριση του ηλεκτρονικού ταχυδρομείου, στα οποία οι μαθητές θα μάθουν πώς να συντηρούν το λειτουργικό τους σύστημα και το λογισμικό τους, να χρησιμοποιούν προγράμματα προστασίας από ιούς και τείχη προστασίας και να αναγνωρίζουν πιθανές απειλές στον κυβερνοχώρο. Εστιάζει επίσης στην ασφάλεια και τη διαχείριση των κωδικών πρόσβασης, διδάσκοντας στους χρήστες πώς να δημιουργούν ισχυρούς κωδικούς πρόσβασης και να χρησιμοποιούν επιτυχώς τους διαχειριστές κωδικών πρόσβασης.

Παρέχονται πρακτικές ασκήσεις ασφάλειας ηλεκτρονικού ταχυδρομείου, που διδάσκουν στους συμμετέχοντες πώς να αναγνωρίζουν απόπειρες ηλεκτρονικού ψαρέματος, να εντοπίζουν ύποπτους συνδέσμους ή αρχεία και να παρακολουθούν τα γραμματοκιβώτια τους για μη εξουσιοδοτημένη δραστηριότητα, συμπεριλαμβανομένης της χρήσης ελέγχου ταυτότητας δύο παραγόντων για ενισχυμένη ασφάλεια. Το πρόγραμμα εξετάζει επίσης τον τρόπο ασφάλειας προσωπικών συσκευών όπως υπολογιστές, κινητά τηλέφωνα και tablet, συμπεριλαμβανομένων τακτικών για κλείδωμα οθόνης, παρακολούθηση χαμένων συσκευών, αποφυγή μη εξουσιοδοτημένης φυσικής πρόσβασης και διατήρηση του λογισμικού ενημερωμένου για προστασία από αναδυόμενες απειλές. Τέλος, το πρόγραμμα εστιάζει στη διαχείριση προσωπικών δεδομένων και την ιδιωτικότητα στο διαδίκτυο, διδάσκοντας στους μαθητές πώς να αλλάζουν τις ρυθμίσεις απορρήτου στα μέσα κοινωνικής δικτύωσης, να προστατεύουν κρίσιμες πληροφορίες και να χρησιμοποιούν με ασφάλεια δημόσια δίκτυα Wi-Fi χρησιμοποιώντας VPN.

Συνδυάζοντας αυτά τα υποθέματα, η εκπαίδευση διασφαλίζει ότι οι ηλικιωμένοι όχι μόνο κατανοούν τις πιθανές απειλές στο ψηφιακό περιβάλλον, αλλά και μαθαίνουν πρακτικές μεθόδους για να προστατεύονται. Οι συμμετέχοντες θα ολοκληρώσουν το πρόγραμμα με μεγαλύτερη ευαισθητοποίηση, αυτοπεποίθηση στην αντιμετώπιση ζητημάτων κυβερνοασφάλειας και ικανότητα να εφαρμόζουν τις λύσεις που απέκτησαν σε πραγματικές καταστάσεις.

2.1 Μαθησιακοί στόχοι

Ο κύριος στόχος αυτού του μαθήματος είναι να εξοπλίσει τους συμμετέχοντες με τις πρακτικές γνώσεις και δεξιότητες που είναι απαραίτητες για την αποτελεσματική προστασία των υπολογιστών, των λογαριασμών ηλεκτρονικού ταχυδρομείου και των προσωπικών δεδομένων από απειλές στον κυβερνοχώρο. Οι συμμετέχοντες θα μάθουν πώς να αναγνωρίζουν πιθανές απειλές, να ελαχιστοποιούν τους κινδύνους και να εφαρμόζουν στρατηγικές για την ενίσχυση της ψηφιακής ασφάλειας τόσο στην προσωπική όσο και στην επαγγελματική τους ζωή.

- Κατανόηση των βασικών αρχών της ασφάλειας στον κυβερνοχώρο που βοηθούν στην πρόληψη επιθέσεων και στην προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση.
- Να αναπτύξουν δεξιότητες για τη δημιουργία ισχυρών κωδικών πρόσβασης και την ασφαλή αποθήκευσή τους, αυξάνοντας την ανθεκτικότητα έναντι παραβιάσεων.

- Αναγνώριση και αποφυγή επιθέσεων phishing, οι οποίες αποτελούν μία από τις πιο κοινές μεθόδους διαδικτυακής απάτης.
- Ασφαλίστε αποτελεσματικά τις προσωπικές συσκευές και τα δεδομένα που είναι αποθηκευμένα σε αυτές χρησιμοποιώντας εργαλεία όπως κρυπτογράφηση, κλείδωμα οθόνης και λειτουργίες εντοπισμού θέσης.
- Να διαχειρίζονται συνειδητά τις ρυθμίσεις απορρήτου στις πλατφόρμες κοινωνικών μέσων, ώστε να μειώνουν τον κίνδυνο διαρροής προσωπικών δεδομένων.
- Αποκτήστε γνώσεις και δεξιότητες για την ασφαλή χρήση δημόσιων δικτύων Wi-Fi χρησιμοποιώντας VPN και άλλα εργαλεία προστασίας.

2.2 Δομή, περιεχόμενο και μαθησιακά αποτελέσματα

Με την επιτυχή ολοκλήρωση αυτού του μόδουλο, οι μαθητές θα είναι σε θέση να:

- Εισαγωγή στη βασική ασφάλεια υπολογιστών: πώς να ενημερώνετε το λειτουργικό σύστημα και το λογισμικό, να χρησιμοποιείτε προγράμματα προστασίας από ιούς και τείχη προστασίας, πώς να αναγνωρίζετε σημάδια πιθανών επιθέσεων στον υπολογιστή και πώς να ελαχιστοποιείτε τον κίνδυνο εμφάνισής τους.
- Δημιουργία ασφαλών κωδικών πρόσβασης και αποθήκευσή τους: πώς να δημιουργείτε ισχυρούς κωδικούς πρόσβασης που αποτελούνται από μοναδικούς συνδυασμούς γραμμάτων, αριθμών και συμβόλων, πώς να χρησιμοποιείτε διαχειριστές κωδικών πρόσβασης για να αποφεύγετε την αποθήκευση κωδικών πρόσβασης με μη ασφαλή τρόπο, π.χ. σε χαρτί.
- Πρακτικά σενάρια για την ανίχνευση ηλεκτρονικού ψαρέματος (phishing): ανάλυση δειγμάτων μηνυμάτων ηλεκτρονικού ψαρέματος και εκμάθηση του τρόπου αναγνώρισης ύποπτων συνδέσμων, συνημμένων ή γλωσσικών λαθών, τρόπος αναφοράς ύποπτων μηνυμάτων ηλεκτρονικού ταχυδρομείου στις αρμόδιες υπηρεσίες.
- Παρακολούθηση και προστασία του γραμματοκιβωτίου σας από μη εξουσιοδοτημένη πρόσβαση: πώς να ρυθμίσετε την επαλήθευση δύο βημάτων, να παρακολουθείτε ασυνήθιστη δραστηριότητα στο γραμματοκιβώτιό σας και να ανταποκρίνεστε σε απόπειρες παραβίασης.
- Προστασία προσωπικών συσκευών (υπολογιστές, smartphone, tablet): πώς να κλειδώνετε την οθόνη και να χρησιμοποιείτε εφαρμογές που σας επιτρέπουν να εντοπίζετε χαμένες συσκευές, πώς να προστατεύετε τις συσκευές σας από τη φυσική πρόσβαση μη εξουσιοδοτημένων προσώπων.
- Προστασία προσωπικών συσκευών (υπολογιστές, smartphone, tablet): πώς να κλειδώνετε την οθόνη και να χρησιμοποιείτε εφαρμογές που σας επιτρέπουν να εντοπίζετε χαμένες συσκευές, πώς να προστατεύετε τις συσκευές σας από τη φυσική πρόσβαση μη εξουσιοδοτημένων ατόμων.
- Τακτικές ενημερώσεις λογισμικού για αυξημένη ασφάλεια: γιατί οι τακτικές ενημερώσεις είναι απαραίτητες για την προστασία των συσκευών σας από νέες απειλές και πώς να ρυθμίσετε το σύστημα για αυτόματες ενημερώσεις.
- Προστασία της ιδιωτικής σας ζωής στα μέσα κοινωνικής δικτύωσης: πώς να προσαρμόσετε τις ρυθμίσεις απορρήτου σε δημοφιλείς πλατφόρμες κοινωνικής δικτύωσης, ποιες πληροφορίες πρέπει να παραμείνουν ιδιωτικές και πώς να αποφύγετε την κοινή χρήση δεδομένων που θα μπορούσαν να χρησιμοποιηθούν με ανεπιθύμητο τρόπο.
- Κανόνες για την ασφαλή χρήση δημόσιων δικτύων Wi-Fi: κίνδυνοι από τη χρήση ανοιχτών δικτύων Wi-Fi και πώς να χρησιμοποιήσετε ένα VPN για την προστασία των δεδομένων σας όταν συνδέεστε στο διαδίκτυο σε δημόσιους χώρους.

2.3 Ατζέντα | Λεπτομερής σχέδιο συνεδρίας

ΕΝΌΤΗΤΑ Ι
Βασικές αρχές της κυβερνοασφάλειας | Προστασία των υπολογιστών, του ηλεκτρονικού ταχυδρομείου και των προσωπικών δεδομένων σας

1η Συνεδρία

Καλωσόρισμα
Διάρκεια *5 λεπτά*

Μαθησιακοί στόχοι

- Δημιουργία μιας ανοιχτής και ελκυστικής ατμόσφαιρας που ευνοεί την ενεργό συμμετοχή.

Περιεχόμενο/Μέθοδος

- Καλωσόρισμα των συμμετεχόντων και σύντομη παρουσίαση του εκπαιδευτή.
- Παρουσίαση του προγράμματος της εκπαίδευσης και των κανόνων εργασίας.
- Ενθάρρυνση των συμμετεχόντων να συστηθούν (όνομα και μία λέξη που σχετίζεται με τις απειλές στον κυβερνοχώρο).

Υλικό
Δεν απαιτείται πρόσθετο υλικό.

Σχόλια
Μπορεί να είναι χρήσιμο να παρουσιάσετε τον σκοπό του εργαστηρίου με απλή γλώσσα.

2η Συνεδρία

Δραστηριότητα για το σπάσιμο του πάγου: «Βασικές αρχές της κυβερνοασφάλειας»
Διάρκεια *15 λεπτά*

Μαθησιακοί στόχοι

- Εκμάθηση και κατανόηση βασικών όρων κυβερνοασφάλειας.
- Ενίσχυση των γνώσεων σχετικά με την ασφάλεια στον κυβερνοχώρο.

Περιεχόμενο/Μέθοδος

- Διεξαγωγή άσκησης που περιλαμβάνει την αντιστοίχιση εννοιών με ορισμούς.
- Οι συμμετέχοντες λαμβάνουν ένα φύλλο εργασίας (Παράρτημα 1). Ο στόχος των συμμετεχόντων είναι να αντιστοιχίσουν σωστά κάθε έννοια με τον αντίστοιχο ορισμό της. Η άσκηση είναι ατομική ή ομαδική, ανάλογα με την απόφαση του συντονιστή. Μετά την ολοκλήρωση της άσκησης, ο εκπαιδευτής συντονίζει μια σύντομη συζήτηση κατά την οποία συζητούνται οι απαντήσεις, διευκρινίζονται τυχόν ασαφείς σημεία και διερευνώνται θέματα που σχετίζονται με το αντικείμενο της άσκησης. Ενθάρρυνση των συμμετεχόντων να συστηθούν (όνομα και μία λέξη που σχετίζεται με τις απειλές στον κυβερνοχώρο).

Υλικό

- Φύλλο εργασίας, Icebreaker: «Βασικές έννοιες της κυβερνοασφάλειας» (Παράρτημα 1)

Σχόλια

Αυτή η εργασία εισάγει το θέμα και σας επιτρέπει να αξιολογήσετε το αρχικό επίπεδο γνώσεων των συμμετεχόντων.

3η Συνεδρία

Διάλεξη 1: Ασφάλεια υπολογιστών και ηλεκτρονικού ταχυδρομείου
Διάρκεια *20 λεπτά*

Μαθησιακοί στόχοι

- Κατανόηση της σημασίας της διατήρησης του συστήματος και του λογισμικού σας ενημερωμένων.
- Αναγνώριση των διαφορετικών τύπων απειλών στον κυβερνοχώρο, συμπεριλαμβανομένων των κακόβουλων προγραμμάτων, των προγραμμάτων υποκλοπής δεδομένων και των προγραμμάτων εκβιασμού.
- Κατανόηση του ρόλου του λογισμικού προστασίας από ιούς στην ασφάλειά σας.
- Απόκτηση των γνώσεων και των δεξιοτήτων για την ασφαλή χρήση δημόσιων δικτύων Wi-Fi με τη χρήση VPN και άλλων εργαλείων ασφαλείας.

Περιεχόμενο/Μέθοδος

- Διάλεξη που εξηγεί τις βασικές έννοιες: γιατί είναι ζωτικής σημασίας οι τακτικές ενημερώσεις του συστήματος, πώς το κακόβουλο λογισμικό διεισδύει στα συστήματα, ποιος είναι ο ρόλος του λογισμικού προστασίας από ιούς και πώς να αναγνωρίζετε ένα ασφαλές δίκτυο Wi-Fi.
- Χρήση πραγματικών παραδειγμάτων (π.χ. γνωστές επιθέσεις ransomware) για την απεικόνιση των κινδύνων που συνδέονται με τα ξεπερασμένα συστήματα και τις μη ασφαλείς συσκευές.
- Επισήμανση βέλτιστων πρακτικών, όπως η ενεργοποίηση αυτόματων ενημερώσεων και η αποφυγή ύποπτων λήψεων. Για την υλοποίηση της διάλεξης, ο εκπαιδευτής έχει στη διάθεσή του τις προτάσεις θεμάτων που παρέχονται στο Παράρτημα 2.

Υλικό

- Πρόταση θεμάτων προς συζήτηση (Παράρτημα 2)

Σχόλια

Αξίζει να ενθαρρύνετε τους συμμετέχοντες να συμμετάσχουν ενεργά στη διάλεξη, επιτρέποντάς τους να υποβάλλουν ερωτήσεις.

Δραστηριότητα 1 «Κουίζ: Σωστό/Λάθος»
Διάρκεια *20 λεπτά*

Μαθησιακοί στόχοι

- Ενίσχυση των γνώσεων από τη διάλεξη, ανάπτυξη της ευαισθητοποίησης σχετικά με τις απειλές.

Περιεχόμενο/Μέθοδος

- Το μάθημα περιλαμβάνει μια άσκηση με τη μορφή κουίζ με τίτλο «Σωστό ή λάθος;», η οποία διεξάγεται με βάση ένα φύλλο εργασίας (Παράρτημα 3) που οι συμμετέχοντες λαμβάνουν από τον εκπαιδευτή.
- Οι συμμετέχοντες έχουν 5 λεπτά για να σημειώσουν τις απαντήσεις τους ανεξάρτητα. Μετά την ολοκλήρωση αυτού του σταδίου, ο εκπαιδευτής συντονίζει μια σύντομη συζήτηση κατά την οποία συζητούνται οι σωστές απαντήσεις με την ομάδα, εξηγούνται σημαντικά ζητήματα και διορθώνονται τυχόν παρανοήσεις. Τέλος, ο εκπαιδευτής συνοψίζει το βασικό περιεχόμενο που καλύφθηκε στο κουίζ, ενισχύοντας την κατανόηση και εδραιώνοντας τις ορθές πρακτικές που σχετίζονται με την ψηφιακή ασφάλεια.

Υλικό

- Φύλλο εργασίας Κουίζ: Σωστό/Λάθος (Παράρτημα 3)

Σχόλια

Συνοψίστε τα βασικά σημεία μετά το κουίζ για να ενισχύσετε την κατανόηση των συμμετεχόντων σχετικά με τις βασικές πρακτικές ασφάλειας.

Διάλειμμα | Διάρκεια *5'*

- **Δώστε χρόνο στους συμμετέχοντες να αναζωογονηθούν και να σκεφτούν.**
- **Σύντομο διάλειμμα για ανανέωση.**
- **Ενθαρρύνετε τους συμμετέχοντες να κάνουν διατάσεις ή να πιουν κάτι για να αναζωογονηθούν πριν από την επόμενη διάλεξη.**

4η Συνεδρία

Διάλεξη 2: Πρακτικές ασκήσεις σχετικά με την ασφάλεια των email
Διάρκεια *30 λεπτά*

Μαθησιακοί στόχοι

- Μάθετε τις βέλτιστες πρακτικές για τη δημιουργία ισχυρών, ασφαλών κωδικών πρόσβασης (π.χ. χρήση κεφαλαίων και μικρών γραμμάτων, ειδικών χαρακτήρων και αριθμών).
- Κατανόηση των κινδύνων που ενέχει η κακή αποθήκευση κωδικών πρόσβασης και εκμάθηση της χρήσης προγραμμάτων διαχείρισης κωδικών πρόσβασης.

Περιεχόμενο/Μέθοδος

- Εξηγήστε τον «κανόνα των τριών στοιχείων» (μήκος, πολυπλοκότητα, μοναδικότητα) για τη δημιουργία ισχυρών κωδικών πρόσβασης. Δείξτε πώς λειτουργούν οι διαχειριστές κωδικών πρόσβασης και συζητήστε τα οφέλη τους (π.χ. αυξημένη ασφάλεια, ευκολία). Επισημάνετε τα

συνηθισμένα λάθη, όπως η επαναχρησιμοποίηση κωδικών πρόσβασης ή η αποθήκευσή τους σε μη ασφαλή αρχεία.

Υλικό

- Πρόταση θεμάτων προς συζήτηση (Παράρτημα 4)

Σχόλια

Δώστε πρακτικές συμβουλές με τις οποίες μπορούν να ταυτιστούν οι μαθητές, όπως η δημιουργία κωδικού πρόσβασης με βάση μια φράση που είναι εύκολο να θυμηθεί κανείς αλλά και μοναδική.

Δραστηριότητα 2: Δημιουργία ισχυρών κωδικών πρόσβασης
Διάρκεια *20 λεπτά*

Μαθησιακοί στόχοι

- Εξασκηθείτε στη δημιουργία ισχυρών, μοναδικών κωδικών πρόσβασης ακολουθώντας τις οδηγίες που αναφέρθηκαν.

Περιεχόμενο/Μέθοδος

- Η άσκηση πραγματοποιείται σε δύο στάδια – πρώτα ατομικά και μετά σε ζευγάρια. Έχει προετοιμαστεί ένα φύλλο εργασίας (Παράρτημα 5) για την άσκηση.
- Οι συμμετέχοντες δημιουργούν ανεξάρτητα τουλάχιστον τρεις ισχυρούς κωδικούς πρόσβασης σύμφωνα με τις αρχές ασφάλειας και τους καταγράφουν σε κάρτες. Στη συνέχεια, τους δείχνουν στον σύντροφό τους, ο οποίος αξιολογεί το μήκος, την πολυπλοκότητα και τη μοναδικότητά τους, παρέχοντας σχόλια και πιθανές προτάσεις για βελτίωση. Στο τέλος, ο εκπαιδευτής συζητά τα χαρακτηριστικά ενός ασφαλούς κωδικού πρόσβασης και ξεκινά μια συζήτηση με όλη την ομάδα, επιτρέποντας την ανταλλαγή απόψεων και καλών πρακτικών.

Υλικό

- Φύλλο εργασίας «Δημιουργία ισχυρών κωδικών πρόσβασης» (Παράρτημα 5)

Σχόλια

Αξίζει να ενθαρρύνετε τους συμμετέχοντες να προσέξουν αν οι κωδικοί πρόσβασης που χρησιμοποιούν επί του παρόντος είναι ασφαλείς σύμφωνα με τις οδηγίες του εκπαιδευτή.

Διάλειμμα | Διάρκεια *5 λεπτά*

- **Δώστε χρόνο για ξεκούραση και προετοιμασία.**
- **Σύντομο διάλειμμα για ανανέωση.**
- **Σύντομο διάλειμμα για αναζωογόνηση και χαλάρωση.**

5η Συνεδρία

Διάλεξη 3: Ασφάλεια προσωπικών συσκευών και πληροφοριών
Διάρκεια *30 λεπτά*

Μαθησιακοί στόχοι

- Απόκτηση γνώσεων σχετικά με τον τρόπο αναγνώρισης των ηλεκτρονικών μηνυμάτων phishing.
- Κατανόηση του τρόπου διαμόρφωσης των βασικών ρυθμίσεων ασφαλείας των email.

Περιεχόμενο/Μέθοδος

- Εξηγεί τα προειδοποιητικά σημάδια του phishing, όπως ορθογραφικά λάθη, άγνωστες διευθύνσεις αποστολέα και επείγοντα μηνύματα. Δείχνει πώς να προσαρμόσετε τις ρυθμίσεις ασφαλείας email σε πλατφόρμες όπως το Gmail και το Outlook. Δείχνει παραδείγματα ηλεκτρονικών μηνυμάτων phishing και συζητά πώς να αναγνωρίζετε τα προειδοποιητικά σημάδια.

Υλικό

Δεν απαιτείται πρόσθετο υλικό.

Σχόλια

Παρουσίαση πραγματικών περιπτώσεων phishing από δημοφιλείς υπηρεσίες (π.χ. PayPal, Amazon) προκειμένου να γίνει το περιεχόμενο πιο ελκυστικό.

Δραστηριότητα 3: Ανάλυση ηλεκτρονικών μηνυμάτων phishing
Διάρκεια *20 λεπτά*

Μαθησιακοί στόχοι

- Πρακτική ανάλυση μηνυμάτων ηλεκτρονικού ταχυδρομείου – ανίχνευση ανωμαλιών.

Περιεχόμενο/Μέθοδος

- Ο εκπαιδευτής έχει στη διάθεσή του μια σειρά από πρότυπα ηλεκτρονικών μηνυμάτων (Παράρτημα 6), τα οποία πρέπει να εμπλουτιστούν με λεπτομέρειες πριν διανεμηθούν στους συμμετέχοντες – όπως δείγματα συνδέσμων, ονόματα γνωστών εταιρειών (π.χ. τράπεζες, υπηρεσίες ταχυμεταφορών ή πλατφόρμες αγορών).
- Η άσκηση πραγματοποιείται σε ζεύγη ή μικρές ομάδες. Οι συμμετέχοντες αναλύουν τα προετοιμασμένα ηλεκτρονικά μηνύματα από το φύλλο εργασίας (Παράρτημα 6), εντοπίζοντας και επισημαίνοντας ύποπτα στοιχεία. Μετά την ολοκλήρωση της ανάλυσης, ακολουθεί κοινή συζήτηση με συντονιστή τον υπεύθυνο.

Προτεινόμενες ερωτήσεις για συζήτηση:

- Ποια προειδοποιητικά σημάδια υπάρχουν σε αυτό το email;
- Πώς μπορείτε να προστατευτείτε από μια τέτοια επίθεση;
- Τι πρέπει να κάνετε αν λάβετε ένα ύποπτο email αυτού του τύπου;
- Προετοιμαστείτε να συζητήσετε τις απαντήσεις με την ομάδα.

Υλικό

- Φύλλο εργασίας, Ανάλυση ηλεκτρονικού μηνύματος phishing (Παράρτημα 6)

Σχόλια

Σύνοψη των αποτελεσμάτων της ανάλυσης της ομάδας, με έμφαση στις βασικές διαφορές μεταξύ πραγματικών και ψεύτικων μηνυμάτων ηλεκτρονικού ταχυδρομείου.

Διάλειμμα

Διάρκεια 5 λεπτά

- **Δώστε χρόνο για ξεκούραση και προετοιμασία.**
- **Σύντομο διάλειμμα για ανανέωση.**
- **Σύντομο διάλειμμα για αναζωογόνηση και χαλάρωση.**

6η Συνεδρία

Διάλεξη 4: Διαχείριση προσωπικών δεδομένων και ιδιωτικότητα στο διαδίκτυο

Διάρκεια *30 λεπτά*

Μαθησιακοί στόχοι

- Ενημέρωση σχετικά με τις πολιτικές απορρήτου, τις ρυθμίσεις απορρήτου, τα κλειδώματα και τις ενημερώσεις. Ενημέρωση σχετικά με τις βασικές ρυθμίσεις ασφαλείας για την προστασία των συσκευών (π.χ. ενεργοποίηση κλειδώματος οθόνης και αυτόματων ενημερώσεων).
- Κατανόηση του τρόπου αποτελεσματικής διαχείρισης των ρυθμίσεων απορρήτου στο διαδίκτυο.

Περιεχόμενο/Μέθοδος

- Συζήτηση για τρόπους προστασίας των δεδομένων σας στα μέσα κοινωνικής δικτύωσης (Instagram, Facebook), τις ρυθμίσεις απορρήτου στα smartphone και τους περιορισμούς κοινής χρήσης εφαρμογών.
- Ο εκπαιδευτής συζητά τις βασικές ρυθμίσεις ασφαλείας σε smartphone και υπολογιστές, όπως κλειδώματα οθόνης, κρυπτογράφηση δεδομένων, διαχείριση εφαρμογών και ρυθμίσεις δικαιωμάτων σε Android και iOS.
- Συζητήστε τη διαχείριση της ιδιωτικότητας στο διαδίκτυο – πώς να ρυθμίσετε τις παραμέτρους ιδιωτικότητας στις πλατφόρμες κοινωνικών μέσων, ελέγχοντας ποιος μπορεί να δει τις αναρτήσεις, τις προσωπικές πληροφορίες και ποιες εφαρμογές έχουν πρόσβαση στα δεδομένα σας.
- Συζητήστε τις αρχές ελέγχου της ασφάλειας Wi-Fi – πώς να αναγνωρίζετε μη ασφαλείς συνδέσεις, γιατί πρέπει να αποφεύγετε τα μη προστατευμένα δημόσια δίκτυα και πώς να αυξήσετε την ασφάλεια του οικιακού σας δικτύου internet.
- Τονίστε τη σημασία της τακτικής αναθεώρησης των ρυθμίσεων απορρήτου – τη σημασία της περιοδικής αναθεώρησης και ενημέρωσης των ρυθμίσεων απορρήτου για την προσαρμογή στις μεταβαλλόμενες ανάγκες και τις νέες διαδικτυακές απειλές.

Υλικό

Δεν απαιτείται πρόσθετο υλικό.

Σχόλια

Εστιάστε σε πρακτικά, εύκολα εφαρμόσιμα βήματα για την ενίσχυση της ασφάλειας και της ιδιωτικότητας των συσκευών.

Δραστηριότητα 4: Ασφαλής διαμόρφωση συσκευών
Διάρκεια *20 λεπτά*

Μαθησιακοί στόχοι

- Εφαρμογή γνώσεων μέσω της διαμόρφωσης των ρυθμίσεων ασφαλείας σε προσωπικές συσκευές.

Περιεχόμενο/Μέθοδος

- Οι συμμετέχοντες εξασκούνται στη ρύθμιση κλειδώματος οθόνης, στην ενεργοποίηση της επαλήθευσης δύο βημάτων και στην προσαρμογή των ρυθμίσεων απορρήτου. Ο εκπαιδευτής παρέχει ατομική υποστήριξη, όπως απαιτείται.

Υλικό

- Smartphone και/ή υπολογιστές.

Σχόλια

Ενθαρρύνετε τους συμμετέχοντες να επιλύουν προβλήματα και να κάνουν ερωτήσεις καθώς ρυθμίζουν τις συσκευές τους.

7η Συνεδρία

Συζήτηση
Διάρκεια *10 λεπτά*

Μαθησιακοί στόχοι

- Σκεφτείτε τα βασικά διδάγματα που αποκομίσατε.
- Ενθαρρύνετε τους συμμετέχοντες να μοιραστούν τα πιο σημαντικά συμπεράσματα και τις απορίες που τους έχουν απομείνει.

Περιεχόμενο/Μέθοδος

- Μια συζήτηση με συντονιστή, στην οποία οι συμμετέχοντες μοιράζονται τις παρατηρήσεις, τις εμπειρίες και τις ερωτήσεις τους που απαιτούν διευκρίνιση. Ο εκπαιδευτής συνοψίζει τα βασικά σημεία και απαντά στις ερωτήσεις.

Υλικό

Δεν απαιτείται πρόσθετο υλικό.

Σχόλια

Ενθαρρύνετε τους συμμετέχοντες να συνδέσουν τις έννοιες που έμαθαν με την καθημερινή τους συμπεριφορά στο διαδίκτυο.

Σύνοψη
Διάρκεια *5 λεπτά*

Μαθησιακοί στόχοι

- ❖ Συνοψίστε τα βασικά σημεία της μάθησης και παρέχετε πόρους για περαιτέρω μάθηση.
- ❖ Ευχαριστήστε τους συμμετέχοντες και κλείστε τη συνεδρία.

Περιεχόμενο/Μέθοδος

- ❖ Σύνοψη των βασικών σημείων μάθησης από την εκπαίδευση.
- ❖ Κοινή χρήση πρόσθετων πόρων (π.χ. ιστότοποι και άρθρα σχετικά με την ασφάλεια στον κυβερνοχώρο).
- ❖ Ευχαριστήστε τους συμμετέχοντες για τη συμμετοχή τους και ενθαρρύνετέ τους να συνεχίσουν να βελτιώνουν τις πρακτικές τους στον τομέα της κυβερνοασφάλειας.

Υλικό

- ❖ Συστάσεις για περαιτέρω ανάγνωση και μάθηση για τους συμμετέχοντες (Παράρτημα 7)
- ❖ Ιστοσελίδες για την ασφάλεια στον κυβερνοχώρο: Ευρωπαϊκοί και κυβερνητικοί οργανισμοί ασφάλειας στον κυβερνοχώρο

Σχόλια

Τέλος, αξίζει να διεξαχθεί μια σύντομη έρευνα αξιολόγησης.

2.4 Πρόσθετες πληροφορίες

2.4.1 Αυτοαξιολόγηση των εκπαιδευτών

- ➢ Μεταβίβασα με σαφήνεια και αποτελεσματικότητα στους συμμετέχοντες τη σημασία της ασφάλειας στο διαδίκτυο και της συνειδητής χρήσης των μέσων κοινωνικής δικτύωσης;
- ➢ Χρησιμοποίησα πρακτικά παραδείγματα που βοήθησαν στην καλύτερη κατανόηση των ψηφιακών απειλών;
- ➢ Διασφάλισα ότι οι συμμετέχοντες κατανόησαν τις τεχνικές πτυχές των ρυθμίσεων απορρήτου και της αναγνώρισης απάτης;
- ➢ Διασφάλισα ότι οι συμμετέχοντες κατανόησαν τις τεχνικές πτυχές των ρυθμίσεων απορρήτου και ήταν σε θέση να αναγνωρίσουν απάτες όπως το phishing;
- ➢ Προσάρμοσα τις πληροφορίες που παρείχα στο επίπεδο προόδου των συμμετεχόντων;
- ➢ Πώς ενθάρρυνα τη συμμετοχή των συμμετεχόντων κατά τη διάρκεια των δραστηριοτήτων και των συζητήσεων;
- ➢ Ενθάρρυνα την ενεργό συμμετοχή, την ανταλλαγή εμπειριών και την υποβολή ερωτήσεων;
- ➢ Τα υλικά και οι πόροι που χρησιμοποιήθηκαν (π.χ. παρουσιάσεις, κουίζ, πρακτικές ασκήσεις) ήταν χρήσιμα και κατάλληλα για τους συμμετέχοντες;
- ➢ Τα υλικά που προετοιμάστηκαν ήταν σαφή και κατανοητά;

2.4.2 Αξιολόγηση του προγράμματος από τους εκπαιδευτές

- Ήταν το περιεχόμενο της εκπαίδευσης σχετικό με τις ανάγκες των ηλικιωμένων και κατάλληλα προσαρμοσμένο στο επίπεδο γνώσεων και εμπειρίας τους;
- Είχαν οι συμμετέχοντες την ευκαιρία να κατανοήσουν τις βασικές αρχές της ασφάλειας στον κυβερνοχώρο και της ιδιωτικότητας στο διαδίκτυο;
- Οι δραστηριότητες όπως κουίζ, πρακτικές ασκήσεις και ανάλυση παραδειγμάτων ηλεκτρονικού ψαρέματος (phishing) υποστήριξαν τη μαθησιακή διαδικασία των συμμετεχόντων;
- Οι συζητήσεις επέτρεψαν την εμβάθυνση των γνώσεων και ενθάρρυναν τον προβληματισμό σχετικά με την ψηφιακή ασφάλεια;
- Τα επιτευχθέντα αποτελέσματα (π.χ. κατανόηση των ψηφιακών απειλών, ικανότητα διαμόρφωσης των ρυθμίσεων ασφαλείας) είναι σύμφωνα με τους επιδιωκόμενους εκπαιδευτικούς στόχους του μαθήματος;
- Οι συμμετέχοντες απέκτησαν βασικές δεξιότητες, όπως η δημιουργία ισχυρών κωδικών πρόσβασης, η αναγνώριση της απάτης και η διαχείριση της ιδιωτικότητας στο διαδίκτυο;

2.4.3 Υλικό, πρόσθετοι πόροι

Παράρτημα 1 | Φύλλο εργασίας Δραστηριότητα για το σπάσιμο του πάγου: «Βασικές έννοιες της κυβερνοασφάλειας»

Ταιριάξτε την έννοια με τον σωστό ορισμό:

Phishing	**μια δόλια μέθοδος υποκρισίας αξιόπιστων οντοτήτων με σκοπό την κλοπή ευαίσθητων δεδομένων.**
Ransomware	**κακόβουλο λογισμικό που κρυπτογραφεί δεδομένα και απαιτεί λύτρα για την απελευθέρωσή τους.**
Διπλή αυθεντικοποίηση (2FA)	**ένα επιπλέον επίπεδο ασφάλειας που απαιτεί έναν δεύτερο παράγοντα πιστοποίησης.**
Κωδικοί πρόσβασης & διαχειριστές κωδικών πρόσβασης	**στρατηγικές για τη διαχείριση ισχυρών και μοναδικών κωδικών πρόσβασης για διαφορετικές υπηρεσίες.**
Τείχος προστασίας	**ένα σύστημα ασφαλείας που προστατεύει από μη εξουσιοδοτημένη πρόσβαση σε ένα δίκτυο.**
Κρυπτογράφηση δεδομένων	**Μέθοδος προστασίας των δεδομένων από μη εξουσιοδοτημένη πρόσβαση, μετατρέποντάς τα σε μη αναγνώσιμο κώδικα.**
VPN (Εικονικό ιδιωτικό δίκτυο)	**μια τεχνολογία που εξασφαλίζει ασφαλείς και ιδιωτικές συνδέσεις στο διαδίκτυο.**
Ασφαλής ηλεκτρονική αλληλογραφία	**πρακτικές για την προστασία των μηνυμάτων ηλεκτρονικού ταχυδρομείου από επιθέσεις, όπως το φιλτράρισμα ανεπιθύμητων μηνυμάτων και η**
SOC (Κέντρο Λειτουργιών Ασφαλείας)	**ένα κέντρο επιχειρήσεων υπεύθυνο για την παρακολούθηση και την αντιμετώπιση απειλών στον τομέα της ασφάλειας στον κυβερνογώρο.**

Παράρτημα 1 | Φύλλο εργασίας Δραστηριότητα για το σπάσιμο του πάγου: «Βασικές έννοιες της ασφάλειας στον κυβερνοχώρο»
Σωστές απαντήσεις

1. **Phishing** – μια δόλια μέθοδος υποκρισίας αξιόπιστων οντοτήτων με σκοπό την κλοπή ευαίσθητων δεδομένων.
2. **Ransomware** – κακόβουλο λογισμικό που κρυπτογραφεί δεδομένα και απαιτεί λύτρα για την απελευθέρωσή τους.
3. **Διπλή επαλήθευση ταυτότητας (2FA)** – ένα επιπλέον επίπεδο ασφάλειας που απαιτεί έναν δεύτερο παράγοντα επαλήθευσης ταυτότητας.
4. **Κωδικοί πρόσβασης και διαχειριστές κωδικών πρόσβασης** – στρατηγικές για τη διαχείριση ισχυρών και μοναδικών κωδικών πρόσβασης για διαφορετικές υπηρεσίες.
5. **Τείχος προστασίας** – ένα σύστημα ασφαλείας που προστατεύει από μη εξουσιοδοτημένη πρόσβαση σε ένα δίκτυο.
6. **Κρυπτογράφηση δεδομένων** – μέθοδος προστασίας των δεδομένων από μη εξουσιοδοτημένη πρόσβαση, μετατρέποντάς τα σε μη αναγνώσιμο κώδικα.
7. **Κακόβουλο λογισμικό** – λογισμικό που έχει σχεδιαστεί για να βλάπτει τους χρήστες ή τα συστήματα υπολογιστών.
8. **VPN (Virtual Private Network)** – τεχνολογία που εξασφαλίζει ασφαλείς και ιδιωτικές συνδέσεις στο διαδίκτυο.
9. **Ασφαλές ηλεκτρονικό ταχυδρομείο** – πρακτικές για την προστασία των μηνυμάτων ηλεκτρονικού ταχυδρομείου από επιθέσεις, όπως το φιλτράρισμα ανεπιθύμητων μηνυμάτων και η κρυπτογράφηση.
10. **SOC (Κέντρο Λειτουργιών Ασφαλείας)** – ένα κέντρο λειτουργιών υπεύθυνο για την παρακολούθηση και την αντιμετώπιση απειλών στον κυβερνοχώρο.

Παράρτημα 2 | Προτεινόμενα θέματα προς συζήτηση Διάλεξη 1 | Ασφάλεια υπολογιστών και ηλεκτρονικού ταχυδρομείου

- Η σημασία των τακτικών ενημερώσεων των λειτουργικών συστημάτων και των εφαρμογών.
- Οι κίνδυνοι των ξεπερασμένων συστημάτων και των μη ασφαλών συσκευών.
- Τύποι κακόβουλου λογισμικού: ιοί, Trojan horses, ransomware και πώς λειτουργούν.
- Οι μηχανισμοί που επιτρέπουν στο κακόβουλο λογισμικό να διεισδύσει στα συστήματα.
- Ο ρόλος του λογισμικού προστασίας από ιούς στην προστασία από απειλές στον κυβερνοχώρο.
- Χρήση τειχών προστασίας για προστασία από επιθέσεις.
- Πρακτικές διαχείρισης κωδικών πρόσβασης, συμπεριλαμβανομένης της χρήσης διαχειριστών κωδικών πρόσβασης.
- Κανόνες για την αποφυγή επικίνδυνων συνημμένων και ύποπτων συνδέσμων σε μηνύματα ηλεκτρονικού ταχυδρομείου.

- Η σημασία της κρυπτογράφησης δεδομένων για την προστασία της ιδιωτικότητας και της ασφάλειας.
- Οι αυτόματες ενημερώσεις ως βέλτιστη πρακτική για τη διασφάλιση της ασφάλειας.
- Τα VPN και ο ρόλος τους στην προστασία της ιδιωτικότητας στο διαδίκτυο.
- Γιατί δεν είναι όλα τα δωρεάν δίκτυα Wi-Fi ασφαλή;
- Βασική προστασία email από phishing και spam.
- Βέλτιστες πρακτικές για τη δημιουργία ισχυρών κωδικών πρόσβασης και η επίδρασή τους στην ασφάλεια.
- Ασφάλεια κινητών συσκευών και εφαρμογών.
- Η σημασία της εκπαίδευσης και της ευαισθητοποίησης των χρηστών στην πρόληψη των κυβερνοεπιθέσεων.

Παράρτημα 3 | Φύλλο εργασίας Κουίζ: Σωστό/Λάθος

Σημειώστε ποιες από τις παρακάτω προτάσεις είναι σωστές και ποιες είναι λάθος.

- Οι τακτικές ενημερώσεις του λειτουργικού συστήματος και των εφαρμογών είναι απαραίτητες μόνο για τις νέες συσκευές. **Σωστό/Λάθος**
- Το κακόβουλο λογισμικό, όπως οι ιοί ή τα trojans, μπορεί να διεισδύσει στα συστήματα μέσω παρωχημένου λογισμικού και τρωτών σημείων ασφαλείας. **Σωστό/Λάθος**
- Το λογισμικό προστασίας από ιούς είναι περιττό εάν το σύστημα ενημερώνεται τακτικά. **Σωστό/Λάθος**
- Το τείχος προστασίας χρησιμοποιείται μόνο για την προστασία από φυσικές επιθέσεις σε συσκευές. **Σωστό/Λάθος**
- Η διαχείριση κωδικών πρόσβασης και η χρήση προγραμμάτων διαχείρισης κωδικών πρόσβασης είναι ζωτικής σημασίας για τη διατήρηση ισχυρών, μοναδικών κωδικών πρόσβασης για διάφορες υπηρεσίες. **Σωστό/Λάθος**
- Η αποφυγή ύποπτων συνημμένων σε μηνύματα ηλεκτρονικού ταχυδρομείου δεν είναι σημαντική εάν έχει εγκατασταθεί λογισμικό προστασίας από ιούς. **Σωστό/Λάθος**
- Η κρυπτογράφηση δεδομένων βοηθά στην προστασία της ιδιωτικότητας και της ασφάλειας από μη εξουσιοδοτημένη πρόσβαση. **Σωστό/Λάθος**
- Οι αυτόματες ενημερώσεις είναι προαιρετικές, καθώς η χειροκίνητη ενημέρωση του συστήματος είναι πάντα αρκετή για να διασφαλιστεί η ασφάλεια. **Σωστό/Λάθος**
- Ένα VPN (Virtual Private Network) επιτρέπει την ασφαλή σύνδεση στο διαδίκτυο, κρύβοντας τη δραστηριότητά μας στο διαδίκτυο. **Σωστό/Λάθος**
- Το phishing είναι μια τεχνική επίθεσης που περιλαμβάνει την κλοπή κωδικών πρόσβασης μέσω ηλεκτρονικών μηνυμάτων που φαίνονται αξιόπιστα. **Σωστό/Λάθος**
- Ένας ισχυρός κωδικός πρόσβασης πρέπει να αποτελείται μόνο από γράμματα και να είναι εύκολος να θυμηθεί, ώστε να μην είναι δύσκολο να χρησιμοποιηθεί. Οι κινητές συσκευές απαιτούν λιγότερα μέτρα ασφαλείας από τους επιτραπέζιους υπολογιστές, καθώς είναι λιγότερο επιρρεπείς σε επιθέσεις. **Σωστό/Λάθος**
- Οι κινητές συσκευές απαιτούν λιγότερα μέτρα ασφαλείας από τους επιτραπέζιους υπολογιστές, καθώς είναι λιγότερο επιρρεπείς σε επιθέσεις. **Σωστό/Λάθος**
- Η γνώση των χρηστών σχετικά με τις διαδικτυακές απειλές είναι απαραίτητη για την πρόληψη των κυβερνοεπιθέσεων. **Σωστό/Λάθος**
- Το ransomware είναι ένα λογισμικό που μπλοκάρει την πρόσβαση σε ένα σύστημα ή αρχεία και απαιτεί λύτρα για να τα ξεκλειδώσει. **Σωστό/Λάθος**
- Ένα ξεπερασμένο λειτουργικό σύστημα είναι ασφαλές, επειδή οι παλαιότερες εκδόσεις λογισμικού σπάνια αποτελούν στόχο επιθέσεων. **Σωστό/Λάθος**

Παράρτημα 3 | Φύλλο εργασίας Κουίζ: Σωστό/Λάθος
Σωστές απαντήσεις

1. Οι τακτικές ενημερώσεις του λειτουργικού συστήματος και των εφαρμογών είναι απαραίτητες μόνο για τις νέες συσκευές. **Λάθος**
2. Το κακόβουλο λογισμικό, όπως οι ιοί ή τα trojans, μπορεί να διεισδύσει σε συστήματα μέσω παλαιού λογισμικού και τρωτών σημείων ασφαλείας. **Σωστό**
3. Το λογισμικό προστασίας από ιούς είναι περιττό εάν το σύστημα ενημερώνεται τακτικά. **Λάθος**
4. Το τείχος προστασίας χρησιμοποιείται μόνο για την προστασία από φυσικές επιθέσεις σε συσκευές. **Λάθος**
5. Η διαχείριση κωδικών πρόσβασης και η χρήση προγραμμάτων διαχείρισης κωδικών πρόσβασης είναι ζωτικής σημασίας για τη διατήρηση ισχυρών, μοναδικών κωδικών πρόσβασης για διάφορες υπηρεσίες. **Σωστό**
6. Η αποφυγή ύποπτων συνημμένων σε μηνύματα ηλεκτρονικού ταχυδρομείου δεν είναι σημαντική εάν έχει εγκατασταθεί λογισμικό προστασίας από ιούς. **Λάθος**
7. Η κρυπτογράφηση δεδομένων βοηθά στην προστασία της ιδιωτικότητας και της ασφάλειας από μη εξουσιοδοτημένη πρόσβαση. **Σωστό**
8. Οι αυτόματες ενημερώσεις είναι προαιρετικές, επειδή η χειροκίνητη ενημέρωση του συστήματος είναι πάντα αρκετή για να διασφαλιστεί η ασφάλεια. **Λάθος**
9. Ένα VPN (Virtual Private Network) επιτρέπει την ασφαλή σύνδεση στο διαδίκτυο, κρύβοντας τη δραστηριότητά μας στο διαδίκτυο. **Σωστό**
10. Το phishing είναι μια τεχνική επίθεσης που περιλαμβάνει την κλοπή κωδικών πρόσβασης μέσω email που φαίνονται αξιόπιστα. **Σωστό**
11. Ένας ισχυρός κωδικός πρόσβασης πρέπει να αποτελείται μόνο από γράμματα και να είναι εύκολος να θυμηθεί, ώστε να μην είναι δύσκολο να χρησιμοποιηθεί. **Λάθος**
12. Οι κινητές συσκευές απαιτούν λιγότερα μέτρα ασφαλείας από τους επιτραπέζιους υπολογιστές, καθώς είναι λιγότερο επιρρεπείς σε επιθέσεις. **Λάθος**
13. Η γνώση των χρηστών σχετικά με τις διαδικτυακές απειλές είναι απαραίτητη για την πρόληψη των κυβερνοεπιθέσεων. **Σωστό**
14. Το ransomware είναι ένα λογισμικό που μπλοκάρει την πρόσβαση σε ένα σύστημα ή αρχεία και απαιτεί λύτρα για να τα ξεκλειδώσει. **Λάθος**
15. Ένα ξεπερασμένο λειτουργικό σύστημα είναι ασφαλές, επειδή οι παλαιότερες εκδόσεις λογισμικού σπάνια αποτελούν στόχο επιθέσεων. **Λάθος**

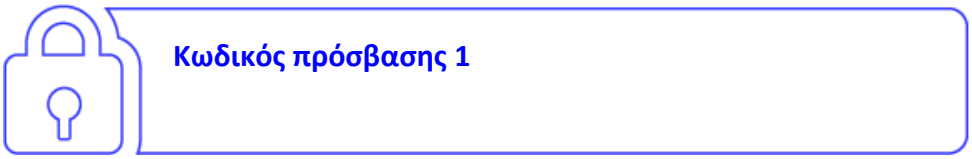
Παράρτημα 4 | Προτεινόμενα θέματα για τη Διάλεξη 2 «Πρακτικές ασκήσεις για την ασφάλεια του ηλεκτρονικού ταχυδρομείου»

- Δημιουργία ασφαλών κωδικών πρόσβασης – αρχές για τη δημιουργία ισχυρών κωδικών πρόσβασης που είναι δύσκολο να παραβιαστούν, συμπεριλαμβανομένης της χρήσης διαφορετικών τύπων χαρακτήρων (κεφαλαία, μικρά, αριθμοί, ειδικοί χαρακτήρες).
- Διαχείριση κωδικών πρόσβασης – πώς να αποφύγετε την αποθήκευση κωδικών πρόσβασης σε μη ασφαλείς θέσεις, όπως σημειώσεις σε χαρτί, και πώς να χρησιμοποιείτε προγράμματα διαχείρισης κωδικών πρόσβασης για ασφαλή αποθήκευση.
- Η αρχή των τριών συστατικών – εξήγηση του λόγου για τον οποίο ένας κωδικός πρόσβασης πρέπει να έχει το κατάλληλο μήκος, πολυπλοκότητα και μοναδικότητα για να εξασφαλίζει υψηλή ασφάλεια.
- Ο ρόλος των προγραμμάτων διαχείρισης κωδικών πρόσβασης – συζήτηση για τον τρόπο λειτουργίας των προγραμμάτων διαχείρισης κωδικών πρόσβασης και τα οφέλη που προσφέρουν, όπως ασφάλεια και ευκολία στη διαχείριση πολλαπλών κωδικών πρόσβασης.
- Συνηθισμένα λάθη στη διαχείριση κωδικών πρόσβασης – πόσο επικίνδυνο είναι να επαναχρησιμοποιείτε τους ίδιους κωδικούς πρόσβασης σε διαφορετικές υπηρεσίες ή να τους αποθηκεύετε σε μη ασφαλή αρχεία.
- Πρακτικές ασφάλειας ηλεκτρονικού ταχυδρομείου – πώς να αποφεύγετε ύποπτους συνδέσμους και συνημμένα και πώς να χρησιμοποιείτε πρόσθετες μεθόδους προστασίας, όπως η κρυπτογράφηση.

Παράρτημα 5 | Φύλλο εργασίας «Δημιουργία ισχυρών κωδικών πρόσβασης»
Δημιουργήστε ισχυρούς και ασφαλείς κωδικούς πρόσβασης με βάση τις ακόλουθες αρχές:

· Κατάλληλο μήκος (τουλάχιστον 12 χαρακτήρες),
· Πολυπλοκότητα (κεφαλαία και μικρά γράμματα, αριθμοί, ειδικοί χαρακτήρες),
· Μοναδικότητα (χωρίς προφανή μοτίβα, όπως η ημερομηνία γέννησης).

Ατομική εργασία: Γράψτε τουλάχιστον τρεις διαφορετικούς κωδικούς πρόσβασης:



Παράρτημα 5 | Φύλλο εργασίας | Δημιουργία ισχυρών κωδικών πρόσβασης

Εργαστείτε σε ζευγάρια:

· Αφού ολοκληρώσετε την ατομική εργασία, σχηματίστε ζευγάρια με έναν άλλο συμμετέχοντα.
· Δείξτε τους τους κωδικούς πρόσβασής σας.
· Ζητήστε τους να σημειώσουν (π.χ. με ένα συν) αν οι κωδικοί πληρούν όλα τα κριτήρια.
· Ο εκπαιδευτής μπορεί να κάνει σχόλια και προτάσεις για πιθανές βελτιώσεις.

Κωδικός πρόσβασης 1

Μήκος	**Σημειώσεις**
Πολυπλοκότητα	
Ευελιξία	

Κωδικός πρόσβασης 2

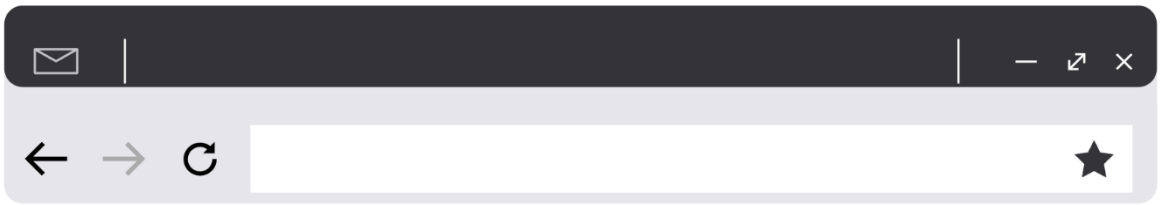
Μήκος	**Σημειώσεις**
Πολυπλοκότητα	
Ευελιξία	

Κωδικός πρόσβασης 3

Μήκος	**Σημειώσεις**
Πολυπλοκότητα	
Ευελιξία	

Παράρτημα 6 | Φύλλο εργασίας | Ανάλυση ηλεκτρονικού ταχυδρομείου phishing

Διαβάστε προσεκτικά τα παρακάτω email. Προσδιορίστε τα στοιχεία που υποδηλώνουν ότι πρόκειται για email phishing.



Subject : **Επείγον! Ο λογαριασμός σας έχει αποκλειστεί!**

Αγαπητέ χρήστη,

Λόγω ύποπτης δραστηριότητας στον λογαριασμό σας, ο λογαριασμός σας έχει αποκλειστεί προσωρινά για την προστασία των προσωπικών σας δεδομένων. Για να αποφύγετε τον μόνιμο αποκλεισμό, επαληθεύστε αμέσως τον λογαριασμό σας.

Κάντε κλικ εδώ για να επαληθεύσετε τα στοιχεία σας και να ξεκλειδώσετε τον λογαριασμό σας: [Σύνδεσμος ηλεκτρονικού ψαρέματος]

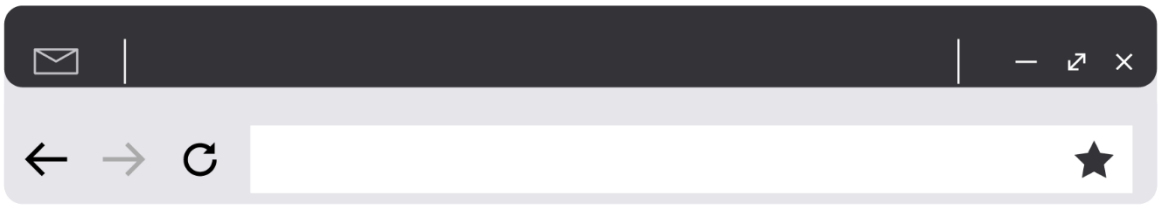
Εάν δεν ολοκληρώσετε αυτή την ενέργεια εντός 24 ωρών, ο λογαριασμός σας θα αποκλειστεί μόνιμα. Παρακαλούμε να αναλάβετε άμεση δράση για να αποφύγετε τυχόν ταλαιπωρία.

Εάν έχετε οποιεσδήποτε ερωτήσεις, επικοινωνήστε με την ομάδα τεχνικής υποστήριξης.

Με εκτίμηση,
Ομάδα ασφαλείας
[Ψεύτικη εταιρεία]

Παράρτημα 6 | Φύλλο εργασίας | Ανάλυση ηλεκτρονικού ταχυδρομείου phishing

Διαβάστε προσεκτικά τα παρακάτω email. Προσδιορίστε τα στοιχεία που υποδηλώνουν ότι πρόκειται για email phishing.



Subject : **Ενημερώστε τα στοιχεία σας! Ο λογαριασμός σας απαιτεί επαλήθευση**

Γεια σας [Όνομα],

Ο λογαριασμός σας στην [Ψεύτικη εταιρεία] απαιτεί άμεση ενημέρωση των προσωπικών σας στοιχείων. Λόγω ενός τακτικού ελέγχου ασφαλείας, πρέπει να βεβαιωθούμε ότι τα δεδομένα σας είναι ενημερωμένα, ώστε να σας παραχωρήσουμε πλήρη πρόσβαση στις υπηρεσίες μας. Για να ενημερώσετε τα στοιχεία σας, κάντε κλικ στον παρακάτω σύνδεσμο και συνδεθείτε στον λογαριασμό σας:

[Σύνδεσμος ηλεκτρονικού ψαρέματος – κάντε κλικ εδώ για να ενημερώσετε τα στοιχεία σας]

Αφού κάνετε κλικ στον σύνδεσμο, θα μεταφερθείτε σε μια σελίδα όπου θα πρέπει να εισαγάγετε τα στοιχεία σύνδεσης, τον αριθμό της πιστωτικής σας κάρτας και άλλες ευαίσθητες πληροφορίες.

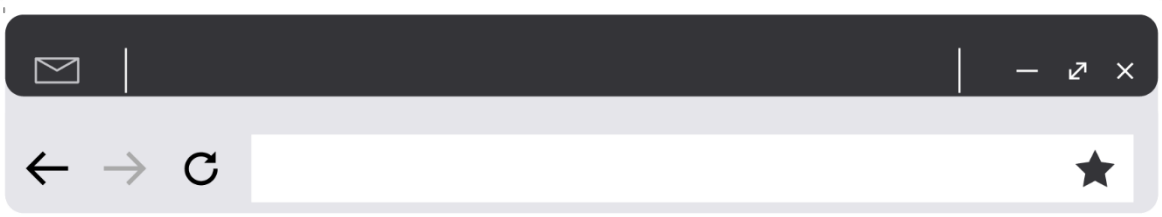
ΠΡΟΕΙΔΟΠΟΙΗΣΗ: Εάν δεν ενημερώσετε τα στοιχεία σας εντός 48 ωρών, ο λογαριασμός σας θα ανασταλεί μόνιμα.

Σας ευχαριστούμε για την κατανόηση και τη συνεργασία σας.

Με εκτίμηση
[Ψεύτικη εταιρεία]
Ομάδα υποστήριξης πελατών

Παράρτημα 6 | Φύλλο εργασίας | Ανάλυση ηλεκτρονικού μηνύματος phishing

Διαβάστε προσεκτικά τα παρακάτω email. Προσδιορίστε τα στοιχεία που υποδηλώνουν ότι πρόκειται για email phishing.



Subject : **Επιβεβαίωση αποστολής - το δέμα δεν μπόρεσε να παραδοθεί**

Καλημέρα

Το δέμα σας δεν μπόρεσε να παραδοθεί λόγω λανθασμένων στοιχείων διεύθυνσης. Παρακαλούμε επαληθεύστε αμέσως τα στοιχεία σας, ώστε να μπορέσουμε να επαναλάβουμε την παράδοση.

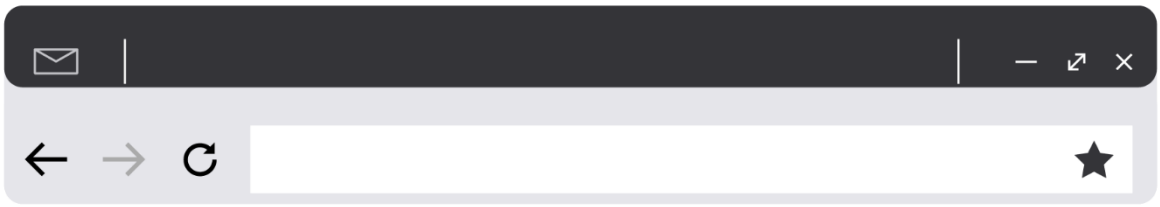
Κάντε κλικ εδώ για να ενημερώσετε τα στοιχεία παράδοσης: [σύνδεσμος ηλεκτρονικού ψαρέματος]

Εάν δεν επιβεβαιώσετε τη διεύθυνσή σας εντός 24 ωρών, το δέμα θα επιστραφεί στον αποστολέα και θα επιβαρυνθείτε με επιπλέον έξοδα.

Σας ευχαριστούμε για την άμεση ανταπόκρισή σας.
Ομάδα αποστολών
[Ψεύτικη εταιρεία ταχυμεταφορών]

Παράρτημα 6 | Φύλλο εργασίας | Ανάλυση ηλεκτρονικού μηνύματος phishing

Διαβάστε προσεκτικά τα παρακάτω email. Προσδιορίστε τα στοιχεία που υποδηλώνουν ότι πρόκειται για email phishing.



Subject : **Λάβατε μια ηλεκτρονική δωροκάρτα! Αξιώστε την τώρα!**

Συγχαρητήρια!

Έχετε επιλεγεί ως νικητής της τυχαίας προωθητικής μας ενέργειας. Λαμβάνετε μια ηλεκτρονική δωροκάρτα αξίας 500 PLN που μπορείτε να χρησιμοποιήσετε στο [Δημοφιλές δίκτυο λιανικής πώλησης].

Για να διεκδικήσετε το έπαθλο σας, κάντε κλικ στον παρακάτω σύνδεσμο και επιβεβαιώστε τα στοιχεία σας: [σύνδεσμος ηλεκτρονικού ψαρέματος - αξίωση ηλεκτρονικής κάρτας]

Η προσφορά ισχύει μόνο για 12 ώρες.
Μην χάσετε την ευκαιρία!

Καλή σας μέρα!
Τμήμα Προώθησης
[Ψεύτικη εταιρεία ή δίκτυο λιανικής πώλησης]

Παράρτημα 7 | Προτάσεις για περαιτέρω ανάγνωση και μάθηση για τους συμμετέχοντες

Ιστοσελίδες για την ασφάλεια στον κυβερνοχώρο: Ευρωπαϊκοί και κυβερνητικοί οργανισμοί που ασχολούνται με την ασφάλεια στον κυβερνοχώρο

1) **ENISA (Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια)**
   Ιστότοπος: https://www.enisa.europa.eu/
   Η ENISA είναι ο οργανισμός της ΕΕ που ασχολείται με την κυβερνοασφάλεια και δημοσιεύει εκθέσεις, οδηγούς και προειδοποιήσεις σχετικά με τις κυβερνοαπειλές.

2) **CERT-EU (Ομάδα Αντιμετώπισης Έκτακτων Περιστατικών Πληροφορικής για τα Όργανα της ΕΕ)**
   Ιστότοπος: https://cert.europa.eu/
   Ο οργανισμός παρακολουθεί τις κυβερνοαπειλές και ανταποκρίνεται στις κυβερνοεπιθέσεις κατά των ευρωπαϊκών θεσμικών οργάνων.

3) **EC3 – Κέντρο Κυβερνοεγκλημάτων της Ευρωπόλης**
   Ιστοσελίδα: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime
   Η Europol παρέχει πληροφορίες σχετικά με το έγκλημα στον κυβερνοχώρο και την ασφάλεια των δεδομένων.

4) **NCSC UK (Εθνικό Κέντρο Κυβερνοασφάλειας)**
   Ιστοσελίδα: https://www.ncsc.gov.uk/
   Η πύλη κυβερνοασφάλειας της βρετανικής κυβέρνησης, η οποία προσφέρει οδηγούς, ειδοποιήσεις και διαδικτυακά μαθήματα για πολίτες, επιχειρήσεις και δημόσιους φορείς.

2.5 Ενότητα Ι - Προ/Μετα-τεστ

1. Ποιο από τα παρακάτω περιγράφει καλύτερα τον όρο «phishing»;

Α) Εγκατάσταση ενημερώσεων για τη βελτίωση της απόδοσης του υπολογιστή
Β) Μια μέθοδος εξαπάτησης των ανθρώπων ώστε να αποκαλύψουν προσωπικές πληροφορίες μέσω ψεύτικων μηνυμάτων ηλεκτρονικού ταχυδρομείου
Γ) Ένας τύπος προγράμματος προστασίας από ιούς
Δ) Μια διαδικασία κρυπτογράφησης δεδομένων

2. Γιατί είναι σημαντικές οι τακτικές ενημερώσεις λογισμικού;

Α) Κάνουν τον υπολογιστή σας πιο αργό
Β) Αλλάζουν τον σχεδιασμό του υπολογιστή σας
Γ) Διορθώνουν τα κενά ασφαλείας και προστατεύουν από νέες απειλές
Δ) Αφαιρούν το λογισμικό προστασίας από ιούς

3. Ποια είναι η κύρια λειτουργία ενός τείχους προστασίας;

Α) Να επιταχύνει τη σύνδεσή σας στο διαδίκτυο
Β) Να προστατεύει από μη εξουσιοδοτημένη πρόσβαση σε ένα δίκτυο
Γ) Να αποθηκεύει κωδικούς πρόσβασης με ασφάλεια
Δ) Να διαγράφει αυτόματα τα ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου

4. Ποιος από τους παρακάτω κωδικούς πρόσβασης είναι ο πιο ασφαλής;

Α) password123
Β) 12345678
Γ) MyDogIsCute
Δ) M@rK_82!x

5. Τι πρέπει να κάνετε αν λάβετε ένα email από άγνωστο αποστολέα που σας ζητά προσωπικά δεδομένα;

Α) Να απαντήσετε αμέσως με τα στοιχεία σας
Β) Κάντε κλικ στον σύνδεσμο για να δείτε τι αφορά
Γ) Διαγράψτε το email ή αναφέρετέ το ως phishing
Δ) Προωθήστε το στους φίλους σας για να τους προειδοποιήσετε

6. Σε τι χρησιμεύει η «αυθεντικοποίηση δύο παραγόντων (2FA)»;

Α) Σας επιτρέπει να χρησιμοποιείτε δύο κωδικούς πρόσβασης ταυτόχρονα
Β) Προσθέτει ένα επιπλέον επίπεδο ασφάλειας, απαιτώντας δύο μορφές επαλήθευσης
Γ) Κρυπτογραφεί αυτόματα τα email σας
Δ) Αποθηκεύει τα στοιχεία σύνδεσής σας

7. Ποια από τις παρακάτω προτάσεις σχετικά με τα δημόσια δίκτυα Wi-Fi είναι ΣΩΣΤΗ;

Α) Είναι πάντα ασφαλή αν η σύνδεση είναι δωρεάν
Β) Πρέπει να αποφεύγετε την εισαγωγή ευαίσθητων δεδομένων όταν χρησιμοποιείτε δημόσιο Wi-Fi
Γ) Μπορείτε να τα χρησιμοποιείτε με ασφάλεια χωρίς κωδικό πρόσβασης
Δ) Κρυπτογραφούν αυτόματα τα δεδομένα σας

8. Ποιος είναι ο σκοπός ενός VPN (Εικονικού Ιδιωτικού Δικτύου);

Α) Να βελτιώσει την ταχύτητα του διαδικτύου σας
Β) Για να μπλοκάρει τις αναδυόμενες διαφημίσεις
Γ) Να παρέχει μια ασφαλή και ιδιωτική σύνδεση στο διαδίκτυο
Δ) Για να διαχειριστείτε τους κωδικούς πρόσβασής σας

9. Ποιο από τα παρακάτω είναι παράδειγμα ransomware;

Α) Λογισμικό που κρυπτογραφεί τα αρχεία σας και απαιτεί πληρωμή για να τα ξεκλειδώσει
Β) Ένα πρόγραμμα προστασίας από ιούς που σαρώνει το σύστημά σας
Γ) Ένα εργαλείο για τον αποκλεισμό ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου
Δ) Μια εφαρμογή τείχους προστασίας

10. Ποια είναι μια καλή πρακτική για την προστασία της ιδιωτικότητάς σας στα μέσα κοινωνικής δικτύωσης;

Α) Να μοιράζεστε την πλήρη διεύθυνση και τον αριθμό τηλεφώνου σας
Β) Ρύθμιση όλων των αναρτήσεων ως «δημόσιες»
Γ) Να ελέγχετε και να προσαρμόζετε τακτικά τις ρυθμίσεις απορρήτου
Δ) Χρήση του ίδιου κωδικού πρόσβασης για όλους τους λογαριασμούς

Περίληψη απαντήσεων

1	**Β**
2	**Γ**
3	**Β**
4	**Δ**
5	**C**
6	**Β**
7	**Β**
8	**C**
9	**A**
10	**C**

ΕΝΟΤΗΤΑ ΙΙ

Συνήθεις διαδικτυακές απάτες που στοχεύουν ηλικιωμένους

3. Ενότητα ΙΙ - Συνηθισμένες διαδικτυακές απάτες που στοχεύουν ηλικιωμένους

Αυτό το τετράωρο μάθημα βοηθά τους ηλικιωμένους να αναγνωρίζουν, να κατανοούν και να προστατεύονται από διαδικτυακές απάτες και απειλές για την ασφάλεια στον κυβερνοχώρο. Αντιμετωπίζει τις ιδιαίτερες ευπάθειές τους μέσω πρακτικών στρατηγικών και προληπτικών μέτρων, ενισχύοντας την αυτοπεποίθησή τους στην ασφαλή χρήση των ψηφιακών τεχνολογιών. Οι συμμετέχοντες θα μάθουν πώς λειτουργούν οι απάτες, θα αναγνωρίσουν τα προειδοποιητικά σημάδια στις ψηφιακές επικοινωνίες και θα κατανοήσουν τις τακτικές χειραγώγησης, όπως η κοινωνική μηχανική. Το μάθημα καλύπτει κοινές απάτες (phishing, smishing, vishing) και τεχνικές απειλές (κακόβουλο λογισμικό, ransomware, spyware), προσφέροντας στρατηγικές προστασίας. Επιπλέον, δίνει έμφαση στην ασφάλεια των προσωπικών δεδομένων, ενδυναμώνοντας τους ηλικιωμένους να αποθηκεύουν, να μοιράζονται και να δημιουργούν αντίγραφα ασφαλείας ευαίσθητων πληροφοριών με σιγουριά.

3.1 Μαθησιακοί στόχοι

Στόχος αυτού του μοδγλου είναι να βελτιώσει την κατανόηση των ηλικιωμένων σχετικά με τις συνήθεις διαδικτυακές απάτες, τις τακτικές που χρησιμοποιούν οι απατεώνες και τη σημασία της αναγνώρισης και αποφυγής των ψηφιακών απειλών. Να εξοπλίσει τους συμμετέχοντες με πρακτικές δεξιότητες και προληπτικά μέτρα για την προστασία τους από κινδύνους στον τομέα της ασφάλειας στον κυβερνοχώρο, όπως phishing, smishing, vishing και κακόβουλο λογισμικό. Να ενισχύσει την αυτοπεποίθηση και την ψηφιακή παιδεία των ηλικιωμένων, διδάσκοντάς τους πώς να προστατεύουν τα προσωπικά τους δεδομένα, να αναγνωρίζουν τις τακτικές χειραγώγησης και να χρησιμοποιούν με ασφάλεια τις ψηφιακές τεχνολογίες.

- Κατανόηση του τρόπου λειτουργίας των απάτων και αναγνώριση των ψυχολογικών και τεχνολογικών μεθόδων που χρησιμοποιούν οι απατεώνες.
- Αναγνώριση ύποπτου περιεχομένου και διάκριση μεταξύ νόμιμης και δόλιας επικοινωνίας.
- Απόκτηση γνώσεων σχετικά με τους συνηθισμένους τύπους απάτης και εκμάθηση στρατηγικών για την προστασία από τις απειλές στον κυβερνοχώρο.
- Οικοδόμηση εμπιστοσύνης στην προστασία των προσωπικών δεδομένων, τη δημιουργία αντιγράφων ασφαλείας και την ασφαλή πλοήγηση στα ψηφιακά εργαλεία.

3.2 Δομή, περιεχόμενο και μαθησιακά αποτελέσματα

Με την επιτυχή ολοκλήρωση αυτού του μοδγλου, οι μαθητές θα είναι σε θέση να:

- Αναγνωρίζουν κοινές τεχνικές, τεχνολογίες και στόχους που χρησιμοποιούνται στις απάτες και να εξηγούν πώς οι απατεώνες εξαπατούν τα θύματά τους.
- Αναγνωρίζουν προειδοποιητικά σημάδια σε ψηφιακό περιεχόμενο, όπως μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα SMS, ιστότοπους και διαφημίσεις, και να διακρίνουν μεταξύ νόμιμων και ύποπτων επικοινωνιών.
- Ορίζουν την κοινωνική μηχανική, να αναγνωρίζουν κοινές τακτικές που χρησιμοποιούν οι απατεώνες, να κατανοούν γιατί οι ηλικιωμένοι είναι συχνά στόχος και να εφαρμόζουν προληπτικά μέτρα για την προστασία από επιθέσεις κοινωνικής μηχανικής.

- Εξηγήσουν πώς οι απατεώνες εκμεταλλεύονται τα συναισθήματα και τα κοινά πρότυπα συμπεριφοράς των ηλικιωμένων και να εφαρμόσουν στρατηγικές για να παραμείνουν ψύχραιμοι και προσεκτικοί όταν βρίσκονται υπό συναισθηματική πίεση.
- Αναγνωρίστε τους πιο συνηθισμένους τύπους απάτης, όπως phishing, smishing, vishing και απάτες με πλαστή ταυτότητα ή οικονομικές απάτες, και περιγράψτε τις τεχνικές χειραγώγησης που χρησιμοποιούνται σε κάθε μία από αυτές.
- Προσδιορίστε διαφορετικούς τύπους κακόβουλου λογισμικού, όπως malware, ransomware, spyware, ιούς και trojans, περιγράψτε μεθόδους προστασίας από αυτά, αναγνωρίστε επικίνδυνα αναδυόμενα παράθυρα, κλείστε τα με ασφάλεια και χρησιμοποιήστε εργαλεία για να αποκλείσετε τα αναδυόμενα παράθυρα και να επαληθεύσετε την ασφάλεια των ιστότοπων.
- Ορίστε τα προσωπικά δεδομένα, προσδιορίστε ποιοι τύποι είναι πολύτιμοι για τους απατεώνες και πώς εκμεταλλεύονται, και εφαρμόστε βέλτιστες πρακτικές για την ασφαλή αποθήκευση και κοινή χρήση προσωπικών δεδομένων.
- Εξηγήστε τη σημασία της δημιουργίας αντιγράφων ασφαλείας των δεδομένων, εφαρμόστε συμβουλές για τη μείωση της ευπάθειας σε απώλεια δεδομένων και ενισχύστε την εμπιστοσύνη στην ασφαλή χρήση της τεχνολογίας.

3.3 Ατζέντα I Λεπτομερής σχέδιο συνεδρίας

ΕΝΌΤΗΤΑ II
Συνηθισμένες διαδικτυακές απάτες που στοχεύουν ηλικιωμένους

1η Συνεδρία

Καλωσόρισμα
Διάρκεια *5 λεπτά*

Μαθησιακοί στόχοι

- Εισαγωγή στο θέμα και δημιουργία ενός φιλόξενου περιβάλλοντος.

Περιεχόμενο/Μέθοδος

- Σύντομη εισαγωγή στη συνεδρία, περιγραφή των στόχων και καθορισμός των προσδοκιών
- Προετοιμάστε το έδαφος για την εκπαίδευση περιγράφοντας το μάθημα και τη σημασία του.

Υλικό

- Λευκός πίνακας ή flip chart για τους στόχους της συνεδρίας.
- Μαρκαδόροι.
- Εκτυπωμένη ατζέντα ή διαφάνεια παρουσίασης που περιγράφει τη συνεδρία.

[2η]συνεδρία

Δραστηριότητα για το σπάσιμο του πάγου: «Δύο αλήθειες και μια απάτη»
Διάρκεια *10 λεπτά*

Μαθησιακοί στόχοι

- Μετά την ολοκλήρωση αυτής της δραστηριότητας, οι μαθητές θα είναι σε θέση να διακρίνουν μεταξύ των σωστών πρακτικών ασφάλειας στο διαδίκτυο και των κοινών παρανοήσεων που χρησιμοποιούνται στις απάτες.

Περιεχόμενο/Μέθοδος

- Μια διαδραστική ομαδική άσκηση με τη μορφή ενός παιχνιδιού που ονομάζεται «Δύο αλήθειες και ένα ψέμα» με στόχο την παρουσίαση βασικών εννοιών που σχετίζονται με την απάτη και την ασφάλεια στο Διαδίκτυο. Οι συμμετέχοντες αναλύουν σύντομες δηλώσεις, τις συζητούν σε ζευγάρια ή μικρές ομάδες και προσδιορίζουν ποια είναι ψευδής (ψέμα ή μύθος). Ο εκπαιδευτής παρέχει γρήγορη ανατροφοδότηση και διευκρινίζει τυχόν αμφιβολίες.
- Ο συμμετέχων λαμβάνει μια κάρτα με τρεις δηλώσεις και πρέπει να αποφασίσει ποια από αυτές είναι απάτη. Στη συνέχεια, ο συμμετέχων συστηνεται και, αφού δώσει το όνομά του, πρέπει να διαβάσει τις δηλώσεις του και να πει ποια από αυτές θεωρεί απάτη. Όλοι οι άλλοι θα ακούσουν και θα δηλώσουν αν συμφωνούν ή διαφωνούν. Αν κάποιος διαφωνεί, σηκώνεται όρθιος και εξηγεί ποια δήλωση θεωρεί πραγματική απάτη. Στο τέλος, ο εκπαιδευτής ρωτά τους συμμετέχοντες αν κάποιος έχει συναντήσει ποτέ κάποια από αυτές τις απάτες ή έχει ακούσει για αυτές.

Υλικό

- Εκτυπωμένη ή ψηφιακή λίστα με σύνολα δηλώσεων (2 αλήθειες + 1 απάτη) – Παράρτημα 1, 2
- Στυλό και χαρτί (προαιρετικά, για σημειώσεις ή υποθέσεις της ομάδας)
- Λευκός πίνακας ή οθόνη (προαιρετικά, για την προβολή απαντήσεων και εξηγήσεων)

[3η] Συνεδρία

Διάλεξη 1: Αναγνώριση απάτης
Διάρκεια *30 λεπτά*

Μαθησιακοί στόχοι

- Βοηθήστε τους συμμετέχοντες να κατανοήσουν τους βασικούς μηχανισμούς των απάτων, τα κόλπα και τους στόχους των απατεώνων.

Περιεχόμενο/Μέθοδος

- Ο εκπαιδευτής χρησιμοποιεί διαφάνειες για να παρουσιάσει τις πιο συνηθισμένες απάτες που στοχεύουν τους ηλικιωμένους και εξηγεί τους στόχους και τους μηχανισμούς αυτών των απάτων. Τέλος, ο εκπαιδευτής ρωτά τους συμμετέχοντες ποιος μηχανισμός τους φοβίζει περισσότερο.

Υλικό

- Διαφάνειες παρουσίασης που καλύπτουν διάφορες πιθανές διαδικτυακές απάτες που στοχεύουν ηλικιωμένους.
- Ένας προβολέας και ένας φορητός υπολογιστής για την παρουσίαση.
- Φυλλάδια που συνοψίζουν τους διάφορους μηχανισμούς των απάτων και τα κόλπα που χρησιμοποιούνται για την επίτευξη των στόχων τους - Παράρτημα 3.

Δραστηριότητα 1: Αναγνώριση ύποπτου περιεχομένου
Διάρκεια *15 λεπτά*

Μαθησιακοί στόχοι

- Εξοικείωση των συμμετεχόντων με τα προειδοποιητικά σημάδια σε μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα SMS, ιστότοπους και διαφημίσεις.

Περιεχόμενο/Μέθοδος

- Στους συμμετέχοντες θα δείχνονται πραγματικά στιγμιότυπα οθόνης από πραγματικά μηνύματα SMS, ηλεκτρονικά μηνύματα, ιστότοπους και επικίνδυνα αναδυόμενα παράθυρα. Θα τους ζητηθεί να εντοπίσουν τις αποκλίσεις και να προσδιορίσουν ποια παραδείγματα είναι νόμιμα και ποια είναι απάτες. Μετά από κάθε απόφαση, θα ακολουθεί εξήγηση που θα διευκρινίζει γιατί κάτι είναι απάτη και γιατί κάτι άλλο δεν είναι.
- Ο εκπαιδευτής δείχνει δύο στιγμιότυπα οθόνης το ένα δίπλα στο άλλο και ζητά από την ομάδα να εντοπίσει τις διαφορές μεταξύ της απάτης και του γνήσιου παραδείγματος και να προσδιορίσει ποιο από τα δύο είναι απάτη. Ο εκπαιδευτής συνεχίζει με τον ίδιο τρόπο με όλα τα παραδείγματα, διατηρώντας τον τόνο ελαφρύ και ελκυστικό, ώστε να διατηρήσει την προσοχή και τη συμμετοχή της ομάδας. Ο εκπαιδευτής εξηγεί κάθε ζεύγος παραδειγμάτων αφού οι συμμετέχοντες έχουν μοιραστεί τις σκέψεις τους. Ρωτήστε τους ποιο ήταν το πιο δύσκολο παράδειγμα για να αναγνωρίσουν ως απάτη. Στη συνέχεια, ο εκπαιδευτής μοιράζει φυλλάδια.

Υλικό

- Διαφάνειες παρουσίασης με οπτικά παραδείγματα πραγματικών και ψεύτικων στιγμιότυπων οθόνης από μηνύματα SMS, ηλεκτρονικά μηνύματα, ιστότοπους και αναδυόμενα παράθυρα.
- Έναν προβολέα και έναν φορητό υπολογιστή για την παρουσίαση.
- Φύλλα εργασίας για τους συμμετέχοντες να σημειώσουν τις απαντήσεις ή να γράψουν σημειώσεις.
- Φυλλάδια με οδηγίες για την αναγνώριση των ψεύτικων παραδειγμάτων από τα πραγματικά - Παράρτημα 4.

Διάλειμμα | Διάρκεια *5 λεπτά*

- **Δώστε χρόνο στους συμμετέχοντες να αναζωογονηθούν και να σκεφτούν.**
- **Σύντομο διάλειμμα για ανανέωση.**

Διάλεξη 2: Κατανόηση της χειραγώγησης
Διάρκεια *30 λεπτά*

Μαθησιακοί στόχοι

- Να βοηθήσει τους συμμετέχοντες να κατανοήσουν την κοινωνική μηχανική.

Περιεχόμενο/Μέθοδος

- Ενημέρωση των συμμετεχόντων σχετικά με την κοινωνική μηχανική - Επισκόπηση των πιο συνηθισμένων τακτικών, των λόγων για τους οποίους οι απατεώνες στοχεύουν τους ηλικιωμένους και των τρόπων προστασίας από αυτού του είδους τις απάτες. Προσδιορισμός της κατάστασης με τέτοιο τρόπο ώστε, εάν κάποιος βρεθεί θύμα απάτης κοινωνικής μηχανικής, να παραμείνει ψύχραιμος και συγκεντρωμένος και να μην υποκύψει στην πίεση.
- Ο εκπαιδευτής παρουσιάζει παραδείγματα μηνυμάτων phishing και smishing που προκαλούν φόβο και αγωνία, ακολουθούμενα από τον τρόπο με τον οποίο συχνά προτείνουν μια εύκολη και γρήγορη λύση, όπως το να κάνετε κλικ σε έναν σύνδεσμο και να εισαγάγετε τα τραπεζικά σας στοιχεία ή προσωπικές πληροφορίες, ή ακόμα και να ακολουθήσετε μια σειρά εντολών ώστε «αυτοί» να μπορούν να λύσουν το πρόβλημα για εσάς. Ο εκπαιδευτής ρωτά τους συμμετέχοντες τι θα έκαναν σε περίπτωση επίθεσης κοινωνικής μηχανικής. Ο εκπαιδευτής μοιράζει έντυπο υλικό με πρόσθετες πληροφορίες σχετικά με τις τακτικές κοινωνικής μηχανικής και τον τρόπο αναγνώρισής τους.

Υλικό

- Διαφάνειες παρουσίασης που εξηγούν την κοινωνική μηχανική.
- Ένας προβολέας και ένας φορητός υπολογιστής για ζωντανές επιδείξεις των ρυθμίσεων απορρήτου.
- Εκτυπωμένα φυλλάδια με περιγραφή της κοινωνικής μηχανικής και οδηγίες για προειδοποιητικά σημάδια και προληπτικά μέτρα σε περίπτωση που κάποιος γίνει στόχος αυτού του είδους απάτης — Παράρτημα 5.

Δραστηριότητα 2: Κοινωνική μηχανική ζωντανά
Διάρκεια *20 λεπτά*

Μαθησιακοί στόχοι

- Να δοθεί στους συμμετέχοντες η ευκαιρία να βιώσουν διαφορετικές μεθόδους κοινωνικής μηχανικής σε ένα ασφαλές περιβάλλον.

Περιεχόμενο/Μέθοδος

- Στους συμμετέχοντες θα παρουσιαστούν διάφορα σενάρια, μερικά από τα οποία αποτελούν μορφές κοινωνικής μηχανικής και άλλα όχι. Τα σενάρια κοινωνικής μηχανικής θα στοχεύουν στα συναισθήματα και τις συμπεριφορές τους.
- Ο εκπαιδευτής ζητά από τους συμμετέχοντες να σχηματίσουν πέντε ομάδες των τριών ατόμων. Ο εκπαιδευτής μοιράζει τα φύλλα εργασίας και δίνει οδηγίες στις ομάδες. Η

αποστολή τους είναι να προσδιορίσουν ποια από αυτά είναι απάτες και ποια είναι γνήσια και να καταγράψουν τους λόγους πίσω από τα συμπεράσματά τους. Μόλις οι ομάδες εξετάσουν όλα τα σενάρια και λάβουν τις αποφάσεις τους, ο εκπαιδευτής ζητά να μοιραστούν τα ευρήματά τους με την ομάδα. Ο εκπαιδευτής συντονίζει τη συζήτηση σχετικά με τα σενάρια και ζητά από τους συμμετέχοντες να εξηγήσουν γιατί πιστεύουν ότι κάποια είναι γνήσια και άλλα είναι απάτες, ποιο σενάριο θα τους προκαλούσε τον μεγαλύτερο φόβο αν βρισκόντουσαν σε αυτό και γιατί.

Υλικό

- Εκτυπωμένα φυλλάδια με διαφορετικά σενάρια.
- Φύλλο εργασίας όπου οι συμμετέχοντες σημειώνουν ποια σενάρια είναι απάτη και ποια όχι – Παράρτημα 6.

Διάλειμμα | Διάρκεια *5 λεπτά*

- **Δώστε χρόνο για ξεκούραση και προετοιμασία για την επόμενη συνεδρία.**
- **Ένα σύντομο διάλειμμα για να αναζωογονηθούν.**

5η Συνεδρία

Διάλεξη 3: Οι πιο συνηθισμένοι τύποι απάτης
Διάρκεια *30 λεπτά*

Μαθησιακοί στόχοι

- Για να ανανεώσουμε τις απάτες που έχουν ήδη αναφερθεί, μια γρήγορη επισκόπηση των πιο συνηθισμένων απάτων, όπως smishing, vishing και phishing.
- Προσθήκη στις γνώσεις που έχουν ήδη δοθεί σε προηγούμενες διαλέξεις σχετικά με το κακόβουλο λογισμικό.

Περιεχόμενο/Μέθοδος

- Σύντομη επισκόπηση των πιο συνηθισμένων απάτων. Phishing, smishing, wishing, ψεύτικες ταυτότητες και απάτες με χρήματα. Επιπλέον, ενημέρωση των συμμετεχόντων σχετικά με το κακόβουλο λογισμικό, τι είναι και πώς να το εντοπίζουν.
- Ο εκπαιδευτής εξηγεί τις πιο σημαντικές πληροφορίες σχετικά με τις πιο συνηθισμένες απάτες και το κακόβουλο λογισμικό χρησιμοποιώντας διαφάνειες. Στη συνέχεια, μοιράζει υλικό που τις περιγράφει και το συζητά με τους συμμετέχοντες στην εκπαίδευση, για να βεβαιωθεί ότι όλοι κατανοούν τα πάντα όσο το δυνατόν πιο καθαρά. Τέλος, ρωτά τους συμμετέχοντες αν γνωρίζουν ποια σημάδια πρέπει να αναζητούν στο Διαδίκτυο.

Υλικό

- Διαφάνειες παρουσίασης με παραδείγματα απάτης phishing, vishing, smishing.
- Ένας προβολέας και ένας φορητός υπολογιστής για την προβολή παραδειγμάτων των πιο συνηθισμένων απάτων.
- Εκτυπωμένα φυλλάδια που περιγράφουν λεπτομερώς τις πιο συνηθισμένες απάτες και το κακόβουλο λογισμικό, τι είναι, πώς μπορεί να βλάψει το θύμα και πώς να το αναγνωρίσετε - Παράρτημα 7.

Δραστηριότητα 3: Εντοπίστε το κακόβουλο λογισμικό
Διάρκεια *20 λεπτά*

Μαθησιακοί στόχοι

- Ανάπτυξη της ικανότητας αναγνώρισης διαφορετικών τύπων κακόβουλου λογισμικού.

Περιεχόμενο/Μέθοδος

- Ομαδική δραστηριότητα όπου οι συμμετέχοντες αναγνωρίζουν και συζητούν διαφορετικούς τύπους κακόβουλου λογισμικού μέσω φυλλαδίων.
- Ο εκπαιδευτής εξηγεί ότι οι συμμετέχοντες θα δοκιμάσουν τις γνώσεις τους σχετικά με το κακόβουλο λογισμικό σε ομάδες των τριών. Ο εκπαιδευτής μοιράζει τα σενάρια και ζητά από τους συμμετέχοντες να τα διαβάσουν. Ο στόχος των συμμετεχόντων είναι να προσδιορίσουν τον τύπο του λογισμικού που χρησιμοποιήθηκε (Trojan, ιός, adware, ransomware ή spyware) και να απαντήσουν στις ερωτήσεις που ακολουθούν κάθε σενάριο. Κάθε ομάδα μοιράζεται τις απαντήσεις της με τις άλλες ομάδες. Στη συνέχεια, ο εκπαιδευτής μοιράζει φύλλα απαντήσεων και ζητά από τους συμμετέχοντες να εξετάσουν τις απαντήσεις και να αναλύσουν τα βασικά στοιχεία για την αναγνώριση του λογισμικού που χρησιμοποιήθηκε και τους τρόπους προστασίας από μια τέτοια επίθεση. Τέλος, ο εκπαιδευτής ρωτά ποιος τύπος λογισμικού θεωρούν ότι είναι ο πιο επιβλαβής και ποιος ο λιγότερο επιβλαβής.

Υλικό

- Φυλλάδια με περιγραφές κακόβουλου λογισμικού.
- Φύλλα εργασίας για τους συμμετέχοντες, ώστε να γράψουν ποιο είναι το λογισμικό για το συγκεκριμένο παράδειγμα, τι κάνει στη συσκευή και ποια είναι τα προληπτικά μέτρα για το συγκεκριμένο παράδειγμα.
- Φυλλάδιο για τους συμμετέχοντες – Εντοπίστε το κακόβουλο λογισμικό - Παράρτημα 8

Διάλειμμα | Διάρκεια 5’

- **Δώστε χρόνο για ξεκούραση και προετοιμασία.**
- **Σύντομο διάλειμμα για ανανέωση.**

6η Συνεδρία

Διάλεξη 4: Βασική προστασία δεδομένων και δημιουργία αντιγράφων ασφαλείας δεδομένων
Διάρκεια *30 λεπτά*

Μαθησιακοί στόχοι

- Οι συμμετέχοντες θα είναι σε θέση να ορίσουν τα προσωπικά δεδομένα και ποια δεδομένα είναι πολύτιμα για τους απατεώνες. Θα συνειδητοποιήσουν επίσης τη σημασία της δημιουργίας αντιγράφων ασφαλείας των δεδομένων.

Περιεχόμενο/Μέθοδος

- Παρουσίαση με διευκρινίσεις σχετικά με τα προσωπικά δεδομένα. Οι συμμετέχοντες θα ενημερωθούν σχετικά με το πού είναι ασφαλές να μοιράζονται δεδομένα και πού όχι, θα ενημερωθούν για τη σημασία του να αναγνωρίζουν τα δεδομένα που μπορούν να χρησιμοποιηθούν εναντίον τους. Οι συμμετέχοντες θα ενημερωθούν επίσης για το ποια δεδομένα πρέπει να δημιουργούνται αντίγραφα ασφαλείας και γιατί.
- Ο εκπαιδευτής μοιράζει έντυπο υλικό και καθοδηγεί τους μαθητές στο περιεχόμενο χρησιμοποιώντας διαφάνειες, εξηγώντας: τις κατηγορίες προσωπικών πληροφοριών, ποια δεδομένα μπορούν να είναι επιβλαβή αν πέσουν σε λάθος χέρια και γιατί, πού μπορούμε να μοιραζόμαστε προσωπικά δεδομένα στο διαδίκτυο, τι δεν πρέπει ποτέ να μοιραζόμαστε στο διαδίκτυο, τι είναι η δημιουργία αντιγράφων ασφαλείας, πώς τα αντίγραφα ασφαλείας μπορούν να σας προστατεύσουν από επιθέσεις κακόβουλου λογισμικού, βέλτιστες πρακτικές για ασφαλή αντίγραφα ασφαλείας και συμβουλές για να διατηρήσετε τα δεδομένα σας ασφαλή.
- Ο εκπαιδευτής ενθαρρύνει τη συζήτηση και ρωτά τους συμμετέχοντες αν έχουν ποτέ γίνει μάρτυρες απόπειρας κυβερνοεπίθεσης με χρήση λογισμικού ή αν έχουν συμμετάσχει σε τέτοια επίθεση. Τέλος, ο εκπαιδευτής ρωτά αν θα δημιουργήσουν αντίγραφα ασφαλείας των σημαντικών δεδομένων τους.

Υλικό

- Παρουσίαση σχετικά με τα προσωπικά δεδομένα, πού και τι μπορούμε να μοιραζόμαστε στο διαδίκτυο, σε συνδυασμό με τις απαραίτητες πληροφορίες σχετικά με τη δημιουργία αντιγράφων ασφαλείας των δεδομένων.
- Φυλλάδια με τις οδηγίες σχετικά με τα προσωπικά δεδομένα, πού να τα μοιραζόμαστε και πού όχι, και γιατί είναι σημαντικό να δημιουργούμε αντίγραφα ασφαλείας των σημαντικών πληροφοριών - Παράρτημα 9.

Δραστηριότητα 4: Δημιουργία αντιγράφων ασφαλείας αρχείων σε υπηρεσία cloud και εξωτερική μνήμη αποθήκευσης.
Διάρκεια *20 λεπτά*

Μαθησιακοί στόχοι

- Αυτές οι γνώσεις θα βοηθήσουν τους συμμετέχοντες να δημιουργούν αντίγραφα ασφαλείας των αρχείων τους με ασφάλεια, χρησιμοποιώντας επαληθευμένες υπηρεσίες cloud και εξωτερικούς σκληρούς δίσκους.

Περιεχόμενο/Μέθοδος

- Οι συμμετέχοντες θα δημιουργήσουν αντίγραφα ασφαλείας εικονικών αρχείων σε μια υπηρεσία cloud με την οποία είναι εξοικειωμένοι (Google Drive, Dropbox, iCloud, OneDrive). Θα δημιουργήσουν επίσης αντίγραφα ασφαλείας των ίδιων εικονικών αρχείων σε μια μονάδα USB.
- Ο εκπαιδευτής διανέμει υλικό που περιέχει πληροφορίες σχετικά με τη δημιουργία αντιγράφων ασφαλείας αρχείων σε εξωτερικό δίσκο και σε υπηρεσία cloud. Ο εκπαιδευτής κάνει επίδειξη σε οθόνη ή προβολέα και οι συμμετέχοντες ακολουθούν τη διαδικασία

αντιγραφής αρχείων από έναν υπολογιστή σε εξωτερικό δίσκο και μεταφόρτωσης αρχείων σε υπηρεσία cloud. Ο εκπαιδευτής βοηθά όσους χρειάζονται βοήθεια. Ερώτηση για προβληματισμό στο τέλος: «Πιστεύετε ότι μπορείτε να δημιουργήσετε αντίγραφα ασφαλείας των αρχείων σας μόνοι σας ή χρειάζεται κάποιος επιπλέον πληροφορίες;», «Υπάρχει κάτι που θα θέλατε να ρωτήσετε ή να μοιραστείτε τη γνώμη σας σχετικά με το σημερινό θέμα της διαδικτυακής απάτης;»

Υλικό

- Ψεύτικα αρχεία για να δημιουργηθεί αντίγραφο ασφαλείας.
- Υπολογιστές και μονάδες USB.
- Φορητός υπολογιστής και προβολέας, ώστε ο εκπαιδευτής να μπορεί να δείξει ένα παράδειγμα της διαδικασίας.
- Φυλλάδια με οδηγίες για τη δημιουργία αντιγράφων ασφαλείας αρχείων σε εξωτερικό δίσκο και σε υπηρεσία cloud - οδηγίες προσαρμοσμένες για όλους τους μεγάλους παρόχους cloud - Πώς να δημιουργήσετε αντίγραφα ασφαλείας των αρχείων σας - Παράρτημα 10

7η Συνεδρία

Συζήτηση | Διάρκεια *10* λεπτά

Μαθησιακοί στόχοι

- Ενθάρρυνση μιας προληπτικής νοοτροπίας γεμάτης συνειδητοποίηση όσον αφορά τις διαδικτυακές απάτες.
- Συνοψίστε την εκπαίδευση και βεβαιωθείτε ότι οι συμμετέχοντες κατανοούν πώς να προστατεύονται από τις διαδικτυακές απάτες.

Περιεχόμενο/Μέθοδος

- Εξετάστε τα βασικά σημεία των πιο συνηθισμένων διαδικτυακών απάτων. Ενισχύστε την ευαισθητοποίηση ότι, αν κάτι επικοινωνείται με εξαιρετικά επείγοντα τρόπο, πρέπει πάντα να είστε προσεκτικοί για πιθανή απάτη.
- Ομαδική συζήτηση σχετικά με τον τρόπο αντιμετώπισης μιας κατάστασης στην οποία μπορεί να βρεθεί κανείς σε μια διαδικτυακή απάτη. Ποια είναι τα βασικά σημάδια που προδίδουν κάποιες ύποπτες δραστηριότητες που μπορεί να συναντήσουμε και τι πρέπει να κάνουμε σε τέτοιου είδους σενάρια.
- Ο εκπαιδευτής συνοψίζει τις πιο σημαντικές πληροφορίες σχετικά με το τι πρέπει να κάνετε εάν πέσετε θύμα διαδικτυακής απάτης και παραθέτει τα βασικά σημάδια ύποπτης δραστηριότητας. Ο εκπαιδευτής ευχαριστεί τους συμμετέχοντες και παρέχει υποστηρικτικό υλικό, στη συνέχεια διανέμει έναν κατάλογο ελέγχου σχετικά με τον τρόπο αναγνώρισης της διαδικτυακής απάτης και τι πρέπει να κάνετε σε αυτή την περίπτωση. Ο εκπαιδευτής θέτει στους συμμετέχοντες ανοιχτές ερωτήσεις: «Ποιο είναι το πιο σημαντικό πράγμα που μάθατε σήμερα σχετικά με την ηλεκτρονική απάτη και πώς να προστατευτείτε από αυτήν;» «Αισθάνεστε πιο σίγουροι τώρα για το πώς να αναγνωρίζετε και να αποφεύγετε τις απάτες;» «Υπάρχει κάποιο θέμα ή ερώτηση από τη σημερινή συνεδρία για το οποίο θα θέλατε περισσότερες πληροφορίες;»

Υλικό

- ❖ Λευκός πίνακας και μαρκαδόροι για να σκεφτούν τρόπους αναγνώρισης των απάτων.
- ❖ Φυλλάδιο: λίστα ελέγχου σχετικά με τις διαδικτυακές απάτες - Παράρτημα 11. Φυλλάδια Λίστα ελέγχου για την ασφάλεια στο διαδίκτυο.

Σύνοψη
Διάρκεια 5

Μαθησιακοί στόχοι

- ❖ Συνοψίστε τη συνεδρία και ενθαρρύνετε τους συμμετέχοντες να συνεχίσουν να ασκούνται με ασφάλεια.

Περιεχόμενο/Μέθοδος

- ❖ Τελική ανακεφαλαίωση των βασικών σημείων, παροχή πρόσθετων πόρων για μελλοντική μάθηση.

Υλικό

- ❖ Φυλλάδια με τα βασικά σημεία και τους πόρους.

3.4 Πρόσθετες πληροφορίες

3.4.1 Αυτοανασκόπηση των εκπαιδευτών

- ➢ Μεταβίβασα αποτελεσματικά τη σημασία των κινδύνων που ενέχει το διαδίκτυο;
- ➢ Διασφάλισα ότι οι συμμετέχοντες κατανόησαν τα προληπτικά μέτρα;
- ➢ Πώς ενέπλεξα τους συμμετέχοντες στις δραστηριότητες και τις συζητήσεις;
- ➢ Ήταν οι πόροι και τα υλικά χρήσιμα για τους συμμετέχοντες;

3.4.2 Αξιολόγηση του προγράμματος από τους εκπαιδευτές

- ➢ Είναι το περιεχόμενο της εκπαίδευσης σχετικό και σαφές για τους ηλικιωμένους;
- ➢ Ήταν οι δραστηριότητες και οι συζητήσεις αποτελεσματικές στο να βοηθήσουν τους συμμετέχοντες να μάθουν το υλικό;
- ➢ Τα αποτελέσματα συνάδουν με τους μαθησιακούς στόχους του προγράμματος;

3.4.3 Υλικό, πρόσθετοι πόροι

Παράρτημα 1 | Δύο αλήθειες και μια απάτη

Σετ 1

Οι απατεώνες συχνά προσποιούνται ότι είναι

Οι νόμιμες εταιρείες δεν θα σας στείλουν ποτέ email.

Τα ηλεκτρονικά μηνύματα phishing συχνά δημιουργούν

Σύνολο 2

Ποτέ δεν πρέπει να μοιράζεστε τον τραπεζικό σας PIN με

Όλοι οι ιστότοποι που ξεκινούν με «https» είναι 100% ασφαλείς.

Οι απατεώνες μπορεί να χρησιμοποιούν λογότυπα που

Σετ 3

Το ransomware μπορεί να σας αποκλείσει από τον υπολογιστή

Κάνοντας κλικ σε άγνωστα αναδυόμενα παράθυρα μπορεί

Είναι ασφαλές να ανοίγετε συνημμένα από φίλους χωρίς

Σετ 4

Η κοινωνική μηχανική συχνά περιλαμβάνει συναισθηματική

Οι κυβερνητικές υπηρεσίες επικοινωνούν πάντα πρώτα μαζί

Οι ηλικιωμένοι είναι συχνά στόχος λόγω της αντιληπτής

Σετ 5

Είναι εντάξει να χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης για

Ένας ισχυρός κωδικός πρόσβασης περιλαμβάνει

Η χρήση της επαλήθευσης δύο παραγόντων προσθέτει

Σετ 6

Οι απατεώνες μπορούν να πλαστογραφήσουν την

Είναι ασφαλές να δώσετε την πλήρη διεύθυνσή σας σε ένα

Να είστε πάντα προσεκτικοί με τις ανεπιθύμητες προσφορές.

Σετ 7

- Το smishing είναι μια απάτη που αποστέλλεται μέσω μηνύματος
- Το κακόβουλο λογισμικό επηρεάζει μόνο παλιούς
- Το λογισμικό προστασίας από ιούς βοηθά στην προστασία

Σετ 8

- Οι απατεώνες μπορεί να προσποιούνται ότι είναι τεχνική
- Πρέπει να κάνετε κλικ σε άγνωστους συνδέσμους για να
- Πάντα να ελέγχετε τις διευθύνσεις URL πριν

Σετ 9

- Οι ψεύτικες προσφορές εργασίας μπορούν να
- Οι απάτες συμβαίνουν μόνο σε άτομα που δεν είναι
- Οι διαδικτυακές διαφημίσεις μπορεί μερικές φορές να

Σετ 10

- Ορισμένες απάτες ζητούν δωροκάρτες ως πληρωμή.
- Είναι ασφαλές να κατεβάζετε εφαρμογές από αξιόπιστα
- Πρέπει να μοιράζεστε τα στοιχεία σύνδεσής σας με

Σετ 11

- Οι απατεώνες μερικές φορές χρησιμοποιούν τον φόβο για να
- Κάθε αναδυόμενη προειδοποίηση είναι μια
- Είναι σημαντικό να επαληθεύετε τα μηνύματα πριν

Σετ 12

- Οι νόμιμες εταιρείες δεν ζητούν προσωπικά στοιχεία μέσω
- Τα δημόσια δίκτυα Wi-Fi είναι πάντα ασφαλή και μπορούν να
- Η ενημέρωση της συσκευής σας βοηθά στην επιδιόρθωση των

Σετ 13

Οι απάτες μπορούν να συμβούν στις πλατφόρμες

Το να κάνετε κλικ στο «κατάργηση εγγραφής» σε ένα

Πρέπει να αναφέρετε ύποπτες δραστηριότητες στην

Σετ 14

Δεν υπάρχει πρόβλημα να δημοσιεύετε τα ταξιδιωτικά σας

Οι απατεώνες μπορούν να παρακολουθούν τις αναρτήσεις

Να είστε προσεκτικοί με αιτήματα φιλίας από

Σετ 15

Τα αντίγραφα ασφαλείας προστατεύουν τα δεδομένα σας

Πρέπει να αγνοείτε τις υπενθυμίσεις για ενημέρωση

Χρησιμοποιήστε ισχυρούς, μοναδικούς κωδικούς

Παράρτημα 2 | Σωστές απαντήσεις

Σύνολο 1

- Σωστό – Οι απατεώνες συχνά προσποιούνται ότι είναι κάποιος που εμπιστεύεστε.
- Λάθος – Οι νόμιμες εταιρείες δεν θα σας στείλουν ποτέ email. (Αυτό είναι μύθος. Οι νόμιμες εταιρείες μπορεί να επικοινωνούν με τους χρήστες μέσω email, αλλά δεν ζητούν ευαίσθητες προσωπικές ή οικονομικές πληροφορίες.)
- Σωστό – Τα ηλεκτρονικά μηνύματα phishing συχνά δημιουργούν μια αίσθηση επείγοντος.

Σύνολο 2

- Σωστό – Δεν πρέπει ποτέ να μοιράζεστε τον τραπεζικό σας PIN με κανέναν.
- Ψευδές – Όλοι οι ιστότοποι που ξεκινούν με «https» είναι απολύτως ασφαλείς. (Αυτό είναι μύθος. Το «https» υποδηλώνει κρυπτογράφηση, όχι νομιμότητα.)
- Σωστό – Οι απατεώνες μπορεί να χρησιμοποιούν λογότυπα που μοιάζουν με επίσημα για να εξαπατήσουν τους χρήστες.

Σύνολο 3

- Σωστό – Το ransomware μπορεί να κλειδώσει τους χρήστες έξω από τους υπολογιστές τους.
- Σωστό – Κάνοντας κλικ σε άγνωστα αναδυόμενα παράθυρα μπορεί να εγκατασταθεί κακόβουλο λογισμικό.
- Λάθος – Είναι ασφαλές να ανοίγετε συνημμένα από φίλους χωρίς να τα ελέγχετε. (Αυτό είναι μύθος. Τα συνημμένα από αξιόπιστους επαφές μπορεί επίσης να είναι μολυσμένα.)

Σύνολο 4

- Σωστό – Η κοινωνική μηχανική συχνά βασίζεται στην συναισθηματική χειραγώγηση.
- Ψευδές – Οι κυβερνητικές υπηρεσίες επικοινωνούν πάντα πρώτα με τα άτομα μέσω τηλεφώνου. (Αυτό είναι μύθος. Η επίσημη επικοινωνία πραγματοποιείται συχνά μέσω ταχυδρομείου.)
- Σωστό – Οι ηλικιωμένοι είναι συχνά στόχος λόγω της αντιληπτής ευπάθειας τους.

Σύνολο 5

- Λάθος – Είναι αποδεκτό να επαναχρησιμοποιείτε τον ίδιο κωδικό πρόσβασης για πολλούς λογαριασμούς. (Αυτό είναι μύθος. Η επαναχρησιμοποίηση κωδικών πρόσβασης αυξάνει τους κινδύνους ασφαλείας.)
- Σωστό – Οι ισχυροί κωδικοί πρόσβασης περιλαμβάνουν συνδυασμό γραμμάτων, αριθμών και συμβόλων.
- Σωστό – Η επαλήθευση δύο παραγόντων παρέχει ένα επιπλέον επίπεδο ασφάλειας.

Σύνολο 6

- Σωστό – Οι απατεώνες μπορούν να παραποιήσουν τις πληροφορίες αναγνώρισης καλούντος.
- Λάθος – Είναι ασφαλές να μοιράζεστε την πλήρη διεύθυνσή σας σε διαδικτυακούς διαγωνισμούς. (Αυτό είναι μύθος. Οι προσωπικές πληροφορίες μπορούν να χρησιμοποιηθούν καταχρηστικά για απάτες.)
- Αληθές – Οι αυτόκλητες προσφορές πρέπει πάντα να αντιμετωπίζονται με προσοχή.

Σετ 7

- Σωστό – Το smishing αναφέρεται σε απάτες που αποστέλλονται μέσω μηνυμάτων κειμένου.
- Λάθος – Το κακόβουλο λογισμικό επηρεάζει μόνο παλιούς υπολογιστές. (Αυτό είναι μύθος. Οποιαδήποτε συσκευή μπορεί να επηρεαστεί.)
- Σωστό – Το λογισμικό προστασίας από ιούς βοηθά στην προστασία από κακόβουλες απειλές.

Σύνολο 8

- Σωστό – Οι απατεώνες μπορεί να προσποιούνται ότι είναι υπηρεσίες τεχνικής υποστήριξης.
- Λάθος – Πρέπει να κάνετε κλικ σε άγνωστους συνδέσμους για να ελέγξετε αν είναι νόμιμοι. (Αυτό είναι μύθος. Το να κάνετε κλικ σε άγνωστους συνδέσμους μπορεί να είναι επικίνδυνο.)
- Σωστό – Πρέπει πάντα να ελέγχονται οι διευθύνσεις URL πριν από την εισαγωγή προσωπικών πληροφοριών.

Σύνολο 9

- Σωστό – Οι ψεύτικες προσφορές εργασίας μπορούν να χρησιμοποιηθούν για την κλοπή προσωπικών στοιχείων.
- Ψευδές – Οι απάτες στοχεύουν μόνο άτομα με χαμηλές ψηφιακές δεξιότητες. (Αυτό είναι μύθος. Οποιοσδήποτε μπορεί να γίνει στόχος.)
- Σωστό – Οι διαδικτυακές διαφημίσεις μπορεί μερικές φορές να ανακατευθύνουν τους χρήστες σε ιστότοπους απάτης.

Σύνολο 10

- Σωστό – Ορισμένες απάτες ζητούν πληρωμή με δωροκάρτες.
- Σωστό – Η λήψη εφαρμογών από αξιόπιστα καταστήματα εφαρμογών είναι γενικά ασφαλέστερη.
- Λάθος – Τα στοιχεία σύνδεσης πρέπει να μοιράζονται με στενούς φίλους. (Αυτό είναι μύθος. Τα στοιχεία σύνδεσης δεν πρέπει ποτέ να μοιράζονται.)

Σύνολο 11

- Σωστό – Οι απατεώνες χρησιμοποιούν συχνά τον φόβο για να ασκήσουν πίεση στα θύματά τους.
- Ψευδές – Κάθε αναδυόμενη προειδοποίηση υποδηλώνει μια πραγματική απειλή από ιό. (Αυτό είναι μύθος. Πολλές προειδοποιήσεις είναι ψεύτικες.)
- Σωστό – Τα μηνύματα πρέπει πάντα να επαληθεύονται πριν από την ανάληψη δράσης.

Σύνολο 12

- Σωστό – Οι νόμιμες εταιρείες δεν ζητούν προσωπικά στοιχεία μέσω email.
- Ψευδές – Τα δημόσια δίκτυα Wi-Fi είναι πάντα ασφαλή. (Αυτό είναι μύθος. Τα δημόσια δίκτυα μπορούν να εκθέσουν προσωπικά δεδομένα.)
- Σωστό – Οι τακτικές ενημερώσεις λογισμικού βοηθούν στην επιδιόρθωση των τρωτών σημείων ασφαλείας.

Σύνολο 13

- Σωστό – Οι απάτες μπορούν να συμβούν σε πλατφόρμες κοινωνικών μέσων.
- Ψευδές – Το κλικ στο «κατάργηση εγγραφής» σε ηλεκτρονικά μηνύματα απάτης είναι ακίνδυνο. (Αυτό είναι μύθος. Μπορεί να επιβεβαιώσει τον χρήστη ως ενεργό στόχο.)
- Σωστό – Οι ύποπτες δραστηριότητες πρέπει να αναφέρονται στην αντίστοιχη πλατφόρμα.

Σύνολο 14

- Λάθος – Είναι ασφαλές να μοιράζεστε δημόσια τα ταξιδιωτικά σας σχέδια στο διαδίκτυο. (Αυτό είναι μύθος. Τέτοιες πληροφορίες μπορούν να αξιοποιηθούν από απατεώνες.)
- Σωστό – Οι απατεώνες ενδέχεται να παρακολουθούν τη δραστηριότητα στα μέσα κοινωνικής δικτύωσης.
- Σωστό – Οι αιτήσεις φιλίας από άγνωστα άτομα πρέπει να αντιμετωπίζονται με προσοχή.

Σύνολο 15

- Σωστό – Τα αντίγραφα ασφαλείας των δεδομένων προστατεύουν τις πληροφορίες σε περίπτωση κυβερνοεπιθέσεων.
- Λάθος – Οι υπενθυμίσεις για ενημέρωση λογισμικού πρέπει να αγνοούνται. (Αυτό είναι μύθος. Οι ενημερώσεις είναι κρίσιμες για την ασφάλεια.)
- Σωστό – Πρέπει να χρησιμοποιούνται ισχυροί και μοναδικοί κωδικοί πρόσβασης για κάθε λογαριασμό.

Παράρτημα 3 | Μηχανισμοί που χρησιμοποιούνται σε διαδικτυακές απάτες που στοχεύουν ηλικιωμένους

1. Phishing (απάτες μέσω email)

Οι ηλικιωμένοι λαμβάνουν email που φαίνεται να προέρχονται από αξιόπιστες πηγές (τράπεζες, υπηρεσίες υγείας κ.λπ.).

Τέχνασμα: Ψεύτικοι σύνδεσμοι ή σελίδες σύνδεσης

Στόχος: Κλοπή προσωπικών ή οικονομικών πληροφοριών

2. Smishing (απάτες μέσω SMS)

Οι απατεώνες στέλνουν μηνύματα SMS με ψεύτικες ειδοποιήσεις παράδοσης, ειδοποιήσεις για κέρδη ή προειδοποιήσεις.

Τέχνασμα: Επείγουσα γλώσσα + σύνδεσμος προς κακόβουλο ιστότοπο

Στόχος: Εγκατάσταση κακόβουλου λογισμικού ή συλλογή προσωπικών δεδομένων

3. Vishing (απάτες μέσω φωνητικών κλήσεων)

Τηλεφωνικές κλήσεις από απατεώνες που προσποιούνται ότι είναι από τράπεζα, τεχνική υποστήριξη ή την κυβέρνηση.

Τέχνασμα: Ψεύτικη ταυτότητα καλούντος + συναισθηματική πίεση

Στόχος: Απόκτηση τραπεζικών στοιχείων ή απομακρυσμένης πρόσβασης

4. Ψεύτικες ιστοσελίδες (Spoofing)

Οι ηλικιωμένοι κατευθύνονται σε ψεύτικους ιστότοπους που μοιάζουν με πραγματικούς (τράπεζες, καταστήματα, ιατρικά portals).

Τέχνασμα: Ελαφρώς τροποποιημένες διευθύνσεις URL (π.χ. paypa1.com)

Στόχος: Λήψη στοιχείων σύνδεσης ή πληρωμής

5. Απάτες τεχνικής υποστήριξης (απάτες μέσω email)

Αναδυόμενα παράθυρα ή τηλεφωνήματα προειδοποιούν για «ιό» ή πρόβλημα στον υπολογιστή, προτρέποντας τους ηλικιωμένους να ζητήσουν βοήθεια.

Τέχνασμα: Ψεύτικα μηνύματα σφάλματος + αιτήματα για απομακρυσμένη πρόσβαση

Στόχος: Έλεγχος της συσκευής ή κλοπή δεδομένων πιστωτικής κάρτας

6. Απάτες με ρομαντικές σχέσεις

Στα μέσα κοινωνικής δικτύωσης ή σε ιστότοπους γνωριμιών, οι απατεώνες δημιουργούν συναισθηματικούς δεσμούς για να χειραγωγήσουν τα θύματα.

Τέχνασμα: Ψεύτικες φωτογραφίες, ιστορίες και αγάπη

Στόχος: Να πείσουν τους ηλικιωμένους να στείλουν χρήματα

7. Απάτες επενδύσεων ή λαχειοφόρων αγορών

Υποσχέσεις για τεράστια κέρδη ή μηνύματα του τύπου «κερδίσατε» που απαιτούν προκαταβολή.

Τέχνασμα: Ψεύτικα έγγραφα, επείγοντα ή επίσημα ονόματα

Στόχος: Λήψη τραπεζικών εμβασμάτων, κρυπτονομισμάτων ή δωροκαρτών

Παράρτημα 4 | Εντοπίστε την απάτη: Γρήγορες οδηγίες

Χρησιμοποιήστε αυτήν τη λίστα ελέγχου για να αποφασίσετε αν ένα μήνυμα, ένα email, ένας ιστότοπος ή μια διαφήμιση είναι πραγματικά ή ψεύτικα.

1. Ελέγξτε τον αποστολέα ή την πηγή

- *Διεύθυνση email / αριθμός τηλεφώνου: Οι πληροφορίες του αποστολέα φαίνονται ύποπτες ή άγνωστες;*

✗ ***Ψεύτικο:*** *support@paypal-secure123.com*
✓ ***Αληθινό:*** *support@paypal.com*

- *Λάθος ορθογραφία ονομάτων εμπορικών σημάτων ή παράξενες διευθύνσεις URL:*

✗ *netfflix-billing.com*
✓ *netflix.com*

2. Αναζητήστε σημάδια επείγοντος ή πίεσης

- Το μήνυμα προσπαθεί να σας τρομάξει ή να σας πιέσει;

  «Δράστε τώρα, αλλιώς ο λογαριασμός σας θα κλειδωθεί!»
  «Τελευταία προειδοποίηση πριν από νομική δράση!»

Οι πραγματικές εταιρείες δεν σας απειλούν ή σας πιέζουν με αυτόν τον τρόπο

3. Εξετάστε τη γλώσσα και τον τόνο

- Ψάξτε για ορθογραφικά και γραμματικά λάθη
- Είναι ο τόνος πολύ ανεπίσημος ή πολύ επιθετικός;
- Ακούγεται αφύσικο ή μεταφρασμένο;
  ✗**Ψεύτικο:** «Αγαπητέ πελάτη, ο λογαριασμός σας έχει αποκλειστεί επειγόντως, παρακαλούμε να ενεργήσετε άμεσα».
  ✔ **Αληθινό:** «Παρατηρήσαμε ασυνήθιστη δραστηριότητα στον λογαριασμό σας. Παρακαλούμε ελέγξτε τον.»

4. Ελέγξτε τον σύνδεσμο πριν κάνετε κλικ

- Τοποθετήστε τον κέρσορα πάνω από τους συνδέσμους για να δείτε πού οδηγούν πραγματικά

- Η διεύθυνση URL ταιριάζει με την πραγματική ιστοσελίδα της εταιρείας;
  ✗ **Ψεύτικο:** http://paypal.verify-now-support.com
  ✓ **Αληθινό:** https://www.paypal.com

5. Προσέξτε τα αιτήματα για προσωπικά στοιχεία

Οι πραγματικές εταιρείες δεν ζητούν ποτέ:

- Κωδικούς πρόσβασης
- Κωδικούς PIN
- Αριθμούς τραπεζικών λογαριασμών ή καρτών
- Αριθμούς κοινωνικής ασφάλισης
  ✗ «Παρακαλώ στείλτε τα στοιχεία σύνδεσής σας για να επαληθεύσουμε τον λογαριασμό σας.»
  ✓ «Δεν θα σας ζητήσουμε ποτέ τον κωδικό πρόσβασής σας μέσω email.»

6. Ελέγξτε τα λογότυπα και το σχεδιασμό

- Τα λογότυπα είναι θολά, παραμορφωμένα ή έχουν αλλοιωμένα χρώματα;
- Η διάταξη είναι περίεργη ή ασυνεπής;

Οι πραγματικές εταιρείες χρησιμοποιούν καθαρό, επαγγελματικό και συνεπή σχεδιασμό.

7. Πολύ καλό για να είναι αληθινό; Πιθανότατα είναι.

«Κερδίσατε ένα νέο iPhone!»

«Έχετε επιλεγεί για μια δωροκάρτα αξίας 1.000 δολαρίων!»

Τα πραγματικά έπαθλα δεν απαιτούν προκαταβολή ή ευαίσθητες πληροφορίες.

✔ **Αληθινό ή ✗ Ψεύτικο;**

Ρωτήστε τον εαυτό σας:

- **Εμπιστεύομαι την πηγή;**
- **Με πιέζουν ή με φοβίζουν για να δράσω;**
- **Υπάρχει κάτι που μου φαίνεται παράξενο ή ασυνήθιστο;**

Σε περίπτωση αμφιβολίας, μην κάνετε κλικ, μην απαντήσετε και αναφέρετε το!

Παράρτημα 5 | Απάτες κοινωνικής μηχανικής – Τι πρέπει να γνωρίζετε

Τι είναι η κοινωνική μηχανική;

Κοινωνική μηχανική είναι όταν οι απατεώνες χρησιμοποιούν χειραγώγηση, πίεση και συναισθήματα για να σας ξεγελάσουν και να σας κάνουν να αποκαλύψετε προσωπικές πληροφορίες, χρήματα ή πρόσβαση στους λογαριασμούς σας.

Κίνδυνοι της κοινωνικής μηχανικής

Οι απατεώνες μπορεί να προσποιούνται ότι προέρχονται από αξιόπιστες πηγές, όπως:

- Τράπεζες (π.χ. «Ο λογαριασμός σας έχει κλειδωθεί!»)
- Υπηρεσίες ταχυμεταφορών (π.χ. «Έχετε χάσει ένα δέμα. Πληρώστε τώρα!»)
- Κυβερνητικές υπηρεσίες (π.χ. «Έχετε απλήρωτους φόρους.»)
- Η αστυνομία ή το Υπουργείο Δικαιοσύνης (π.χ. «Είστε υπό έρευνα.»)
- Τεχνική υποστήριξη (π.χ. «Εντοπίσαμε έναν ιό στον υπολογιστή σας.»)
- Οικογένεια ή φίλοι (π.χ. «Έχω μπλέξει, στείλε μου χρήματα!»).

Συχνά δημιουργούν ένα αίσθημα επείγοντος ή φόβου για να σας κάνουν να δράσετε γρήγορα χωρίς να σκεφτείτε.

Προειδοποιητικά σημάδια που πρέπει να προσέχετε

- Σας λένε να δράσετε **αμέσως,** αλλιώς θα υποστείτε τις συνέπειες
- Σας ζητούν **προσωπικές πληροφορίες**, κωδικούς πρόσβασης ή τραπεζικά στοιχεία
- Σας ζητούν να **πληρώσετε με δωροκάρτες, κρυπτονομίσματα ή τραπεζικά εμβάσματα**
- Τα μηνύματα έχουν **παράξενη γραμματική ή ορθογραφία**
- Σας επικοινωνεί ξαφνικά κάποιος που δεν γνωρίζετε

Προληπτικά μέτρα

Πάντα να κάνετε τα εξής:

1. Διατηρήστε την ψυχραιμία σας. Πάρτε μια ανάσα και μην βιαστείτε.
2. Ποτέ μην δίνετε προσωπικές πληροφορίες μέσω τηλεφώνου, email ή SMS.
3. Κλείστε το τηλέφωνο ή διαγράψτε το μήνυμα αν σας φαίνεται ύποπτο.
4. Επαληθεύστε το αίτημα οι ίδιοι:

Αν κάποιος ισχυρίζεται ότι είναι από τράπεζα, εταιρεία διανομής, κυβερνητική υπηρεσία ή τεχνική υποστήριξη, επικοινωνήστε πάντα απευθείας με τον οργανισμό. Χρησιμοποιήστε την επίσημη ιστοσελίδα ή τον αριθμό τηλεφώνου τους, όχι αυτά που αναφέρονται στο μήνυμα ή στο email.

Παράδειγμα:

- **Καλέστε την τράπεζά σας χρησιμοποιώντας τον αριθμό που αναγράφεται στην τραπεζική σας κάρτα ή στον επίσημο ιστότοπο**
- **Επισκεφθείτε την επίσημη ιστοσελίδα της κυβέρνησης εάν δεν είστε σίγουροι για μηνύματα που σχετίζονται με φόρους**
- **Επικοινωνήστε με την επίσημη υποστήριξη της εταιρείας ταχυμεταφορών για να ελέγξετε αν ένα πακέτο είναι πραγματικό**

Να θυμάστε:

- **Οι πραγματικές εταιρείες δεν σας απειλούν ούτε σας πιέζουν**
- **Οι πραγματικές εταιρείες δεν θα σας ζητήσουν ποτέ κωδικούς πρόσβασης ή PIN**
- **Τα πραγματικά μηνύματα θα είναι επαγγελματικά και θα εκφράζουν σεβασμό.**
- **Οι απάτες βασίζονται στον φόβο, τη σύγχυση και την ταχύτητα**

Αν κάτι σας φαίνεται «περίεργο», σταματήστε και ρωτήστε κάποιον που εμπιστεύεστε. Είναι πάντα καλύτερο να ελέγχετε δύο φορές παρά να πέσετε σε παγίδα.

Παράρτημα 6 | Σενάρια: Εντοπίστε την απάτη

Σενάριο 1: Επείγον μήνυμα από τράπεζα

Λαμβάνετε ένα email που φαίνεται να προέρχεται από την τράπεζά σας. Το θέμα του μηνύματος είναι: «ΕΠΕΙΓΟΝ: Πρόβλημα πρόσβασης στο λογαριασμό». Το μήνυμα ισχυρίζεται ότι έχει σημειωθεί ύποπτη δραστηριότητα στο λογαριασμό σας και ότι πρέπει να επαληθεύσετε αμέσως τα προσωπικά και τραπεζικά σας στοιχεία. Περιέχει έναν σύνδεσμο και προειδοποιεί ότι, αν δεν απαντήσετε εντός 24 ωρών, ο λογαριασμός σας θα κλειστεί μόνιμα.

Σενάριο 2: Ειδοποίηση πλήρους αποθήκευσης τηλεφώνου

Καθώς περιηγείστε στο διαδίκτυο ή χρησιμοποιείτε μια εφαρμογή, εμφανίζεται ένα αναδυόμενο μήνυμα που λέει: «Προειδοποίηση! Η μνήμη του τηλεφώνου σας είναι πλήρης. Πατήστε εδώ για να καθαρίσετε τη συσκευή σας και να αποφύγετε την απώλεια δεδομένων». Το μήνυμα φαίνεται επείγον, μιμείται το στυλ του συστήματος του τηλεφώνου σας και, όταν το πατήσετε, σας ανακατευθύνει για να κατεβάσετε μια εφαρμογή τρίτου μέρους που υπόσχεται να βελτιστοποιήσει τη συσκευή σας.

Σενάριο 3: Κλήση τεχνικής υποστήριξης

Λαμβάνετε μια κλήση από κάποιον που ισχυρίζεται ότι είναι τεχνικός της Microsoft. Σας λένε ότι ο υπολογιστής σας έχει μολυνθεί από έναν επικίνδυνο ιό και στέλνει μηνύματα σφάλματος. Προσφέρονται να το διορθώσουν εξ αποστάσεως και σας καθοδηγούν στη λήψη λογισμικού για να τους δώσετε πρόσβαση στον υπολογιστή σας. Μόλις συνδεθούν, «σαρώνουν» τον υπολογιστή σας και στη συνέχεια απαιτούν πληρωμή για την αφαίρεση του ιού, ζητώντας συχνά την πιστωτική σας κάρτα ή πρόσβαση στο online banking.

Σενάριο 4: Απάτη με πληρωμή λογαριασμών κοινής ωφέλειας

Λαμβάνετε ένα email ή ένα μήνυμα κειμένου που φαίνεται να προέρχεται από τον πάροχο ηλεκτρικού ρεύματος. Ισχυρίζεται ότι η τελευταία σας πληρωμή απέτυχε και ότι, αν δεν πληρώσετε το οφειλόμενο ποσό εντός 12 ωρών, θα διακοπεί η παροχή ηλεκτρικού ρεύματος. Το μήνυμα περιλαμβάνει έναν σύνδεσμο προς μια σελίδα πληρωμής που μοιάζει πολύ με την πραγματική ιστοσελίδα του παρόχου, αλλά ζητά τα στοιχεία της πιστωτικής σας κάρτας και τα προσωπικά σας στοιχεία.

Σενάριο 5: Ειδοποίηση τραπεζικής συναλλαγής

Λαμβάνετε ένα email από την τράπεζά σας με θέμα: «Επιβεβαίωση συναλλαγής – 74,60 € στο MERKUR». Το μήνυμα επιβεβαιώνει μια συναλλαγή που πραγματοποιήθηκε σήμερα στις 13:45. Εάν δεν αναγνωρίζετε τη χρέωση, σας ζητά να καλέσετε το τμήμα απάτης της τράπεζας στον επίσημο αριθμό που αναγράφεται στον ιστότοπό της. Το email δεν περιλαμβάνει συνδέσμους στους οποίους μπορείτε να κάνετε κλικ και χρησιμοποιεί ήρεμο και επαγγελματικό τόνο.

Σενάριο 6: Προειδοποίηση αποθήκευσης Google

Λαμβάνετε ένα email από την Google με το εξής μήνυμα: «Ο χώρος αποθήκευσης του λογαριασμού σας Google είναι γεμάτος κατά 98%. Αυτή τη στιγμή χρησιμοποιείτε 14,8 GB από τα 15 GB που σας παρέχονται. Για να συνεχίσετε να λαμβάνετε email και να χρησιμοποιείτε το Google Drive, διαχειριστείτε ή αναβαθμίστε τον χώρο αποθήκευσης σας». Το μήνυμα περιέχει δύο κουμπιά: ένα για τη διαχείριση του χώρου αποθήκευσης και ένα για την αναβάθμιση, τα οποία οδηγούν και τα δύο σε επίσημους ιστότοπους της Google.

Παράρτημα 7 | Συνηθισμένες διαδικτυακές απάτες και πώς να προστατευτείτε

1. Smishing (SMS Phishing)
Λαμβάνετε ένα μήνυμα κειμένου που φαίνεται να προέρχεται από την τράπεζά σας, την υπηρεσία παράδοσης ή έναν κυβερνητικό φορέα. Μπορεί να ισχυρίζεται ότι υπάρχει κάποιο πρόβλημα με τον λογαριασμό ή το πακέτο σας και να περιλαμβάνει έναν σύνδεσμο.

Smishing: Phishing μέσω μηνυμάτων κειμένου, που συχνά περιέχουν επείγοντα μηνύματα που σας παραπλανούν να κάνετε κλικ σε έναν σύνδεσμο ή να παρέχετε προσωπικές πληροφορίες.

Κόκκινες σημαίες:
- Επείγουσα γλώσσα («ο λογαριασμός σας θα κλείσει»)
- Ύποπτοι σύνδεσμοι
- Ζήτηση προσωπικών ή τραπεζικών στοιχείων

Τι να κάνετε:
- Μην κάνετε ποτέ κλικ σε συνδέσμους από άγνωστους αριθμούς.
- Επικοινωνήστε απευθείας με την εταιρεία χρησιμοποιώντας έναν επίσημο αριθμό τηλεφώνου ή ιστότοπο.
- Αποκλείστε και αναφέρετε τον αποστολέα.

2. Vishing (Voice Phishing)
Λαμβάνετε μια τηλεφωνική κλήση από κάποιον που προσποιείται ότι είναι από την τράπεζά σας, την αστυνομία ή την τεχνική υποστήριξη. Σας ζητούν προσωπικές πληροφορίες ή ισχυρίζονται ότι έχει σημειωθεί ύποπτη δραστηριότητα.

Vishing: φωνητικό phishing, όπου οι απατεώνες υποδύονται νόμιμους φορείς μέσω τηλεφώνου για να κλέψουν πληροφορίες.

Παραλλαγή: Ψεύτικη φωνή με χρήση τεχνητής νοημοσύνης
Οι απατεώνες μπορούν πλέον να μιμηθούν τη φωνή ενός αγαπημένου προσώπου χρησιμοποιώντας τεχνητή νοημοσύνη. Μπορεί να καλέσουν προσποιούμενοι ότι είναι το εγγόνι ή το παιδί σας, ζητώντας επείγουσα βοήθεια ή χρήματα.

Προειδοποιητικά σημάδια:
- Ο καλών σας πιέζει να δράσετε γρήγορα
- Συναισθηματική χειραγώγηση («Έχω μπλέξει!»)
- Ζητάει χρήματα ή πληροφορίες

Τι να κάνετε:
- Κλείστε το τηλέφωνο και καλέστε τον αριθμό απευθείας χρησιμοποιώντας έναν γνωστό αριθμό.
- Επικοινωνήστε με άλλο μέλος της οικογένειας για να επαληθεύσετε την ιστορία.
- Μην δίνετε ποτέ προσωπικές ή τραπεζικές πληροφορίες μέσω τηλεφώνου.

3. Phishing (απάτη μέσω email)
Λαμβάνετε ένα email που φαίνεται επίσημο (από την τράπεζά σας, το PayPal, την εφορία κ.λπ.) και σας ζητά να επιβεβαιώσετε στοιχεία, να επαναφέρετε τον κωδικό πρόσβασής σας ή να κάνετε κλικ σε έναν σύνδεσμο.

Phishing: Ψεύτικα email ή μηνύματα κειμένου που σας παραπλανούν ώστε να αποκαλύψετε εμπιστευτικές πληροφορίες (όπως κωδικούς πρόσβασης ή τραπεζικά στοιχεία).

Προειδοποιητικά σημάδια:
- Το email περιέχει γραμματικά λάθη
- Χρησιμοποιεί εκφοβισμό («εντοπίστηκε μη εξουσιοδοτημένη σύνδεση»)
- Ζητά προσωπικές πληροφορίες

Τι να κάνετε:
- Μην κάνετε κλικ σε ύποπτους συνδέσμους.
- Ελέγξτε προσεκτικά τη διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα.
- Επικοινωνήστε με την εταιρεία μέσω της επίσημης ιστοσελίδας της.

4. Οικονομική απάτη

Οι απατεώνες προσποιούνται ότι είναι σύμβουλοι επενδύσεων, ψεύτικες φιλανθρωπικές οργανώσεις ή ακόμη και ερωτικοί σύντροφοι. Κερδίζουν την εμπιστοσύνη σας και στη συνέχεια ζητούν χρήματα, δωρεές ή βοήθεια.

Οικονομικές απάτες: οι απατεώνες ζητούν χρήματα με ψευδείς προφάσεις, συχνά υποσχόμενοι ανταμοιβές ή απειλώντας με συνέπειες.

Προειδοποιητικά σημάδια:
- Επενδυτικές αποδόσεις που είναι πολύ καλές για να είναι αληθινές
- Συναισθηματική χειραγώγηση
- Μη επαληθεύσιμες φιλανθρωπικές οργανώσεις ή σκοποί

Τι να κάνετε:
- Μην στέλνετε ποτέ χρήματα σε άτομα που δεν έχετε συναντήσει προσωπικά.
- Πάντα να ερευνάτε την εταιρεία ή το άτομο.
- Συμβουλευτείτε ένα έμπιστο μέλος της οικογένειας ή σύμβουλο πριν λάβετε οικονομικές αποφάσεις.

5. Ψεύτικες ταυτότητες και πλαστοπροσωπία

Οι απατεώνες μπορεί να προσποιούνται ότι είναι κάποιος άλλος, όπως κυβερνητικός υπάλληλος, τραπεζικός υπάλληλος ή ακόμα και μέλος της οικογένειας. Χρησιμοποιούν πλαστά έγγραφα, ηλεκτρονικά μηνύματα ή φωνές που δημιουργούνται με τεχνητή νοημοσύνη για να εξαπατήσουν τους ανθρώπους και να τους κάνουν να αποκαλύψουν ευαίσθητες πληροφορίες ή να στείλουν χρήματα.

Ψεύτικες ταυτότητες: Οι απατεώνες δημιουργούν ψεύτικα προφίλ στο διαδίκτυο για να κερδίσουν την εμπιστοσύνη των θυμάτων και να τα παρασύρουν να τους δώσουν χρήματα ή προσωπικές πληροφορίες.

Προειδοποιητικά σημάδια:
- Απροσδόκητα αιτήματα για προσωπικά δεδομένα ή χρήματα
- Αίσθημα επείγοντος ή συναισθηματική πίεση
- Επικοινωνία μέσω ανεπίσημων ή ύποπτων καναλιών

Τι να κάνετε:
- Πάντα να επαληθεύετε την ταυτότητα καλώντας το πραγματικό πρόσωπο ή τον πραγματικό φορέα μέσω των επίσημων στοιχείων επικοινωνίας.
- Μην φοβάστε να κλείσετε το τηλέφωνο και να ελέγξετε πρώτα.
- Όταν έχετε αμφιβολίες, ζητήστε από κάποιον που εμπιστεύεστε να σας βοηθήσει να αξιολογήσετε την κατάσταση.

6. Κακόβουλο λογισμικό ή malware

Είναι οποιοδήποτε λογισμικό που έχει σχεδιαστεί για να βλάψει έναν υπολογιστή ή να κλέψει προσωπικές πληροφορίες. Οι απατεώνες συχνά ξεγελούν τους χρήστες να το κατεβάσουν μέσω ψεύτικων email, συνδέσμων ή αναδυόμενων διαφημίσεων. Μόλις εγκατασταθεί, το κακόβουλο λογισμικό μπορεί να κλέψει κωδικούς πρόσβασης, να κλειδώσει αρχεία και ακόμη και να πάρει τον έλεγχο της συσκευής σας. Να είστε πάντα προσεκτικοί με άγνωστους συνδέσμους ή συνημμένα και βεβαιωθείτε ότι ο υπολογιστής σας διαθέτει ενημερωμένο λογισμικό προστασίας από ιούς για να είστε προστατευμένοι.

Παράρτημα 8 | Φυλλάδιο για τους συμμετέχοντες – Εντοπίστε το κακόβουλο λογισμικό

Στόχος

Εξοικειωθείτε με τους συνηθισμένους τύπους κακόβουλου λογισμικού (ιούς, trojans, spyware, ransomware, adware) διαβάζοντας και αναλύοντας αυτά τα ρεαλιστικά σενάρια.
Για κάθε απάτη, σημειώστε τι είδους απάτη είναι (trojan, ιός, adware, ransomware, spyware) και απαντήστε στην ερώτηση.

Σενάριο 1

«Λαμβάνετε ένα email από έναν αξιόπιστο φίλο με ένα συνημμένο με τίτλο «Σημαντικό έγγραφο». Όταν το ανοίγετε, ο υπολογιστής σας αρχίζει να επιβραδύνεται και εμφανίζονται παράξενα αναδυόμενα παράθυρα».

Ερώτηση: Τι είδους κακόβουλο λογισμικό πιστεύετε ότι είναι αυτό; Πώς θα προστατευόσασταν;

Σενάριο 2

«Κατά την περιήγησή σας, εμφανίζεται ένα αναδυόμενο παράθυρο με το μήνυμα «Η συσκευή σας είναι παλιά! Κάντε κλικ εδώ για να κατεβάσετε μια ενημέρωση». Κάνετε κλικ στον σύνδεσμο και, χωρίς να το γνωρίζετε, κατεβάζετε κακόβουλο λογισμικό που έχει μεταμφιεστεί ως ενημέρωση».

Ερώτηση: Ποιος είναι ο κίνδυνος σε αυτή την περίπτωση; Τι πρέπει να κάνετε αντ' αυτού;

Σενάριο 3

«Κατεβάζετε μια δωρεάν εφαρμογή επεξεργασίας φωτογραφιών από έναν άγνωστο ιστότοπο. Με την πάροδο του χρόνου, παρατηρείτε ότι εμφανίζονται διαφημίσεις στον browser σας και αρχίζετε να λαμβάνετε ανεπιθύμητα διαφημιστικά email».

Ερώτηση: Τι πιστεύετε ότι έχει συμβεί; Τι πρέπει να κάνετε στη συνέχεια;

Σενάριο 4

«Αφού κάνετε κλικ σε έναν σύνδεσμο σε ένα email που λέει: "Η συνδρομή σας στο Netflix πρόκειται να λήξει, κάντε κλικ εδώ για να επιβεβαιώσετε την πληρωμή", εμφανίζεται ένα μήνυμα που σας ζητά να πληρώσετε λύτρα για να ξεκλειδώσετε τα αρχεία σας».

Ερώτηση: Πώς μπορείτε να καταλάβετε ότι πρόκειται για απάτη; Τι πρέπει να κάνετε αν συμβεί κάτι τέτοιο;

Σενάριο 5

«Αφού κάνετε κλικ σε έναν σύνδεσμο σε ένα email που λέει: «Η συνδρομή σας στο Netflix πρόκειται να λήξει, κάντε κλικ εδώ για να επιβεβαιώσετε την πληρωμή», εμφανίζεται ένα μήνυμα που σας ζητά να πληρώσετε λύτρα για να ξεκλειδώσετε τα αρχεία σας».

Ερώτηση: Πρόκειται για επικίνδυνο λογισμικό; Ποια είναι η λύση για να το εξαλείψετε;

Παράρτημα 9 | Προστασία προσωπικών δεδομένων

1. Τι είναι τα προσωπικά δεδομένα;

Τα προσωπικά δεδομένα είναι οποιαδήποτε πληροφορία που μπορεί να χρησιμοποιηθεί για την ταυτοποίησή σας, είτε άμεσα είτε έμμεσα. Αυτά περιλαμβάνουν:

- **Βασικά δεδομένα:** Όνομα, επώνυμο, ημερομηνία γέννησης, διεύθυνση
- **Στοιχεία επικοινωνίας:** Διεύθυνση ηλεκτρονικού ταχυδρομείου, αριθμός τηλεφώνου
- **Αριθμούς ταυτοποίησης:** αριθμό ταυτότητας, αριθμό φορολογικού μητρώου, αριθμό διαβατηρίου
- **Οικονομικά δεδομένα:** Αριθμοί τραπεζικών λογαριασμών, αριθμοί πιστωτικών καρτών
- **Διαπιστευτήρια σύνδεσης:** Ονόματα χρήστη, κωδικοί πρόσβασης
- **Δεδομένα υγείας:** Ιατρικά αρχεία, συνταγές
- **Βιομετρικά δεδομένα:** δακτυλικά αποτυπώματα, αναγνώριση προσώπου, φωνή
- **Δεδομένα τοποθεσίας:** Εντοπισμός GPS, διεύθυνση IP
- **Προσωπικές προτιμήσεις:** Ιστορικό αναζήτησης, δραστηριότητα στα μέσα κοινωνικής δικτύωσης

2. Ποια δεδομένα μπορούν να είναι επιβλαβή αν πέσουν σε λάθος χέρια (και γιατί);

Οι απατεώνες και οι εγκληματίες του κυβερνοχώρου στοχεύουν συγκεκριμένα δεδομένα που μπορούν να χρησιμοποιηθούν για:

- **Κλέψουν την ταυτότητά σας**
- **Πρόσβαση στους τραπεζικούς σας λογαριασμούς**
- **Διαπράξουν απάτη στο όνομά σας**

Να σας χειραγωγήσουν συναισθηματικά ή οικονομικά

Τα πιο πολύτιμα δεδομένα για τους απατεώνες:

- **Προσωπική ταυτότητα (διαβατήριο κ.λπ.) -** Χρησιμοποιείται για κλοπή ταυτότητας ή άνοιγμα παράνομων λογαριασμών.
- **Διαπιστευτήρια σύνδεσης -** Παρέχουν πρόσβαση σε email, κοινωνικά δίκτυα, ηλεκτρονική τραπεζική.
- **Στοιχεία τραπεζικού λογαριασμού και πιστωτικής κάρτας -** Χρησιμοποιούνται για μη εξουσιοδοτημένες αγορές ή μεταφορές χρημάτων.
- **Αριθμοί τηλεφώνου και email -** Χρησιμοποιούνται για phishing, smishing, spam και πλαστοπροσωπία.
- **Περιεχόμενο κοινωνικών δικτύων -** Χρησιμοποιείται για τη δημιουργία ψεύτικων προφίλ ή για να σας χειραγωγήσουν.

3. Πού μπορούμε να μοιραζόμαστε τα προσωπικά μας στοιχεία στο διαδίκτυο;

Είναι σημαντικό να γνωρίζετε πού και πότε είναι ασφαλές να μοιράζεστε προσωπικά δεδομένα. Ορισμένες πλατφόρμες είναι αξιόπιστες, ενώ άλλες ενέχουν μεγαλύτερους κινδύνους.

Μέρη όπου είναι γενικά ασφαλές να μοιράζεστε προσωπικά δεδομένα (με προσοχή):

- Επαληθευμένα ηλεκτρονικά καταστήματα (π.χ. Amazon, Zalando, Mimovrste): Για αγορές, μόνο όταν ο ιστότοπος διαθέτει κρυπτογράφηση HTTPS και ασφαλείς μεθόδους πληρωμής.
- Επίσημοι ιστότοποι της κυβέρνησης (π.χ. IRS, πύλες κοινωνικής ασφάλισης, πύλες ηλεκτρονικής διακυβέρνησης): Για την υποβολή εγγράφων, φόρων, αιτήσεων.
- Αξιόπιστοι πάροχοι υπηρεσιών (π.χ. τράπεζα, πάροχος υγειονομικής περίθαλψης): Μόνο μέσω των επίσημων ιστότοπων ή εφαρμογών τους.
- Αξιόπιστοι πάροχοι ηλεκτρονικού ταχυδρομείου και υπηρεσίες cloud (π.χ. Gmail, Outlook, Dropbox): Κατά τη δημιουργία λογαριασμών, τη δημιουργία αντιγράφων ασφαλείας δεδομένων.

Πάντα βεβαιωθείτε ότι ο ιστότοπος είναι επίσημος, διαθέτει HTTPS και είναι γνωστός πριν υποβάλετε οποιαδήποτε πληροφορία.

Μέρη όπου πρέπει να είστε εξαιρετικά προσεκτικοί ή να αποφεύγετε να μοιράζεστε προσωπικές πληροφορίες:

- Μη επαληθευμένα ηλεκτρονικά καταστήματα ή διαφημίσεις (συχνά βρίσκονται μέσω αναδυόμενων παραθύρων ή κοινωνικών μέσων)
- Άγνωστες έρευνες, διαδικτυακά κουίζ ή διαγωνισμοί
- Μη ασφαλή δημόσια δίκτυα Wi-Fi
- Σύνδεσμοι σε ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου ή κειμένου
- Πλατφόρμες κοινωνικών μέσων, ειδικά σε σχόλια ή άμεσα μηνύματα

Συμβουλή: Ακόμα και όταν η πλατφόρμα σας φαίνεται γνωστή, ελέγχετε πάντα διπλά τη διεύθυνση ιστού και αποφύγετε να μοιράζεστε ευαίσθητα δεδομένα, όπως αριθμούς ταυτότητας ή οικονομικές πληροφορίες, εκτός αν είναι απολύτως απαραίτητο και ασφαλές.

4. Ποιες πληροφορίες μπορούμε να μοιραζόμαστε και ποιες δεν πρέπει ποτέ να μοιραζόμαστε στο διαδίκτυο;

- **Μπορούν να μοιραστούν (με προσοχή):** Όνομα, πόλη και μη συγκεκριμένη τοποθεσία, γενικά ενδιαφέροντα ή χόμπι, επαγγελματικές πληροφορίες (π.χ. τίτλος εργασίας), δημόσιο email (για την εργασία), φωτογραφίες προφίλ
- **Δεν πρέπει ΠΟΤΕ να μοιράζονται στο διαδίκτυο:** Κωδικοί πρόσβασης και PIN, πλήρης διεύθυνση (εκτός από επαληθευμένες κυβερνητικές υπηρεσίες και ηλεκτρονικά καταστήματα), αριθμοί ταυτότητας, αριθμοί φορολογικού μητρώου, στοιχεία τραπεζικού λογαριασμού ή πιστωτικής κάρτας, ιατρικά αρχεία ή πληροφορίες υγείας, ευαίσθητα οικογενειακά στοιχεία ή ταξιδιωτικά σχέδια

Βασικός κανόνας: Εάν οι πληροφορίες μπορούν να χρησιμοποιηθούν για πρόσβαση στα χρήματά σας, την ταυτότητά σας ή την ιδιωτική σας ζωή, μην τις μοιράζεστε στο διαδίκτυο, ανεξάρτητα από το ποιος τις ζητά.

5. Η δημιουργία αντιγράφων ασφαλείας των δεδομένων σας σημαίνει τη δημιουργία αντιγράφων σημαντικών αρχείων, εγγράφων, φωτογραφιών και ρυθμίσεων σε ασφαλή και ξεχωριστή τοποθεσία. Αυτή μπορεί να είναι ένας εξωτερικός σκληρός δίσκος, ένα κλειδί USB ή μια ασφαλής υπηρεσία αποθήκευσης στο cloud.

Γιατί είναι σημαντική η δημιουργία αντιγράφων ασφαλείας:

Τα δεδομένα σας μπορεί να χαθούν ή να παραβιαστούν ξαφνικά λόγω:

- Βλάβη της συσκευής (π.χ. βλάβη του υπολογιστή, βλάβη του τηλεφώνου)
- Κλοπή ή απώλεια του τηλεφώνου ή του υπολογιστή σας
- Επιθέσεις ransomware ή malware που κλειδώνουν ή καταστρέφουν τα αρχεία σας
- Τυχαία διαγραφή ή μορφοποίηση
- Φυσικές καταστροφές (πυρκαγιά, πλημμύρα κ.λπ.)

Πώς η δημιουργία αντιγράφων ασφαλείας σας προστατεύει από επιθέσεις κακόβουλου λογισμικού:

Το κακόβουλο λογισμικό, όπως το ransomware, μπορεί να κρυπτογραφήσει τα αρχεία σας και να απαιτήσει πληρωμή για να τα ξεκλειδώσει. Εάν διαθέτετε ένα ασφαλές αντίγραφο ασφαλείας, δεν χρειάζεται να πληρώσετε τα λύτρα – μπορείτε να επαναφέρετε τη συσκευή σας και να αποκαταστήσετε τα αρχεία σας με ασφάλεια από το αντίγραφο ασφαλείας.

Ομοίως, οι ιοί και τα trojans μπορούν να καταστρέψουν τα αρχεία ή το λειτουργικό σας σύστημα. Εάν έχετε δημιουργήσει αντίγραφα ασφαλείας των αρχείων σας, μπορείτε να επανεγκαταστήσετε το σύστημά σας και να επαναφέρετε τα σημαντικά δεδομένα σας χωρίς να χάσετε τίποτα.

Βέλτιστες πρακτικές για ασφαλή αντίγραφα ασφαλείας:

- Χρησιμοποιήστε τόσο τοπικό αντίγραφο ασφαλείας όσο και αντίγραφο ασφαλείας στο cloud: Φυλάξτε ένα αντίγραφο σε έναν εξωτερικό σκληρό δίσκο και ένα σε μια αξιόπιστη υπηρεσία cloud (όπως Google Drive, Dropbox, iCloud, OneDrive).
- Κρυπτογραφήστε τα ευαίσθητα αντίγραφα ασφαλείας: Χρησιμοποιήστε προστασία με κωδικό πρόσβασης ή κρυπτογράφηση για ευαίσθητα δεδομένα.
- Δημιουργήστε αντίγραφα ασφαλείας τακτικά: Ορίστε ένα εβδομαδιαίο ή μηνιαίο πρόγραμμα ανάλογα με τη συχνότητα με την οποία ενημερώνετε τα αρχεία σας.
- Αποσυνδέστε τους εξωτερικούς δίσκους όταν δεν τους χρησιμοποιείτε: Σε περίπτωση επίθεσης ransomware, μπορεί να στοχεύσει και τους συνδεδεμένους δίσκους.
- Ελέγξτε τα αντίγραφα ασφαλείας σας: Βεβαιωθείτε ότι το σύστημα δημιουργίας αντιγράφων ασφαλείας λειτουργεί, προσπαθώντας να επαναφέρετε αρχεία περιστασιακά.

6. Συμβουλές για την ασφάλεια των δεδομένων σας

- Χρησιμοποιήστε ισχυρούς, μοναδικούς κωδικούς πρόσβασης (και αλλάζετε τους τακτικά)
- Ενεργοποιήστε την επαλήθευση δύο παραγόντων (2FA)
- Διατηρήστε το λογισμικό και το antivirus ενημερωμένα
- Αποφύγετε να κάνετε κλικ σε ύποπτους συνδέσμους ή συνημμένα
- Μην μοιράζεστε προσωπικές πληροφορίες μέσω τηλεφώνου ή email, εκτός αν έχουν επαληθευτεί
- Δημιουργήστε τακτικά αντίγραφα ασφαλείας των δεδομένων σας (στο cloud ή σε εξωτερικό σκληρό δίσκο)
- Να είστε προσεκτικοί με τα δημόσια δίκτυα Wi-Fi – αποφύγετε να συνδέεστε σε ευαίσθητους λογαριασμούς
- Ελέγξτε τις ρυθμίσεις απορρήτου σας στα μέσα κοινωνικής δικτύωσης
- Σκεφτείτε πριν δημοσιεύσετε – μόλις δημοσιευτεί κάτι στο διαδίκτυο, μπορεί να αντιγραφεί ή να χρησιμοποιηθεί καταχρηστικά

Παράρτημα 10 | Πώς να δημιουργήσετε αντίγραφα ασφαλείας των αρχείων σας

1. Δημιουργία αντιγράφων ασφαλείας αρχείων σε εξωτερικό δίσκο

Βήμα 1: Συνδέστε τον εξωτερικό σας δίσκο

- Συνδέστε τον εξωτερικό σκληρό δίσκο ή το USB stick στον υπολογιστή σας χρησιμοποιώντας το κατάλληλο καλώδιο ή θύρα.
- Βεβαιωθείτε ότι η συσκευή αναγνωρίζεται από τον υπολογιστή σας (ελέγξτε το φάκελο «Αυτός ο υπολογιστής» ή «Ο υπολογιστής μου» για Windows ή το Finder για Mac).

Βήμα 2: Επιλέξτε τα αρχεία που θέλετε να δημιουργήσετε αντίγραφα ασφαλείας

- Ανοίξτε το φάκελο που περιέχει τα αρχεία που θέλετε να δημιουργήσετε αντίγραφα ασφαλείας.
- Μπορείτε να επιλέξετε συγκεκριμένα αρχεία ή ολόκληρους φακέλους. Για να επιλέξετε πολλά αρχεία ή φακέλους, κρατήστε πατημένο το πλήκτρο Ctrl (Windows) ή Cmd (Mac) ενώ κάνετε κλικ στα στοιχεία.

Βήμα 3: Αντιγράψτε τα αρχεία

- Κάντε δεξί κλικ στα επιλεγμένα αρχεία και επιλέξτε "Αντιγραφή" (ή χρησιμοποιήστε το πλήκτρο συντόμευσης **Ctrl+C** για Windows, **Cmd+C** για Mac).
- Μεταβείτε στον εξωτερικό δίσκο στο "Αυτός ο υπολογιστής" (Windows) ή στο Finder (Mac).
- Κάντε δεξί κλικ στον εξωτερικό δίσκο και επιλέξτε Επικόλληση (ή χρησιμοποιήστε **Ctrl+V** για Windows, **Cmd+V** για Mac) για να αντιγράψετε τα αρχεία.

Βήμα 4: Αφαιρέστε με ασφάλεια τον εξωτερικό δίσκο

- Μόλις αντιγραφούν τα αρχεία, βεβαιωθείτε ότι έχετε αποσυνδέσει με ασφάλεια τον εξωτερικό δίσκο για να αποφύγετε τη φθορά των αρχείων.
- Στα Windows, κάντε δεξί κλικ στον εξωτερικό δίσκο στο "Αυτός ο υπολογιστής" και επιλέξτε "Αφαίρεση".
- Σε Mac, σύρετε το εικονίδιο του εξωτερικού δίσκου στον Κάδο απορριμμάτων ή κάντε κλικ στο κουμπί εξαγωγής δίπλα στο δίσκο στο Finder.
- Στη συσκευή Apple (Mac ή iPhone), μεταβείτε στις **Ρυθμίσεις** και συνδεθείτε με το Apple ID σας.
- Σε Mac, μπορείτε να αποκτήσετε πρόσβαση στο iCloud από **τις Προτιμήσεις συστήματος** > **Apple ID** > **iCloud**.
- Σε iPhone, μεταβείτε στις **Ρυθμίσεις** > [Το όνομά σας] > **iCloud**.

2. Δημιουργία αντιγράφων ασφαλείας αρχείων σε μια υπηρεσία cloud

Χρήση του Google Drive

Βήμα 1: Συνδεθείτε στον λογαριασμό σας Google

- Ανοίξτε ένα πρόγραμμα περιήγησης ιστού και μεταβείτε στο Google Drive.
- Συνδεθείτε με τα στοιχεία του λογαριασμού σας Google (ή δημιουργήστε έναν νέο λογαριασμό αν δεν έχετε).

Βήμα 2: Ανεβάστε αρχεία στο Google Drive

- Κάντε κλικ στο κουμπί Νέο στην αριστερή πλευρική γραμμή.
- Επιλέξτε Μεταφόρτωση αρχείου ή Μεταφόρτωση φακέλου, ανάλογα με το τι θέλετε να δημιουργήσετε αντίγραφο ασφαλείας.
- Αναζητήστε τα αρχεία ή τους φακέλους που θέλετε να ανεβάσετε και κάντε κλικ στο κουμπί Άνοιγμα.

Βήμα 3: Οργανώστε τα αρχεία σας (προαιρετικό)

- Μπορείτε να δημιουργήσετε φακέλους στο Google Drive για να οργανώσετε το αντίγραφο ασφαλείας σας. Κάντε κλικ στο Νέο > Φάκελος, ονομάστε το φάκελο και μετακινήστε τα αρχεία σε αυτόν με μεταφορά και απόθεση.

Βήμα 4: Ελέγξτε τη μεταφόρτωση

- Βεβαιωθείτε ότι η μεταφόρτωση των αρχείων σας έχει ολοκληρωθεί. Το Google Drive θα εμφανίσει μια γραμμή κατάστασης ενώ η μεταφόρτωση είναι σε εξέλιξη.

Χρήση του Dropbox

Βήμα 1: Συνδεθείτε στον λογαριασμό σας στο Dropbox

- Ανοίξτε ένα πρόγραμμα περιήγησης και μεταβείτε στο Dropbox.
- Συνδεθείτε ή δημιουργήστε έναν νέο λογαριασμό Dropbox, αν δεν έχετε ήδη.

Βήμα 2: Ανεβάστε αρχεία στο Dropbox

- Μόλις συνδεθείτε, κάντε κλικ στο κουμπί Μεταφόρτωση αρχείων.
- Επιλέξτε τα αρχεία ή τους φακέλους που θέλετε να δημιουργήσετε αντίγραφα ασφαλείας από τον υπολογιστή σας και κάντε κλικ στο κουμπί Άνοιγμα.
- Μπορείτε επίσης να μεταφέρετε και να αποθέσετε αρχεία απευθείας στον ιστότοπο του Dropbox.
- Στο iPhone, ελέγξτε τη χρήση του χώρου αποθήκευσης iCloud μεταβαίνοντας στις Ρυθμίσεις > [Το όνομά σας] > iCloud

Σημαντικές συμβουλές για τη δημιουργία αντιγράφων ασφαλείας:

- Δημιουργείτε αντίγραφα ασφαλείας τακτικά: Συνηθίστε να δημιουργείτε αντίγραφα ασφαλείας των δεδομένων σας τουλάχιστον μία φορά την εβδομάδα, για να βεβαιωθείτε ότι δεν θα χάσετε σημαντικά αρχεία.
- Χρησιμοποιήστε τόσο τοπικά αντίγραφα ασφαλείας όσο και αντίγραφα ασφαλείας στο cloud: Φυλάξτε ένα αντίγραφο των δεδομένων σας τόσο σε έναν εξωτερικό σκληρό δίσκο όσο και στο cloud για επιπλέον ασφάλεια.
- Κρυπτογράφησε ευαίσθητα αρχεία: Όταν αποθηκεύεις ευαίσθητα δεδομένα (π.χ. οικονομικά αρχεία, προσωπικά έγγραφα), σκέψου να τα κρυπτογραφήσεις πριν τα ανεβάσεις στο cloud ή τα αποθηκεύσεις σε εξωτερικό δίσκο.
- Ελέγξτε το αντίγραφο ασφαλείας: Ελέγχετε περιστασιακά το αντίγραφο ασφαλείας επαναφέροντας ορισμένα αρχεία για να βεβαιωθείτε ότι όλα λειτουργούν σωστά.

Η δημιουργία αντιγράφων ασφαλείας των αρχείων σας είναι ζωτικής σημασίας για να διασφαλίσετε ότι τα δεδομένα σας είναι ασφαλή και ανακτήσιμα σε περίπτωση βλάβης της συσκευής, κυβερνοεπίθεσης ή τυχαίας διαγραφής. Τόσο οι εξωτερικοί δίσκοι όσο και οι υπηρεσίες cloud προσφέρουν αξιόπιστους τρόπους για την ασφαλή αποθήκευση των δεδομένων σας. Εάν έχετε οποιεσδήποτε ερωτήσεις, μη διστάσετε να ζητήσετε βοήθεια ή υποστήριξη για τη ρύθμιση του συστήματος δημιουργίας αντιγράφων ασφαλείας!

Παράρτημα 11| Λίστα ελέγχου για την ασφάλεια στο διαδίκτυο

1. Προστασία προσωπικών δεδομένων

- **Ελέγξτε τις προσωπικές πληροφορίες που μοιράζεστε στο διαδίκτυο** – Να είστε πάντα προσεκτικοί με ό,τι δημοσιεύετε στα μέσα κοινωνικής δικτύωσης και σε άλλες πλατφόρμες. Μοιραστείτε μόνο τις απαραίτητες πληροφορίες.

- **Διατηρήστε την εμπιστευτικότητα των ευαίσθητων πληροφοριών** – Μην μοιράζεστε ποτέ κωδικούς πρόσβασης, PIN, αριθμούς τραπεζικών λογαριασμών ή αριθμούς ταυτότητας στο διαδίκτυο.

- **Χρησιμοποιήστε ισχυρούς, μοναδικούς κωδικούς πρόσβασης** για τους λογαριασμούς σας και αλλάζετε τους τακτικά.

  Ενεργοποιήστε την επαλήθευση δύο παραγόντων στους λογαριασμούς σας, όπου είναι δυνατόν, ειδικά για τραπεζικούς λογαριασμούς, email και μέσα κοινωνικής δικτύωσης.

2. Αναγνώριση απάτης

- **Να είστε ενήμεροι για τις συνήθεις διαδικτυακές απάτες** – Μάθετε να αναγνωρίζετε απάτες όπως το phishing, το smishing, το vishing και τις οικονομικές απάτες.

- **Προειδοποιητικά σημάδια για απάτες**:

  - Γλώσσα που υποδηλώνει επείγοντα (π.χ. «Απαιτείται άμεση δράση!»)
  - Αιτήματα για προσωπικά, τραπεζικά ή στοιχεία σύνδεσης
  - Ύποπτοι σύνδεσμοι ή αριθμοί τηλεφώνου
  - Συναισθηματική χειραγώγηση ή απειλές (π.χ. «Ο λογαριασμός σας θα κλείσει»)

- **Γνωρίστε τη διαφορά μεταξύ νόμιμων και δόλιων αιτημάτων** – Επαληθεύστε την αυθεντικότητα κάθε τηλεφωνικής κλήσης, email ή μηνύματος που λαμβάνετε πριν απαντήσετε.

- **Σε περίπτωση αμφιβολίας, επικοινωνήστε πάντα απευθείας με τον οργανισμό** χρησιμοποιώντας τα επίσημα στοιχεία επικοινωνίας του για να επαληθεύσετε τον ισχυρισμό.

3. Αντιμετώπιση απάτης και κακόβουλου περιεχομένου

- **Μην κάνετε κλικ σε ύποπτους συνδέσμους και μην ανοίγετε συνημμένα** από άγνωστους αποστολείς. Αυτά μπορεί να είναι απόπειρες ηλεκτρονικού ψαρέματος ή να περιέχουν κακόβουλο λογισμικό.

- **Αναφέρετε τυχόν ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα ή τηλεφωνικές κλήσεις** στις αρμόδιες αρχές (π.χ. SI-CERT στη Σλοβενία).

- **Ελέγχετε πάντα κάθε οικονομικό αίτημα** (μεταφορές χρημάτων, στοιχεία πιστωτικής κάρτας) καλώντας απευθείας το άτομο ή τον οργανισμό.

- **Να είστε προσεκτικοί με τις ανεπιθύμητες τηλεφωνικές κλήσεις**, ειδικά αν ο καλών σας πιέζει να του δώσετε χρήματα ή προσωπικά στοιχεία. Κλείστε το τηλέφωνο και καλέστε ξανά χρησιμοποιώντας έναν γνωστό αριθμό.

4. Προστασία των συσκευών σας από κακόβουλο λογισμικό

- **Εγκαταστήστε και ενημερώστε το λογισμικό προστασίας από ιούς** για να προστατεύσετε τη συσκευή σας από ιούς, κακόβουλο λογισμικό και λογισμικό υποκλοπής δεδομένων.
- **Αποφύγετε τη λήψη εφαρμογών ή λογισμικού** από μη επαληθευμένες πηγές. Χρησιμοποιείτε μόνο επίσημα καταστήματα εφαρμογών (Google Play Store, Apple App Store).
- **Δημιουργείτε τακτικά αντίγραφα ασφαλείας των δεδομένων σας** σε εξωτερικό δίσκο ή υπηρεσία cloud για να αποτρέψετε την απώλεια δεδομένων από πιθανή επίθεση.
- **Διατηρήστε το λογισμικό και τις συσκευές σας ενημερωμένα** με τις πιο πρόσφατες ενημερώσεις ασφαλείας.
- **Να είστε προσεκτικοί όταν χρησιμοποιείτε δημόσια δίκτυα Wi-Fi** – Αποφύγετε την πρόσβαση σε ευαίσθητους λογαριασμούς ενώ είστε συνδεδεμένοι σε δημόσια δίκτυα.

5. Ασφαλείς διαδικτυακές αγορές

- **Αγοράζετε μόνο από επαληθευμένους, αξιόπιστους ιστότοπους** – Αναζητήστε το σύμβολο του λουκέτου στη γραμμή του προγράμματος περιήγησης και το «https» στη διεύθυνση URL.
- **Χρησιμοποιείτε ασφαλείς μεθόδους πληρωμής**, όπως πιστωτικές κάρτες, όταν πραγματοποιείτε αγορές στο διαδίκτυο, καθώς προσφέρουν προστασία από απάτες .
- **Ελέγξτε τις κριτικές και τις αξιολογήσεις** πριν πραγματοποιήσετε μια αγορά από ένα νέο ηλεκτρονικό κατάστημα.

6. Δημιουργήστε αντίγραφα ασφαλείας των δεδομένων σας

- **Δημιουργήστε** τακτικά **αντίγραφα ασφαλείας σημαντικών αρχείων** (έγγραφα, φωτογραφίες, επαφές) σε εξωτερικό δίσκο ή υπηρεσία cloud. Αυτό θα προστατεύσει τα δεδομένα σας από βλάβη της συσκευής ή επιθέσεις ransomware.
- **Χρησιμοποιήστε μια αξιόπιστη υπηρεσία δημιουργίας αντιγράφων ασφαλείας στο cloud** (Google Drive, Dropbox, OneDrive) για πρόσθετη ασφάλεια.
- **Δημιουργήστε ένα πρόγραμμα δημιουργίας αντιγράφων ασφαλείας,** ώστε να βεβαιώνεστε ότι τα δεδομένα σας είναι πάντα ενημερωμένα και ασφαλή.

7. Ασφάλεια στα μέσα κοινωνικής δικτύωσης

- **Να είστε προσεκτικοί με το τι μοιράζεστε** στις πλατφόρμες κοινωνικών μέσων (Facebook, Instagram κ.λπ.). Αποφύγετε να μοιράζεστε ευαίσθητες πληροφορίες, όπως την πλήρη διεύθυνσή σας, τον αριθμό τηλεφώνου σας και τα οικονομικά σας στοιχεία .

- **Προσαρμόστε τις ρυθμίσεις απορρήτου σας** για να ελέγχετε ποιος μπορεί να δει τις αναρτήσεις και τις προσωπικές σας πληροφορίες.

- **Μην αποδέχεστε αιτήματα φιλίας** ή μηνύματα από άγνωστους. Αν δεν γνωρίζετε το άτομο, είναι ασφαλέστερο να αγνοήσετε το αίτημα.

8. Πώς να αντιμετωπίσετε μια επίθεση κοινωνικής μηχανικής

- **Διατηρήστε την ψυχραιμία σας και μην ενεργείτε βιαστικά** εάν λάβετε ένα ύποπτο μήνυμα ή τηλεφώνημα.

- **Ποτέ μην δίνετε προσωπικές πληροφορίες μέσω τηλεφώνου, email** ή **SMS, εκτός εάν είστε σίγουροι για την ταυτότητα** του ατόμου με το οποίο μιλάτε.

- **Επαληθεύστε την ταυτότητα του καλούντος** καλώντας τον πίσω χρησιμοποιώντας επίσημα τηλέφωνα επικοινωνίας (π.χ. τον επίσημο αριθμό της τράπεζάς σας ή τον ιστότοπο της εταιρείας).

- **Μην πιέζεστε** – Οι απατεώνες συχνά δημιουργούν μια αίσθηση επείγοντος για να σας κάνουν να ενεργήσετε γρήγορα. Πάρτε το χρόνο σας και επαληθεύστε το αίτημα.

9. Αντιμετώπιση έκτακτων περιστατικών

- **Εάν υποψιάζεστε ότι έχετε πέσει θύμα απάτης ή ότι τα προσωπικά σας στοιχεία έχουν παραβιαστεί**, επικοινωνήστε αμέσως με την τράπεζά σας ή την εταιρεία της πιστωτικής σας κάρτας για να παγώσετε τους λογαριασμούς σας.

- **Αναφέρετε τις απάτες στις αρχές**, όπως το SI-CERT στη Σλοβενία ή την τοπική αστυνομία, εάν είναι απαραίτητο.

- **Ζητήστε συμβουλές από έναν έμπιστο φίλο ή** μέλος **της οικογένειας** εάν δεν είστε σίγουροι για μια κατάσταση.

10. Μείνετε ενημερωμένοι

- Μείνετε ενημερωμένοι για τις τελευταίες απάτες – Εγγραφείτε σε ενημερωτικά δελτία ή ειδοποιήσεις από αξιόπιστες πηγές, όπως το SI-CERT ή άλλες πλατφόρμες ασφάλειας.

- Ενημερωθείτε τακτικά για τις διαδικτυακές απειλές και τον τρόπο προστασίας σας.

Να θυμάστε:
Το διαδίκτυο μπορεί να είναι ένα εξαιρετικό εργαλείο, αλλά είναι σημαντικό να παραμένετε σε εγρήγορση και να ενημερώνεστε για τους πιθανούς κινδύνους. Ακολουθώντας αυτόν τον κατάλογο ελέγχου, μπορείτε να μειώσετε σημαντικά την ευπάθειά σας και να διατηρήσετε την ασφάλεια των προσωπικών σας πληροφοριών και των συσκευών σας. Αν έχετε αμφιβολίες, ζητήστε πάντα βοήθεια ή συμβουλές από κάποιον που εμπιστεύεστε. Η ασφάλεια και η ηρεμία σας είναι η κορυφαία προτεραιότητα!

Παράρτημα 12 | Προτάσεις για περαιτέρω ανάγνωση και μάθηση για τους συμμετέχοντες

Ιστοσελίδες για την ασφάλεια στον κυβερνοχώρο: Ευρωπαϊκοί και κυβερνητικοί οργανισμοί που ασχολούνται με την ασφάλεια στον κυβερνοχώρο

1) **OLAF - ΕΥΡΩΠΑΪΚΗ ΥΠΗΡΕΣΙΑ ΚΑΤΑ ΤΗΣ ΑΠΑΤΗΣ**
   Ιστότοπος: https://anti-fraud.ec.europa.eu/olaf-and-you/report-fraud_en
   Η OLAF είναι ένας οργανισμός της ΕΕ που διερευνά περιπτώσεις απάτης, διαφθοράς και σοβαρών παραβάσεων εντός των θεσμικών οργάνων και των ταμείων της ΕΕ .

2) **Υποστήριξη θυμάτων στην Ευρώπη**
   Ιστότοπος: https://victim-support.eu/help-for-victims/info-on-specific-types-of-victims/fraud-victims/
   Η Victim Support Europe είναι μια ευρωπαϊκή οργάνωση που προασπίζει τα δικαιώματα όλων των θυμάτων εγκληματικών πράξεων και παρέχει υπηρεσίες υποστήριξης μέσω του δικτύου των εθνικών οργανώσεων-μελών της.

3) **EC3 – Κέντρο Κυβερνοεγκλημάτων της Ευρωπόλης**
   Ιστοσελίδα: https://www.europol.europa.eu/crime-areas/cybercrime
   Η Europol παρέχει πληροφορίες σχετικά με το έγκλημα στον κυβερνοχώρο και την ασφάλεια των δεδομένων.

4) **CERT-EU (Ομάδα Αντιμετώπισης Έκτακτων Περιστατικών Πληροφορικής για τα Όργανα της ΕΕ)**
   Ιστοσελίδα: https://cert.europa.eu/
   Ο οργανισμός παρακολουθεί τις απειλές στον κυβερνοχώρο και ανταποκρίνεται σε κυβερνοεπιθέσεις κατά των θεσμικών οργάνων της Ευρωπαϊκής Ένωσης.

3.5 Ενότητα ΙΙ – Προ/Μετα-τεστ

1. Ποιο από τα παρακάτω είναι παράδειγμα ασφαλούς συμπεριφοράς στο διαδίκτυο;
Α) Η κοινοποίηση της προσωπικής σας διεύθυνσης στα μέσα κοινωνικής δικτύωσης
Β) Χρήση ισχυρών και μοναδικών κωδικών πρόσβασης για κάθε λογαριασμό
Γ) Αποδοχή αιτημάτων φιλίας από άγνωστα άτομα
Δ) Κλικ σε κάθε σύνδεσμο που φαίνεται ενδιαφέρον

2. Ποιος είναι ένας συνηθισμένος κίνδυνος κατά τη χρήση των μέσων κοινωνικής δικτύωσης;

Α) Η γνωριμία με νέους φίλους
Β) Υπερφόρτωση πληροφοριών
Γ) Η υπερβολική κοινοποίηση προσωπικών πληροφοριών που μπορούν να χρησιμοποιηθούν καταχρηστικά
Δ) Η τακτική ενημέρωση των ρυθμίσεων απορρήτου

3. Γιατί πρέπει να επαληθεύετε την πηγή πριν μοιραστείτε πληροφορίες στο διαδίκτυο;

Α) Για να αποφύγετε τη διάδοση ψευδών πληροφοριών ή απάτες
Β) Για να αυξήσετε τον αριθμό των «μου αρέσει» και των ακολούθων
Γ) Για να βελτιώσετε την απόδοση του υπολογιστή σας
Δ) Για να αλλάξετε το επίπεδο ασφάλειας του προφίλ σας

4. Ποιος από αυτούς τους κωδικούς πρόσβασης είναι ο πιο ισχυρός;

Α) 123456
Β) qwerty
Γ) Sunflower2025!#
Δ) password

5. Τι πρέπει να κάνετε αν λάβετε ένα ύποπτο μήνυμα από τον παραβιασμένο λογαριασμό ενός φίλου σας;

Α) Κάντε κλικ στον σύνδεσμο για να δείτε τι είναι
Β) Να αναφέρετε ή να αποκλείσετε τον λογαριασμό και να ενημερώσετε τον φίλο σας
Γ) Απαντήστε ζητώντας περισσότερες πληροφορίες
Δ) Να το αγνοήσετε εντελώς

6. Τι σημαίνει «ψηφιακό αποτύπωμα»;

Α) Το συνολικό μέγεθος των δεδομένων που είναι αποθηκευμένα στον υπολογιστή σας
Β) Το αρχείο των διαδικτυακών δραστηριοτήτων σας και των πληροφοριών που έχετε μοιραστεί
Γ) Ο κωδικός πρόσβασης που χρησιμοποιείτε για τους λογαριασμούς σας
Δ) Το λογισμικό που προστατεύει τον υπολογιστή σας

7. Γιατί είναι επικίνδυνο να χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης για όλους τους λογαριασμούς σας;

Α) Μπορεί να καθυστερήσει υπερβολικά τη διαδικασία σύνδεσης
Β) Εάν ένας λογαριασμός παραβιαστεί, οι άλλοι μπορούν εύκολα να εκτεθούν σε κίνδυνο
Γ) Εξοικονομεί πολύ χρόνο
Δ) Απαιτεί τη χρήση διαχειριστών κωδικών πρόσβασης

8. Ποιος είναι ο καλύτερος τρόπος για να προστατεύσετε την ιδιωτικότητά σας στα μέσα κοινωνικής δικτύωσης;

Α) Ρυθμίστε το προφίλ σας ως «δημόσιο»
Β) Να μοιραστείτε όλα τα προσωπικά σας στοιχεία
Γ) Ελέγχετε και προσαρμόζετε τακτικά τις ρυθμίσεις απορρήτου
Δ) Χρησιμοποιήστε την πραγματική ημερομηνία γέννησης και διεύθυνσή σας σε κάθε ανάρτηση

9. Ποιο είναι το σημάδι ενός ψεύτικου ή απατηλού ιστότοπου;

Α) Ξεκινά με «https://»
Β) Έχει ορθογραφικά λάθη και μη ρεαλιστικές προσφορές
Γ) Εμφανίζει ένα σύμβολο κλειδώματος στο πρόγραμμα περιήγησης
Δ) Παρέχει στοιχεία επικοινωνίας

10. Γιατί πρέπει να αποσυνδέεστε από τους λογαριασμούς σας σε κοινόχρηστους ή δημόσιους υπολογιστές;

Α) Για να αφήσετε χώρο για τον επόμενο χρήστη
Β) Για να αποτρέψετε τη μη εξουσιοδοτημένη πρόσβαση στα δεδομένα σας
Γ) Για να εξοικονομήσετε ενέργεια της μπαταρίας
Δ) Για να ενημερώσετε αυτόματα τον κωδικό πρόσβασής σας

Περίληψη απαντήσεων

1	**Β**
2	**Γ**
3	**Α**
4	**C**
5	**Β**
6	**Β**
7	**Β**
8	**C**
9	**Β**
10	**Β**

ΕΝΟΤΗΤΑ ΙΙΙ

Ασφάλεια στις ηλεκτρονικές τραπεζικές συναλλαγές και τις αγορές

4. Ενότητα III - Ασφάλεια στις ηλεκτρονικές τραπεζικές συναλλαγές και στις αγορές μέσω διαδικτύου

Στόχος αυτού του ενότητας είναι να δώσει στους ηλικιωμένους τη δυνατότητα να χρησιμοποιούν με αυτοπεποίθηση τις πλατφόρμες ηλεκτρονικής τραπεζικής και ηλεκτρονικών αγορών, παρέχοντάς τους τις απαραίτητες γνώσεις και πρακτικές δεξιότητες για τη διαχείριση των ψηφιακών χρηματοοικονομικών δραστηριοτήτων. Η ενότητα ενισχύει την κατανόηση των συμμετεχόντων σχετικά με τον τρόπο λειτουργίας των υπηρεσιών ηλεκτρονικής τραπεζικής και ηλεκτρονικού εμπορίου, ενώ δίνει έμφαση στις ασφαλείς και υπεύθυνες πρακτικές για την προστασία από απάτες, εξαπατήσεις και απειλές στον κυβερνοχώρο.

Μέσω πρακτικών οδηγιών και παραδειγμάτων από την πραγματική ζωή, η ενότητα υποστηρίζει την ανάπτυξη ψηφιακών δεξιοτήτων και ενθαρρύνει τους ηλικιωμένους να υιοθετήσουν ασφαλείς συνήθειες κατά την πραγματοποίηση ηλεκτρονικών πληρωμών, τη διαχείριση λογαριασμών και την κοινοποίηση προσωπικών πληροφοριών. Στο τέλος της ενότητας, οι συμμετέχοντες είναι καλύτερα προετοιμασμένοι για να διατηρήσουν την οικονομική τους ανεξαρτησία, να αξιοποιήσουν τις ψηφιακές υπηρεσίες και να πραγματοποιούν ηλεκτρονικές τραπεζικές συναλλαγές και αγορές με αυτοπεποίθηση, ασφάλεια και αυτονομία.

Επιπλέον, το πρόγραμμα αντιμετωπίζει τους συνηθισμένους φόβους και αβεβαιότητες που μπορεί να βιώνουν οι ηλικιωμένοι κατά τη χρήση ψηφιακών χρηματοοικονομικών υπηρεσιών, με στόχο τη μείωση του άγχους που σχετίζεται με τις διαδικτυακές συναλλαγές. Οι συμμετέχοντες καθοδηγούνται ώστε να αναγνωρίζουν αξιόπιστες πλατφόρμες, να εφαρμόζουν βασικούς ελέγχους ασφαλείας και να ανταποκρίνονται κατάλληλα σε ύποπτες δραστηριότητες. Ενισχύοντας την εμπιστοσύνη μέσω της πρακτικής και των σαφών εξηγήσεων, το πρόγραμμα βοηθά τους ηλικιωμένους να αισθάνονται ότι έχουν μεγαλύτερο έλεγχο των ψηφιακών χρηματοοικονομικών αποφάσεών τους και υποστηρίζει τη μακροπρόθεσμη συμμετοχή τους σε διαδικτυακές τραπεζικές συναλλαγές και αγορές με ασφαλή και ενημερωμένο τρόπο.

4.1 Μαθησιακοί στόχοι

Ο κύριος στόχος αυτού του μαθήματος είναι να εξοπλίσει τους ηλικιωμένους με τις πρακτικές γνώσεις και δεξιότητες που είναι απαραίτητες για την ασφαλή χρήση των πλατφορμών ηλεκτρονικής τραπεζικής και ηλεκτρονικού εμπορίου. Το μάθημα εστιάζει στην οικοδόμηση της ψηφιακής εμπιστοσύνης, μειώνοντας ταυτόχρονα τον φόβο και το άγχος που σχετίζονται με την τεχνολογία, επιτρέποντας στους συμμετέχοντες να διαχειρίζονται τις χρηματοοικονομικές συναλλαγές με ασφάλεια και ανεξαρτησία. Οι συμμετέχοντες θα μάθουν πώς να προστατεύουν τα προσωπικά και χρηματοοικονομικά τους στοιχεία, να αναγνωρίζουν τους κινδύνους του διαδικτύου και να εφαρμόζουν αποτελεσματικές πρακτικές ασφάλειας στις καθημερινές ψηφιακές χρηματοοικονομικές δραστηριότητες.

- Κατανόηση των βασικών αρχών των ηλεκτρονικών τραπεζικών συναλλαγών και του ηλεκτρονικού εμπορίου που υποστηρίζουν την ασφαλή πλοήγηση, τη διαχείριση λογαριασμών και τις ψηφιακές συναλλαγές.

- Ανάπτυξη δεξιοτήτων για τη δημιουργία ισχυρών κωδικών πρόσβασης και την ενεργοποίηση της επαλήθευσης δύο παραγόντων (2FA) στο, προκειμένου να ενισχυθεί η ασφάλεια των διαδικτυακών λογαριασμών.

- Να αναγνωρίζουν αξιόπιστες πλατφόρμες και πωλητές ηλεκτρονικού εμπορίου, αναγνωρίζοντας δείκτες ασφάλειας όπως HTTPS, εικονίδια λουκέτου, κριτικές πελατών και αξιόπιστες μεθόδους πληρωμής.

- Αναγνωρίστε και αποφύγετε τις διαδικτυακές απάτες και τις οικονομικές απάτες, συμπεριλαμβανομένων των ψεύτικων ιστότοπων, των προσπαθειών ηλεκτρονικού ψαρέματος (phishing) και των παραπλανητικών προσφορών.

- Προστατεύστε τα προσωπικά και οικονομικά σας δεδομένα χρησιμοποιώντας λογισμικό προστασίας από ιούς, παρακολουθώντας τις συναλλαγές σας και ρυθμίζοντας ειδοποιήσεις για ύποπτες δραστηριότητες.

- Εφαρμόστε ασφαλείς πρακτικές στο διαδίκτυο όταν χρησιμοποιείτε δημόσια δίκτυα, συμπεριλαμβανομένης της κατανόησης των κινδύνων του δημόσιου Wi-Fi και της χρήσης VPN για την ασφάλεια των συνδέσεων.

- Αναπτύξτε ψηφιακή αυτοπεποίθηση και οικονομική ανεξαρτησία εφαρμόζοντας τις δεξιότητες που έχετε αποκτήσει σε πραγματικές καταστάσεις ηλεκτρονικής τραπεζικής και αγορών, με μειωμένο άγχος και αυξημένη εμπιστοσύνη στα ψηφιακά εργαλεία.

4.2 Δομή, περιεχόμενο και μαθησιακά αποτελέσματα

Με την επιτυχή ολοκλήρωση αυτού του μαθήματος, οι μαθητές θα είναι σε θέση να:

- Κατανοήσουν τον τρόπο λειτουργίας των διαδικτυακών τραπεζικών συναλλαγών, να μάθουν τα οφέλη της διαχείρισης λογαριασμών στο διαδίκτυο και να αποκτήσουν μια γενική εικόνα των δημοφιλών τραπεζικών πλατφορμών.
- Να πλοηγούνται σε ιστότοπους ηλεκτρονικού εμπορίου, να μαθαίνουν τα οφέλη των διαδικτυακών αγορών και των δημοφιλών πλατφορμών.
- Να δημιουργούν ισχυρούς κωδικούς πρόσβασης και έλεγχο ταυτότητας δύο παραγόντων (2FA): συμβουλές για τη δημιουργία ισχυρών κωδικών πρόσβασης και τη χρήση 2FA για την αύξηση της ασφάλειας.
- Χρησιμοποιούν με ασφάλεια τραπεζικές εφαρμογές και ιστότοπους: να χρησιμοποιούν μόνο επίσημες εφαρμογές/ιστότοπους, να ελέγχουν την ασφάλεια των συνδέσεων (https).
- Να πραγματοποιούν αγορές σε αξιόπιστους ιστότοπους: να επαληθεύουν την αυθεντικότητα ενός ιστότοπου και να κατανοούν τις κριτικές και τις αξιολογήσεις.
- Αναγνωρίστε τις ασφαλείς επιλογές πληρωμής: προσδιορίστε τις ασφαλείς μεθόδους πληρωμής (πιστωτικές κάρτες) και αποφύγετε τις μη ασφαλείς πληρωμές (τραπεζικές μεταφορές).
- Ασφαλίστε τις συσκευές σας: πώς να χρησιμοποιείτε λογισμικό προστασίας από ιούς και να ενημερώνετε το λογισμικό.
- Ασφαλής χρήση δημόσιων δικτύων Wi-Fi για χρηματοοικονομικές συναλλαγές: κίνδυνοι που συνδέονται με τα δημόσια δίκτυα και χρήση VPN για την εξασφάλιση της ασφάλειας.

4.3 Ατζέντα I Λεπτομερής σχέδιο συνεδρίας

ΕΝΌΤΗΤΑ ΙΙΙ
Συνηθισμένες διαδικτυακές απάτες που στοχεύουν ηλικιωμένους

1η Συνεδρία

Καλωσόρισμα
Διάρκεια 5''

Μαθησιακοί στόχοι

- Εισαγωγή στο θέμα και δημιουργία ενός φιλόξενου περιβάλλοντος.

Περιεχόμενο/Μέθοδος

- Σύντομη εισαγωγή στη συνεδρία, περιγραφή των στόχων και καθορισμός των προσδοκιών. Προετοιμασία του εδάφους για την εκπαίδευση με περιγραφή του ενότητας και της σημασίας της.

Υλικό

- Λευκός πίνακας ή flip chart για τους στόχους της συνεδρίας.
- Μαρκαδόροι.
- Εκτυπωμένη ατζέντα ή διαφάνεια παρουσίασης που περιγράφει τη συνεδρία.

2η Συνεδρία

Δραστηριότητα για το σπάσιμο του πάγου: «Η πρώτη μου εμπειρία με το online banking»
Διάρκεια 10 λεπτά

Μαθησιακοί στόχοι

- Δημιουργήστε σύνδεση μέσω κοινών εμπειριών και εισαγάγετε το θέμα.

Περιεχόμενο/Μέθοδος

- Ο εκπαιδευτής ζητά από τους συμμετέχοντες να μοιραστούν μια σύντομη ιστορία σχετικά με τις πρώτες τους εμπειρίες με τις ηλεκτρονικές τραπεζικές συναλλαγές, συμπεριλαμβανομένου του τι έκαναν και πώς ένιωσαν. Καθώς οι συμμετέχοντες μοιράζονται τις εμπειρίες τους, ο εκπαιδευτής ακούει προσεκτικά και καταγράφει τα βασικά συναισθήματα και σκέψεις σε ένα flipchart ή πίνακα (π.χ. νευρικότητα, ενθουσιασμός, σύγχυση), αποτυπώνοντας οπτικά τις κοινές εμπειρίες και συναισθήματα της ομάδας. Τέλος, ο εκπαιδευτής συνοψίζει εν συντομία τα συναισθήματα και τις εμπειρίες που μοιράστηκαν οι συμμετέχοντες.

Υλικό

- Πίνακας ή λευκός πίνακας για να γράψετε λέξεις-κλειδιά (π.χ. νευρικότητα, ενθουσιασμός), μαρκαδόροι.

3η Συνεδρία

Διάλεξη 1: Κατανόηση των βασικών αρχών των ηλεκτρονικών τραπεζικών συναλλαγών και των ηλεκτρονικών αγορών
Διάρκεια 30

Μαθησιακοί στόχοι

- Βοηθήστε τους συμμετέχοντες να κατανοήσουν πώς λειτουργούν οι ηλεκτρονικές τραπεζικές συναλλαγές και οι ηλεκτρονικές αγορές και να διακρίνουν τις ασφαλείς από τις μη ασφαλείς πλατφόρμες.

Περιεχόμενο/Μέθοδος

- Ο εκπαιδευτής συζητά παραδείγματα φιλικά προς τον χρήστη, όπως το Monzo ή το Revolut (τραπεζικές συναλλαγές) και το Zalando ή το Coolblue (αγορές), επισημαίνοντας βασικά χαρακτηριστικά όπως η ασφάλεια, η πλοήγηση και η ευχρηστία. Για να ενισχύσουν τη μάθησή τους, οι συμμετέχοντες συγκρίνουν έναν πραγματικό ιστότοπο με έναν ψεύτικο, χρησιμοποιώντας τις γνώσεις τους για να εντοπίσουν σημάδια αξιοπιστίας και απάτης.
- Ο εκπαιδευτής παρουσιάζει τα βασικά στοιχεία των ηλεκτρονικών τραπεζικών συναλλαγών και αγορών χρησιμοποιώντας στιγμιότυπα οθόνης και ζωντανές επιδείξεις. Ο εκπαιδευτής καθοδηγεί τους συμμετέχοντες σε μια απλή τραπεζική πλατφόρμα, εξηγώντας τους πώς λειτουργούν οι ηλεκτρονικές τραπεζικές συναλλαγές και δείχνοντάς τους πώς να ελέγχουν το υπόλοιπό τους, να μεταφέρουν χρήματα και να χρησιμοποιούν άλλες βασικές λειτουργίες. Στη συνέχεια, ο εκπαιδευτής κάνει το ίδιο για έναν ιστότοπο αγορών, δείχνοντας στους συμμετέχοντες πώς να πλοηγούνται στην πλατφόρμα, να επιλέγουν προϊόντα και να προχωρούν στη διαδικασία αγοράς. Ο εκπαιδευτής εμφανίζει δύο ιστότοπους - έναν ασφαλή και έναν ψεύτικο - και ζητά από τους συμμετέχοντες να προσδιορίσουν ποιος είναι ασφαλής και να εξηγήσουν γιατί, ενθαρρύνοντάς τους να εφαρμόσουν τις γνώσεις τους σχετικά με την ασφάλεια των ιστότοπων. Στο τέλος, ο εκπαιδευτής συζητά τα βασικά συμπεράσματα της συνεδρίας: τη σημασία του ελέγχου των ασφαλών συνδέσεων (HTTPS), την αναγνώριση των νόμιμων πλατφορμών και τους τρόπους αποφυγής των απάτων.

Υλικό

- Παρουσίαση PowerPoint, οπτικά φυλλάδια,
- φορητός υπολογιστής, προβολέας.

Δραστηριότητα 1: Εξερεύνηση πλατφόρμας
Διάρκεια 20

Μαθησιακοί στόχοι

- Εξάσκηση στη χρήση διαδικτυακών πλατφορμών και αναγνώριση βασικών χαρακτηριστικών.

Περιεχόμενο/Μέθοδος

- Ο εκπαιδευτής χωρίζει τους συμμετέχοντες σε ζευγάρια και δίνει σε κάθε ζευγάρι μία κάρτα εργασίας, ενημερώνοντάς τους ότι κάθε κάρτα περιέχει οδηγίες για το τι πρέπει να αναζητήσουν κατά τη διάρκεια της άσκησης, π.χ. αναγνώριση χαρακτηριστικών ασφαλείας

σε έναν ιστότοπο τραπεζικών συναλλαγών ή αγορών. Μόλις ξεκινήσει η άσκηση, ο εκπαιδευτής περιφέρεται στην αίθουσα, παρατηρώντας τους συμμετέχοντες, δίνοντας συμβουλές και απαντώντας σε ερωτήσεις. Ο εκπαιδευτής βοηθά επίσης τους συμμετέχοντες να επικεντρωθούν σε βασικά στοιχεία ασφαλείας, όπως εικονίδια λουκέτου, ρυθμίσεις 2FA, διευθύνσεις «https» ή σύμβολα ασφαλούς πληρωμής, για να βεβαιωθεί ότι κατανοούν πώς να αναγνωρίζουν τα χαρακτηριστικά ασφαλείας. Μετά την άσκηση, ο εκπαιδευτής θα ζητήσει από κάθε ζευγάρι να μοιραστεί εν συντομία τα ευρήματά του κατά τη διάρκεια της έρευνας. Ο εκπαιδευτής ενθαρρύνει μια σύντομη συζήτηση, θέτοντας ερωτήσεις όπως «Τι ήταν εύκολο και τι ήταν δύσκολο στην άσκηση;» και «Τι σας έκανε να θεωρήσετε έναν ιστότοπο ή μια εφαρμογή ασφαλή ή μη ασφαλή;». Αυτό θα βοηθήσει τους συμμετέχοντες να αναστοχαστούν τις εμπειρίες τους και να εμβαθύνουν την κατανόησή τους για το τι κάνει μια διαδικτυακή πλατφόρμα ασφαλή.

- Τέλος, ο εκπαιδευτής παρέχει πρόσθετους πόρους, μοιράζοντας συνδέσμους προς σύντομα άρθρα ή βίντεο σχετικά με την ασφάλεια των διαδικτυακών πλατφορμών. Θα διανεμηθούν επίσης έντυπα υλικά που περιέχουν παραδείγματα ασφαλών και μη ασφαλών στοιχείων ιστότοπων/εφαρμογών, τα οποία θα χρησιμεύσουν ως υλικό αναφοράς και θα ενισχύσουν τις γνώσεις που αποκτήθηκαν κατά τη διάρκεια της άσκησης.

Υλικό

- Εκτυπωμένοι οδηγοί εργασιών για τους συμμετέχοντες.
- Τάμπλετ, φορητοί υπολογιστές ή μεγάλα εκτυπωμένα στιγμιότυπα οθόνης με δοκιμαστικές εκδόσεις τραπεζικών ή εμπορικών πλατφορμών.

Διάλειμμα | Διάρκεια *5’*

- **Δώστε χρόνο στους συμμετέχοντες να αναζωογονηθούν και να σκεφτούν.**
- **Σύντομο διάλειμμα για ανανέωση.**

4η Συνεδρία

Διάλεξη 2: Ασφαλείς πρακτικές ηλεκτρονικής τραπεζικής
Διάρκεια 30’’

Μαθησιακοί στόχοι

- Να βοηθήσει τους συμμετέχοντες να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και να παρακολουθούν τους λογαριασμούς τους.

Περιεχόμενο/Μέθοδος

- Ο εκπαιδευτής ξεκινά με μια παρουσίαση που καλύπτει τις βασικές πρακτικές ασφάλειας στις ηλεκτρονικές τραπεζικές συναλλαγές. Τα θέματα που θα συζητηθούν περιλαμβάνουν τη δημιουργία ισχυρών κωδικών πρόσβασης, την ενεργοποίηση της επαλήθευσης δύο παραγόντων (2FA) και τη ρύθμιση ειδοποιήσεων λογαριασμού. Ο εκπαιδευτής θα συμπεριλάβει στην διάλεξη πραγματικά παραδείγματα ή σύντομες ιστορίες σχετικά με την απάτη στις ηλεκτρονικές τραπεζικές συναλλαγές. Χρησιμοποιώντας πραγματικές περιπτώσεις απάτης, ο εκπαιδευτής επισημαίνει τις κοινές απειλές και μοιράζεται πρακτικές συμβουλές

ασφάλειας. Μια τέτοια περίπτωση είναι η απάτη «Safe Account» που αναφέρθηκε στην Ιρλανδία, η οποία βοηθά να κατανοήσουμε πώς λειτουργεί η απάτη στην πράξη. Οι συμμετέχοντες ενθαρρύνονται να εφαρμόσουν αυτά τα βήματα στις δικές τους συσκευές, καθιστώντας τη συνεδρία πρακτική, χρήσιμη και άμεσα εφαρμόσιμη.

- Ο εκπαιδευτής εξηγεί στους συμμετέχοντες γιατί είναι απαραίτητη η ασφαλής ηλεκτρονική τραπεζική και πόσο συχνά συμβαίνουν παραβιάσεις ασφαλείας. Επισημαίνει τους πιθανούς κινδύνους και δείχνει πώς απλές προφυλάξεις μπορούν να προστατεύσουν τους συμμετέχοντες από την απάτη. Χρησιμοποιώντας ένα εργαλείο ελέγχου ισχύος κωδικού πρόσβασης, ο εκπαιδευτής δείχνει σε πραγματικό χρόνο τη διαφορά μεταξύ αδύναμων και ισχυρών κωδικών πρόσβασης. Ο εκπαιδευτής ζητά από τους συμμετέχοντες να προτείνουν δείγματα κωδικών πρόσβασης και τα δοκιμάζει ζωντανά για να τονίσει τη σημασία της δημιουργίας ισχυρών, μοναδικών κωδικών πρόσβασης. Στη συνέχεια, δείχνει πώς να ενεργοποιήσετε το 2FA χρησιμοποιώντας στιγμιότυπα οθόνης ή ζωντανές προσομοιώσεις. Ο εκπαιδευτής εξηγεί τον ρόλο της 2FA στην πρόληψη της μη εξουσιοδοτημένης πρόσβασης και καθοδηγεί τους συμμετέχοντες στη διαδικασία ενεργοποίησής της. Στη συνέχεια, ο εκπαιδευτής θα εξηγήσει πώς να παρακολουθείτε τη τραπεζική δραστηριότητα και να ρυθμίζετε ειδοποιήσεις για ύποπτες συναλλαγές. Χρησιμοποιώντας στιγμιότυπα οθόνης ή ένα δείγμα τραπεζικής εφαρμογής, ο εκπαιδευτής θα καθοδηγήσει τους συμμετέχοντες στα βήματα για τη ρύθμιση αυτών των ειδοποιήσεων, τονίζοντας τη σημασία της επαγρύπνησης σχετικά με τη δραστηριότητα του λογαριασμού. Κατά τη διάρκεια της συνεδρίας ερωτήσεων και απαντήσεων, ο εκπαιδευτής θα ζητήσει από τους συμμετέχοντες να μοιραστούν τις εμπειρίες ή τις ανησυχίες τους σχετικά με την ασφάλεια των ηλεκτρονικών τραπεζικών συναλλαγών. Τέλος, ο εκπαιδευτής θα διανείμει έντυπες λίστες ελέγχου που συνοψίζουν τις ασφαλείς συνήθειες ηλεκτρονικής τραπεζικής, οι οποίες θα αποτελέσουν χρήσιμο βοήθημα για τους συμμετέχοντες.

Υλικό

- Παρουσίαση, εργαλείο επίδειξης ισχύος κωδικού πρόσβασης.
- Εκτυπωμένη λίστα ελέγχου.

Δραστηριότητα 2: Ασφαλίστε τις ηλεκτρονικές τραπεζικές συναλλαγές σας
Διάρκεια 20

Μαθησιακοί στόχοι

- Οι συμμετέχοντες εξασκούνται στη ρύθμιση της 2FA και στην παρακολούθηση συναλλαγών σε ένα προσομοιωμένο τραπεζικό περιβάλλον.

Περιεχόμενο/Μέθοδος

- Ο εκπαιδευτής χωρίζει τους συμμετέχοντες σε ζευγάρια ή μικρές ομάδες. Κάθε ομάδα θα εργαστεί σε φορητούς υπολογιστές ή smartphone με εγκατεστημένες εφαρμογές επίδειξης ή τραπεζικές πλατφόρμες, όπως Revolut ή Monzo. Ο εκπαιδευτής καθοδηγεί τους συμμετέχοντες στη διαδικασία ενεργοποίησης της 2FA: Χρησιμοποιώντας έναν οδηγό βήμα προς βήμα, βοηθά τους συμμετέχοντες να ολοκληρώσουν τη διαδικασία ρύθμισης της 2FA

στην πλατφόρμα επίδειξης. Περιφέρεται στην αίθουσα για να προσφέρει βοήθεια και να βεβαιωθεί ότι όλοι ακολουθούν σωστά τα βήματα. Στη συνέχεια, ο εκπαιδευτής ζητά από τους συμμετέχοντες να ελέγξουν για τυχόν μη εξουσιοδοτημένες συναλλαγές και τους βοηθά να ρυθμίσουν ειδοποιήσεις για ύποπτες δραστηριότητες. Βεβαιώνεται ότι οι συμμετέχοντες κατανοούν τη διαδικασία και εκτελούν αυτά τα βήματα στην πλατφόρμα επίδειξης.

- Μετά την άσκηση, ζητήστε από κάθε ομάδα να μοιραστεί τις εμπειρίες της: «Ποιες δυσκολίες αντιμετωπίσατε κατά τη ρύθμιση της 2FA;» «Μπορέσατε να βρείτε και να ρυθμίσετε ειδοποιήσεις για συναλλαγές; Ποια βήματα ήταν χρήσιμα και ποια ήταν δύσκολα;» Παρέχει ανατροφοδότηση: Τονίζει τη σημασία της ενεργοποίησης της 2FA και της παρακολούθησης των συναλλαγών για την ασφάλεια των ηλεκτρονικών τραπεζικών συναλλαγών.

Υλικό

- Φορητοί υπολογιστές ή smartphone.
- Εφαρμογή τραπεζικών συναλλαγών για επίδειξη.
- Οδηγός βήμα προς βήμα για τη ρύθμιση της 2FA και την προβολή των συναλλαγών.

Διάλειμμα | Διάρκεια *5'*

- **Δώστε χρόνο για ξεκούραση και προετοιμασία**
- **Ένα σύντομο διάλειμμα για να αναζωογονηθείτε.**

5η Συνεδρία

Διάλεξη 3: Ασφαλείς αγορές στο διαδίκτυο
Διάρκεια 30''

Μαθησιακοί στόχοι

- Να βοηθήσει τους ηλικιωμένους να κατανοήσουν πώς να αξιολογούν ιστότοπους, να αναγνωρίζουν ασφαλείς επιλογές πληρωμής και να εντοπίζουν απατεώνες πωλητές.

Περιεχόμενο/Μέθοδος

- Κατά τη διάρκεια της διάλεξης, ο εκπαιδευτής εξηγεί πώς να αναγνωρίζουν ασφαλείς ιστότοπους για ηλεκτρονικές αγορές και να επαληθεύουν την αυθεντικότητα των πωλητών. Ο εκπαιδευτής εξηγεί πώς να αναγνωρίζουν ασφαλείς ιστότοπους, εστιάζοντας στο πρωτόκολλο HTTPS, στα εικονίδια με το λουκέτο και σε άλλα σύμβολα ασφαλείας. Παρουσιάζει παραδείγματα καλών και κακών ιστότοπων για να δείξει πώς να αξιολογούν την αξιοπιστία τους. Ο εκπαιδευτής δείχνει επίσης πώς να διαβάζουν κριτικές και να ελέγχουν αν οι πωλητές είναι γνήσιοι. Στο τέλος της διάλεξης, ο εκπαιδευτής θέτει στους συμμετέχοντες ερωτήσεις όπως «Τι λέει το πρωτόκολλο HTTPS για την ασφάλεια των ιστότοπων;» και «Πώς μπορείτε να ελέγξετε αν ένας διαδικτυακός πωλητής είναι αξιόπιστος;» για να ενισχύσει τις βασικές έννοιες και να εμπλέξει τους συμμετέχοντες.
- Στο τέλος, ο εκπαιδευτής ενθαρρύνει τους συμμετέχοντες να μοιραστούν τις εμπειρίες τους από τις διαδικτυακές αγορές ή τις ανησυχίες τους σχετικά με την ασφάλεια των διαδικτυακών αγορών. Θα συζητηθούν τυχόν προβλήματα που ενδέχεται να έχουν αντιμετωπίσει οι

συμμετέχοντες κατά τη διάρκεια των διαδικτυακών αγορών τους και ο εκπαιδευτής θα απαντήσει σε τυχόν ερωτήσεις τους.

Υλικό

- Εκτυπωμένα παραδείγματα αγορών, στιγμιότυπα οθόνης ιστότοπων.

Δραστηριότητα 3: Αγορές από αξιόπιστους ιστότοπους
Διάρκεια 20

Μαθησιακοί στόχοι

- Οι συμμετέχοντες μαθαίνουν πώς να αξιολογούν την ασφάλεια των ηλεκτρονικών καταστημάτων και να επαληθεύουν τις μεθόδους πληρωμής.

Περιεχόμενο/Μέθοδος

- Σε ομάδες, οι συμμετέχοντες εξοικειώνονται πρώτα με τον νόμιμο ιστότοπο του καταστήματος για να εντοπίσουν βασικά χαρακτηριστικά ασφαλείας (π.χ. HTTPS, σφραγίδες εμπιστοσύνης, ασφαλείς επιλογές πληρωμής). Στη συνέχεια, με τη χρήση παρουσίασης ή προηχογραφημένου βίντεο, τους παρουσιάζονται παραδείγματα ψεύτικων ιστότοπων ή ύποπτων διαδικτυακών δραστηριοτήτων. Η άσκηση εστιάζει στο να τους βοηθήσει να αναγνωρίσουν κοινά προειδοποιητικά σημάδια και να συγκρίνουν ασφαλείς και μη ασφαλείς ιστότοπους.
- Ο εκπαιδευτής χωρίζει τους συμμετέχοντες σε μικρές ομάδες και τους δίνει μια λίστα με ιστότοπους για να εξετάσουν. Κάθε ομάδα αξιολογεί τους ιστότοπους ως προς την ασφάλειά τους, εστιάζοντας σε δείκτες όπως το πρωτόκολλο HTTPS, τις ασφαλείς μεθόδους πληρωμής και τις αξιόπιστες κριτικές. Ο εκπαιδευτής περιφέρεται μεταξύ των ομάδων, παρέχοντας βοήθεια όποτε χρειάζεται και προσφέροντας καθοδήγηση αν οι ομάδες χρειάζονται βοήθεια για να εντοπίσουν προειδοποιητικά σημάδια, όπως ύποπτες κριτικές ή μη ασφαλή στοιχεία ιστότοπων. Στο τέλος, οι ομάδες μοιράζονται πληροφορίες σχετικά με τους ιστότοπους που κρίθηκαν ασφαλείς και αιτιολογούν την αξιολόγησή τους.

Υλικό

- Υπολογιστές με πρόσβαση στο διαδίκτυο.
- Λίστα ιστότοπων αγορών.

Διάλειμμα | Διάρκεια 5’

- **Δώστε χρόνο για ξεκούραση και προετοιμασία.**
- **Σύντομο διάλειμμα για αναζωογόνηση.**

6η Συνεδρία

Διάλεξη 4: Προστασία προσωπικών και οικονομικών πληροφοριών
Διάρκεια 30''

Μαθησιακοί στόχοι

- Εξοπλισμός των ηλικιωμένων με γνώσεις σχετικά με την ασφάλεια των συσκευών, τη χρήση λογισμικού προστασίας από ιούς και την ασφάλεια των συνδέσεων Wi-Fi.

Περιεχόμενο/Μέθοδος

- Ο εκπαιδευτής δίνει μια διάλεξη στην οποία εξηγεί τις έννοιες του λογισμικού προστασίας από ιούς, των VPN και της ασφαλούς περιήγησης στο διαδίκτυο. Η παρουσίαση θα περιλαμβάνει διαφάνειες με βασικές πληροφορίες και παραδείγματα για κάθε θέμα, επισημαίνοντας τις βέλτιστες πρακτικές για την ασφάλεια των συσκευών. Ο εκπαιδευτής δείχνει πώς να ενημερώνετε τις συσκευές, να εγκαθιστάτε λογισμικό προστασίας από ιούς και να διαχειρίζεστε τις ρυθμίσεις απορρήτου για να βελτιώσετε την ασφάλεια. Παρουσιάζει ένα σύντομο εκπαιδευτικό βίντεο που δείχνει τη σωστή χρήση ενός VPN για ασφαλή περιήγηση στο διαδίκτυο. Καθ' όλη τη διάρκεια της διάλεξης, ο εκπαιδευτής θα ενθαρρύνει τους συμμετέχοντες να συμμετέχουν ενεργά και θα κάνει τη συνεδρία διαδραστική, θέτοντας ερωτήσεις και παρέχοντας παραδείγματα από την πραγματική ζωή για το πώς να παραμένετε ασφαλείς στο διαδίκτυο. Μετά τη διάλεξη, οι συμμετέχοντες θα έχουν την ευκαιρία να υποβάλουν ερωτήσεις και να διευκρινίσουν τυχόν αμφιβολίες που μπορεί να έχουν σχετικά με την ασφάλεια των συσκευών και την προστασία στο διαδίκτυο.
- Τέλος, ο εκπαιδευτής θα μοιραστεί απλές, καθημερινές πρακτικές για την προστασία των προσωπικών δεδομένων, όπως η αποφυγή ύποπτων συνδέσμων, η μη κοινοποίηση υπερβολικών πληροφοριών σε ιστότοπους και η αναγνώριση κοινών παγίδων στο διαδίκτυο. Αυτά τα βήματα βοηθούν τους συμμετέχοντες να αναπτύξουν ασφαλέστερες ψηφιακές συνήθειες.

Υλικό

- Διαφάνειες παρουσίασης, βίντεο με οδηγίες για τα VPN.

Δραστηριότητα 4: Ασφάλεια των συσκευών σας
Διάρκεια 20

Μαθησιακοί στόχοι

- Οι συμμετέχοντες εξασκούνται στην εγκατάσταση λογισμικού προστασίας από ιούς, στη χρήση VPN και στη διαχείριση των ρυθμίσεων απορρήτου.

Περιεχόμενο/Μέθοδος

- Οι συμμετέχοντες εργάζονται σε ομάδες για να εγκαταστήσουν λογισμικό προστασίας από ιούς, να ενεργοποιήσουν VPN για ασφαλή περιήγηση στο διαδίκτυο και να ελέγξουν τις ρυθμίσεις απορρήτου σε εφαρμογές και μέσα κοινωνικής δικτύωσης. Αυτή η πρακτική άσκηση τους βοηθά να εφαρμόσουν πρακτικά μέτρα για την προστασία των συσκευών και των προσωπικών τους δεδομένων στο διαδίκτυο.

- Ο εκπαιδευτής χωρίζει τους συμμετέχοντες σε μικρές ομάδες ή ζευγάρια και τους παρέχει φορητούς υπολογιστές, λογισμικό προστασίας από ιούς και εφαρμογές VPN για χρήση κατά τη διάρκεια της άσκησης. Κάθε ομάδα θα ακολουθήσει τις αναλυτικές οδηγίες που παρέχει ο εκπαιδευτής για την εγκατάσταση λογισμικού προστασίας από ιούς, την ενεργοποίηση VPN για ασφαλή περιήγηση στο διαδίκτυο και τον έλεγχο των ρυθμίσεων απορρήτου σε εφαρμογές και λογαριασμούς κοινωνικών μέσων. Ο εκπαιδευτής κυκλοφορεί μεταξύ των ομάδων, προσφέροντας βοήθεια όποτε χρειάζεται και διασφαλίζοντας ότι όλοι οι συμμετέχοντες μπορούν να ολοκληρώσουν με επιτυχία τις εργασίες. Ο εκπαιδευτής καθοδηγεί επίσης τις ομάδες στη διαδικασία αναγνώρισης των βασικών ρυθμίσεων απορρήτου στις συσκευές και τα προφίλ κοινωνικών μέσων τους που ενισχύουν την ασφάλεια. Μετά την άσκηση, ο εκπαιδευτής ζητά από τους συμμετέχοντες να μοιραστούν τις εμπειρίες τους σχετικά με την ασφάλεια των συσκευών και τις ρυθμίσεις απορρήτου τους.

Υλικό

- Φορητοί υπολογιστές, λογισμικό προστασίας από ιούς, εφαρμογή VPN

7η Συνεδρία

Συζήτηση | Διάρκεια 10’’

Μαθησιακοί στόχοι

- Σκεφτείτε τα βασικά συμπεράσματα της συνεδρίας και διευκρινίστε τυχόν απορίες.

Περιεχόμενο/Μέθοδος

- Ομαδική συζήτηση κατά την οποία οι συμμετέχοντες μοιράζονται τις εμπειρίες και τα συμπεράσματά τους. Ο εκπαιδευτής απαντά σε τυχόν απορίες. Ενθαρρύνει τους συμμετέχοντες να συνεχίσουν να εξασκούν τις δεξιότητες που απέκτησαν κατά τη διάρκεια της συνεδρίας.

Σύνοψη
Διάρκεια 5

Μαθησιακοί στόχοι

- Συνοψίστε τη συνεδρία και ενθαρρύνετε τους συμμετέχοντες να συνεχίσουν να εξασκούν με ασφάλεια.

Περιεχόμενο/Μέθοδος

- Ο εκπαιδευτής συνοψίζει τη συνεδρία, επισημαίνοντας τα πιο σημαντικά θέματα που συζητήθηκαν. Οι συμμετέχοντες θα ενθαρρυνθούν να συνεχίσουν να εξασκούν τις δεξιότητες που απέκτησαν μέσω των προσωπικών τους δραστηριοτήτων στο διαδίκτυο. Ο εκπαιδευτής ευχαριστεί τους συμμετέχοντες για τη συμμετοχή τους και τους ενθαρρύνει να χρησιμοποιήσουν τις γνώσεις που απέκτησαν για να διασφαλίσουν την ασφάλειά τους στο διαδίκτυο.

Υλικό

- ❖ Φυλλάδια με τα βασικά σημεία και τους πόρους.

4.4 Πρόσθετες πληροφορίες

4.4.1 Αυτοανασκόπηση των εκπαιδευτών

- ➢ Ποια στοιχεία της εκπαίδευσης πήγαν ιδιαίτερα καλά;
- ➢ Ποια μέρη της συνεδρίας ήταν πιο δύσκολα για μένα;
- ➢ Πόσο ενεργά συμμετείχαν και ανταποκρίθηκαν οι συμμετέχοντες κατά τη διάρκεια των δραστηριοτήτων;
- ➢ Κατάφεραν οι συμμετέχοντες να επιτύχουν τους μαθησιακούς στόχους; Αν όχι, γιατί;
- ➢ Ποιες προσαρμογές θα μπορούσαν να βελτιώσουν τη συνεδρία σε μελλοντικές επαναλήψεις;

4.4.2 Αξιολόγηση του προγράμματος από τους εκπαιδευτές

- ➢ Ήταν το περιεχόμενο της εκπαίδευσης σχετικό με τις ανάγκες των ηλικιωμένων και προσαρμοσμένο στο επίπεδο γνώσεων και ψηφιακής εμπειρίας τους;
- ➢ Κατάλαβαν οι συμμετέχοντες τις βασικές αρχές του ηλεκτρονικού τραπεζικού συστήματος, του ηλεκτρονικού εμπορίου, της ασφάλειας στον κυβερνοχώρο και της ιδιωτικότητας στο διαδίκτυο;
- ➢ Ήταν οι πρακτικές ασκήσεις, τα κουίζ και οι επιδείξεις αποτελεσματικά στην ενίσχυση της μάθησης και στην ανάπτυξη της ψηφιακής αυτοπεποίθησης;
- ➢ Οι συζητήσεις και οι προβληματισμοί επέτρεψαν στους συμμετέχοντες να εμβαθύνουν την κατανόησή τους σχετικά με τις ασφαλείς διαδικτυακές πρακτικές;
- ➢ Επιτεύχθηκαν τα επιδιωκόμενα μαθησιακά αποτελέσματα, όπως η ικανότητα δημιουργίας ισχυρών κωδικών πρόσβασης, αναγνώρισης ψευδών ιστότοπων, παρακολούθησης συναλλαγών και διαμόρφωσης ρυθμίσεων ασφαλείας;
- ➢ Έδειξαν οι συμμετέχοντες αυξημένη εμπιστοσύνη και ανεξαρτησία στην εκτέλεση εργασιών ηλεκτρονικής τραπεζικής και αγορών;
- ➢ Ποιοι τομείς της εκπαίδευσης ήταν οι πιο επιτυχημένοι και ποιοι τομείς θα μπορούσαν να βελτιωθούν για μελλοντικές συνεδρίες;

4.4.3 Υλικό, πρόσθετοι πόροι

Παράρτημα 1 | Χαρακτηριστικά ισχυρών κωδικών πρόσβασης

Για να διασφαλίσετε την ασφάλεια των διαδικτυακών λογαριασμών σας, ο κωδικός πρόσβασής σας πρέπει να έχει τα ακόλουθα χαρακτηριστικά:

- Τουλάχιστον 8 χαρακτήρες – όσο μεγαλύτερος, τόσο καλύτερος
- Συνδυασμός κεφαλαίων και μικρών γραμμάτων
- Συνδυασμός γραμμάτων και αριθμών
- Περιλαμβάνει τουλάχιστον ένα ειδικό χαρακτήρα, π.χ. !, @, #, ?,]
- Σημείωση: Μην χρησιμοποιείτε < ή > στον κωδικό πρόσβασής σας, καθώς αυτά μπορεί να προκαλέσουν προβλήματα στους περιηγητές ιστού
- Λεπτομερείς οδηγίες βρίσκονται παρακάτω!

Ασφάλεια στις ηλεκτρονικές τραπεζικές συναλλαγές και τις αγορές
Χαρακτηριστικά ισχυρών κωδικών πρόσβασης
Γιατί είναι σημαντικοί οι ισχυροί κωδικοί πρόσβασης

Η δημιουργία ισχυρών κωδικών πρόσβασης είναι ένα βασικό βήμα για την προστασία των προσωπικών και επαγγελματικών σας δεδομένων. Οι αδύναμοι κωδικοί πρόσβασης διευκολύνουν τους χάκερ να έχουν πρόσβαση στους λογαριασμούς σας.

Χρησιμοποιήστε τις παρακάτω οδηγίες για να δημιουργήσετε ασφαλείς κωδικούς πρόσβασης:

<u>Χαρακτηριστικά ισχυρών κωδικών πρόσβασης</u>

- Τουλάχιστον 8 χαρακτήρες – όσο περισσότερο μακρύς, τόσο καλύτερος.
- Συνδυασμός κεφαλαίων και μικρών γραμμάτων.
- Μίγμα γραμμάτων και αριθμών.
- Τουλάχιστον ένας ειδικός χαρακτήρας, όπως: !, @, #, ?,].
- Αποφύγετε τη χρήση των χαρακτήρων < ή > στον κωδικό πρόσβασής σας, καθώς μπορεί να προκαλέσουν προβλήματα σε ορισμένους περιηγητές ιστού.
- Πρόσθετες συμβουλές
- Μην χρησιμοποιείτε προσωπικές πληροφορίες (όπως το όνομά σας ή την ημερομηνία γέννησής σας).
- Χρησιμοποιήστε έναν μοναδικό κωδικό πρόσβασης για κάθε λογαριασμό.
- Εξετάστε το ενδεχόμενο να χρησιμοποιήσετε έναν αξιόπιστο διαχειριστή κωδικών πρόσβασης.
- Αλλάζετε τακτικά τους κωδικούς πρόσβασης και αποφύγετε να επαναχρησιμοποιείτε παλιούς.

Ενότητα πρακτικής (προαιρετική)
Δημιουργήστε έναν ισχυρό κωδικό πρόσβασης χρησιμοποιώντας τις παραπάνω συμβουλές:

Αξιολογήστε την ισχύ του κωδικού πρόσβασής σας:

ΑΔΥΝΑΜΟΣ	ΜΕΣΗ	ΙΣΧΥΡΟΣ

Παράρτημα 2| Οδηγίες βήμα προς βήμα για 2FA και ειδοποιήσεις

Μέρος Ι: *Ρύθμιση της επαλήθευσης δύο παραγόντων (2FA)*

Σκοπός: *Η 2FA παρέχει επιπλέον ασφάλεια, απαιτώντας τόσο τον κωδικό πρόσβασής σας όσο και μια δεύτερη μέθοδο επαλήθευσης (π.χ. κωδικό που αποστέλλεται στο τηλέφωνό σας).*

Βήματα

1. Ανοίξτε την εφαρμογή ή την πλατφόρμα demo banking στη συσκευή σας.
2. Μεταβείτε στις Ρυθμίσεις → Ρυθμίσεις ασφαλείας.
3. Πατήστε Ενεργοποίηση ελέγχου ταυτότητας δύο παραγόντων (2FA).
4. Επιλέξτε τη μέθοδο επαλήθευσης:
- Κωδικός SMS
- Εφαρμογή επαλήθευσης (π.χ. Google Authenticator)
5. Ακολουθήστε τις οδηγίες (εισαγάγετε τον κωδικό επαλήθευσης που λάβατε).
6. Βεβαιωθείτε ότι η 2FA είναι ενεργή και λειτουργεί.

Μέρος 2*: Ελέγξτε τις συναλλαγές και ρυθμίστε ειδοποιήσεις*

Σκοπός: *Η παρακολούθηση των συναλλαγών σας και η ρύθμιση ειδοποιήσεων σας βοηθά να εντοπίσετε έγκαιρα ύποπτες δραστηριότητες.*

Βήματα:

7. Μεταβείτε στο Ιστορικό συναλλαγών στην εφαρμογή.
8. Ελέγξτε τις πρόσφατες συναλλαγές.
9. Εντοπίστε και επισημάνετε οτιδήποτε σας φαίνεται άγνωστο.
10. Μεταβείτε στις Ρυθμίσεις ειδοποιήσεων ή προειδοποιήσεων.
11. Ενεργοποιήστε τις ειδοποιήσεις για:
- Μεγάλες ή ασυνήθιστες συναλλαγές
- Συνδέσεις από νέες συσκευές
- Αλλαγές στις ρυθμίσεις του λογαριασμού σας

Σημαντικές υπενθυμίσεις

- *Ενεργοποιήστε την επαλήθευση δύο παραγόντων (2FA) σε όλες τις χρηματοοικονομικές εφαρμογές.*
- *Ελέγχετε τακτικά το ιστορικό των συναλλαγών σας.*
- *Χρησιμοποιήστε ειδοποιήσεις για να ενημερώνεστε για ασυνήθιστες δραστηριότητες.*

Παράρτημα 3| Αναγνώριση στοιχείων ασφαλείας σε τραπεζικές πλατφόρμες και πλατφόρμες ηλεκτρονικών αγορών

Εργασία 1. Βρείτε το υπόλοιπο του λογαριασμού

Προσπαθήστε να εντοπίσετε το σημείο όπου μπορείτε να ελέγξετε το υπόλοιπο του λογαριασμού.

- Πού βρίσκεται; .....
- Πώς ονομάζεται (π.χ. «Υπόλοιπο», «Επισκόπηση λογαριασμού», «Διαθέσιμα χρήματα»); .....

Εργασία 2. Βρείτε την επιλογή πληρωμής

Προσπαθήστε να βρείτε πού μπορείτε να πραγματοποιήσετε μια πληρωμή ή να ολοκληρώσετε μια αγορά.

- Ποιο είναι το όνομα αυτής της επιλογής;
  ☐ Μεταφορά
  ☐ Πληρωμή
  ☐ Καλάθι / Ταμείο
  ☐ Άλλο: .....
- Ήταν εύκολο να το βρείτε;
  ☐ Ναι
  ☐ Όχι
  Γιατί; .....

Εργασία 3. Προσδιορίστε τα χαρακτηριστικά ασφαλείας του ιστότοπου

Εξετάστε προσεκτικά τον ιστότοπο και σημειώστε τα στοιχεία που υποδηλώνουν ότι είναι ασφαλής.

☐ Εικονίδιο κλειδώματος στη γραμμή διευθύνσεων του προγράμματος περιήγησης
☐ διεύθυνση που ξεκινά με **https**
☐ αναγνωρίσιμα λογότυπα συστημάτων πληρωμών (π.χ. Visa, Mastercard, PayPal, BLIK)
☐ πρόσθετη επιβεβαίωση πληρωμής (κωδικός SMS, τραπεζική εφαρμογή)
☐ πληροφορίες σχετικά με την πολιτική απορρήτου

Παρατηρήσατε κάτι άλλο; .....

Εργασία 4. Αναζητήστε πιθανά προειδοποιητικά σημάδια

Παρατηρήσατε κάτι που θα μπορούσε να υποδηλώνει ότι ο ιστότοπος δεν είναι ασφαλής;

☐ απουσία εικονιδίου κλειδώματος
☐ ύποπτη διεύθυνση ιστότοπου
☐ πάρα πολλά αναδυόμενα παράθυρα
☐ αιτήματα για υπερβολικά πολλές προσωπικές πληροφορίες
☐ άλλο: .....

Εργασία 5. Ελέγξτε τις πρόσθετες ρυθμίσεις ασφαλείας

Αναζητήστε πληροφορίες σχετικά με πρόσθετη προστασία λογαριασμού ή πληρωμών.

Βρήκατε:
☐ έλεγχο ταυτότητας δύο παραγόντων (2FA)
☐ επαλήθευση μέσω SMS
☐ επιβεβαίωση μέσω τραπεζικής εφαρμογής

Πού βρίσκεται αυτή η επιλογή; .....

Περίληψη άσκησης:
Ποιο ήταν το ευκολότερο μέρος της άσκησης; .....
Ποιο ήταν το πιο δύσκολο μέρος; .....
Τι σας βοηθά να αναγνωρίσετε ότι ένας ιστότοπος ή μια εφαρμογή είναι ασφαλής;
.....

Συμπέρασμα: Η ασφαλής χρήση των πλατφορμών ηλεκτρονικής τραπεζικής και ηλεκτρονικών αγορών απαιτεί προσοχή στους δείκτες ασφάλειας του ιστότοπου, στη διεύθυνση του ιστότοπου και στον τρόπο επιβεβαίωσης των πληρωμών.

Να θυμάστε: Εάν κάτι σε έναν ιστότοπο σας κάνει να αισθάνεστε αβέβαιοι ή ύποπτοι, **μην εισάγετε τα προσωπικά σας δεδομένα και διακόψτε τη διαδικασία.**

Παράρτημα 4 | Προτάσεις για περαιτέρω ανάγνωση και μάθηση για τους συμμετέχοντες

Ιστοσελίδες για την ασφάλεια στον κυβερνοχώρο: Ευρωπαϊκοί και κυβερνητικοί οργανισμοί που ασχολούνται με την ασφάλεια στον κυβερνοχώρο

1) **Πώς να ρυθμίσετε την επαλήθευση δύο παραγόντων σε όλους τους διαδικτυακούς λογαριασμούς σας**
   Ιστότοπος: https://www.loginradius.com/blog/identity/how-to-setup-2fa-in-online-accounts/
   Αυτός ο ολοκληρωμένος οδηγός εξηγεί τη σημασία της επαλήθευσης δύο παραγόντων (2FA) και παρέχει αναλυτικές οδηγίες για τη ρύθμισή της σε διάφορους διαδικτυακούς λογαριασμούς, όπως ηλεκτρονικό ταχυδρομείο, μέσα κοινωνικής δικτύωσης και τραπεζικές πλατφόρμες. Καλύπτει μεθόδους όπως κωδικοί SMS, εφαρμογές επαλήθευσης και κλειδιά ασφαλείας υλικού για την ενίσχυση της ασφάλειας των λογαριασμών.

2) **Ρύθμιση της επαλήθευσης δύο παραγόντων | Υπηρεσίες τεχνολογικής υποστήριξης**
   Ιστοσελίδα: https://it.nmu.edu/docs/setting-2-factor-authentication
   Αυτός ο πόρος από το τμήμα πληροφορικής του Πανεπιστημίου Northern Michigan περιγράφει τη διαδικασία ενεργοποίησης της επαλήθευσης δύο παραγόντων (2FA) σε υπηρεσίες του NMU, όπως το MyNMU και το MyUser. Προσφέρει πολλαπλές επιλογές επαλήθευσης, συμπεριλαμβανομένων εφαρμογών επαλήθευσης, κλειδιών ασφαλείας USB και κωδικών ασφαλείας, για να εξασφαλίσει την ασφαλή πρόσβαση στα συστήματα του πανεπιστημίου.

3) **Προειδοποίηση της Τράπεζας της Ιρλανδίας για αύξηση των περιπτώσεων απάτης με «ασφαλείς λογαριασμούς»**
Άρθρο: https://www.rte.ie/news/business/2025/0606/1517043-spike-in-safe-account-scam-warning-boi/
Αυτό το άρθρο αναφέρει σημαντική αύξηση των αναφορών για απάτες «ασφαλούς λογαριασμού» στην Ιρλανδία, με δεκαπλάσια αύξηση την τελευταία εβδομάδα. Η Τράπεζα της Ιρλανδίας προειδοποιεί τους καταναλωτές για αυτόν τον τύπο απάτης, όπου οι απατεώνες εξαπατούν άτομα να μεταφέρουν χρήματα σε «ασφαλείς» λογαριασμούς με ψευδείς προφάσεις, τονίζοντας τη σημασία της επαγρύπνησης και των ασφαλών τραπεζικών πρακτικών.

4) **Εθνικό Κέντρο Κυβερνοασφάλειας – Ασφαλείς ηλεκτρονικές αγορές**
Ιστοσελίδα: https://www.ncsc.gov.uk/guidance/shopping-online-securely
Αυτή η επίσημη οδηγία της βρετανικής κυβέρνησης παρέχει πρακτικές συμβουλές στους καταναλωτές για ασφαλείς διαδικτυακές αγορές. Καλύπτει τομείς όπως η επαλήθευση της νομιμότητας των διαδικτυακών καταστημάτων, η χρήση ασφαλών μεθόδων πληρωμής, η προστασία των προσωπικών πληροφοριών και η αναφορά ύποπτων δραστηριοτήτων. Οι βασικές συστάσεις περιλαμβάνουν τη χρήση πιστωτικών καρτών για διαδικτυακές αγορές, την ενεργοποίηση της επαλήθευσης δύο βημάτων και την προσοχή σε ανεπιθύμητες προσφορές και συνδέσμους.

5) **Πώς να δημιουργήσετε έναν ισχυρό κωδικό πρόσβασης**
Βίντεο: https://www.youtube.com/watch?v=_wQTRMBAvzg
Αυτό το βίντεο παρέχει πρακτικές συμβουλές για τη δημιουργία ισχυρών και εύκολων στην απομνημόνευση κωδικών πρόσβασης. Τονίζει τη σημασία της χρήσης συνδυασμού γραμμάτων, αριθμών και συμβόλων, της αποφυγής κοινών λαθών και της εξέτασης των φράσεων πρόσβασης ως ασφαλούς εναλλακτικής λύσης.

6) **TechRadar – Εικονικά ιδιωτικά δίκτυα (VPN)**
Ιστοσελίδα: https://www.techradar.com/vpn/virtual-private-networks
Αυτός ο ολοκληρωμένος οδηγός από το TechRadar εξερευνά την έννοια των εικονικών ιδιωτικών δικτύων (VPN). Εξηγεί τον τρόπο λειτουργίας των VPN, τα οφέλη τους για την ιδιωτικότητα και την ασφάλεια στο διαδίκτυο και παρέχει συστάσεις για τις κορυφαίες υπηρεσίες VPN με βάση δοκιμές από ειδικούς.

4.5 Ενότητα ΙΙΙ – Προ/Μετά την εξέταση

1. Τι σημαίνει «HTTPS» στη διεύθυνση ενός ιστότοπου;

Α) Ο ιστότοπος φιλοξενείται σε άλλη χώρα
Β) Ο ιστότοπος είναι ασφαλής και τα δεδομένα είναι κρυπτογραφημένα
Γ) Ο ιστότοπος προσφέρει εκπτώσεις
Δ) Ο ιστότοπος απαιτεί σύνδεση

2. Γιατί είναι σημαντικό να χρησιμοποιείτε την επαλήθευση δύο παραγόντων (2FA) για τις ηλεκτρονικές τραπεζικές συναλλαγές;

Α) Επιταχύνει τις ηλεκτρονικές συναλλαγές
Β) Σας επιτρέπει να συνδεθείτε από πολλές συσκευές ταυτόχρονα
Γ) Παρέχει ένα επιπλέον επίπεδο ασφάλειας, απαιτώντας δύο βήματα επαλήθευσης
Δ) Αντικαθιστά την ανάγκη για κωδικό πρόσβασης

3. Ποιο είναι το κύριο πλεονέκτημα της χρήσης λογισμικού προστασίας από ιούς;

Α) Κάνει τον υπολογιστή σας πιο γρήγορο
Β) Προστατεύει από κακόβουλο λογισμικό και επιθέσεις phishing
Γ) Βοηθά στη διαχείριση των κωδικών πρόσβασης στο διαδίκτυο
Δ) Αποκλείει την πρόσβαση σε όλους τους ιστότοπους ηλεκτρονικών αγορών

4. Ποιος από τους παρακάτω κωδικούς πρόσβασης είναι ο πιο ασφαλής;

Α) Shopping2024
Β) 12345678
Γ) Mybankpassword
Δ) H@ppy$hopper92!

5. Τι πρέπει να κάνετε αν δείτε μια προσφορά στο διαδίκτυο που φαίνεται «πολύ καλή για να είναι αληθινή»;

Α) Να τη μοιραστείτε αμέσως με τους φίλους σας
Β) Κάντε κλικ στον σύνδεσμο για να ελέγξετε τις λεπτομέρειες
Γ) Αποφύγετέ την και επαληθεύστε τον ιστότοπο πριν προβείτε σε οποιαδήποτε ενέργεια
Δ) Δώστε τα στοιχεία σας για να διεκδικήσετε γρήγορα την προσφορά

6. Ποια είναι μια ασφαλής μέθοδος πληρωμής για online αγορές;

Α) Η πληρωμή με πιστωτική κάρτα σε έναν ασφαλή ιστότοπο
Β) Αποστολή χρημάτων μέσω άμεσης τραπεζικής μεταφοράς
Γ) Κοινοποίηση του αριθμού της κάρτας σας μέσω email
Δ) Χρήση οποιασδήποτε μεθόδου, εφόσον ο ιστότοπος φαίνεται επαγγελματικός

7. Γιατί πρέπει να αποφεύγετε τη χρήση δημόσιου Wi-Fi για οικονομικές συναλλαγές;

Α) Είναι πολύ αργό για online τραπεζικές συναλλαγές
Β) Μπορεί να μην είναι κρυπτογραφημένο και να επιτρέπει στους χάκερ να κλέψουν τα δεδομένα σας
Γ) Δεν υποστηρίζει ασφαλείς ιστότοπους
Δ) Εμποδίζει την πρόσβαση σε τραπεζικές εφαρμογές

8. Τι σημαίνει το εικονίδιο με το λουκέτο στη γραμμή διευθύνσεων του προγράμματος περιήγησης;

Α) Ο ιστότοπος βρίσκεται υπό συντήρηση
Β) Η σύνδεση μεταξύ της συσκευής σας και του ιστότοπου είναι ασφαλής
Γ) Ο ιστότοπος απαιτεί cookies
Δ) Ο ιστότοπος δεν είναι αξιόπιστος

9. Πώς μπορείτε να αναγνωρίσετε έναν αξιόπιστο ιστότοπο ηλεκτρονικών αγορών;

Α) Ζητά τον κωδικό πρόσβασής σας μέσω email
Β) Περιέχει ορθογραφικά λάθη και ασαφή στοιχεία επικοινωνίας
Γ) Έχει HTTPS, εικονίδιο με λουκέτο και επαληθευμένες κριτικές πελατών
Δ) Προσφέρει δωρεάν προϊόντα χωρίς πληρωμή

10. Τι πρέπει να κάνετε για να προστατεύσετε τη συσκευή και τα οικονομικά σας στοιχεία;

Α) Να απενεργοποιήσετε το λογισμικό προστασίας από ιούς για να γίνει ο υπολογιστής σας πιο γρήγορος
Β) Να διατηρείτε το λογισμικό σας ενημερωμένο και να χρησιμοποιείτε VPN σε δημόσια δίκτυα
Γ) Αποφύγετε να ελέγχετε το ιστορικό των συναλλαγών σας
Δ) Χρησιμοποιήστε τον ίδιο κωδικό πρόσβασης για όλους τους λογαριασμούς σας

Περίληψη απαντήσεων

1	**Β**
2	**C**
3	**Β**
4	**Δ**
5	**C**
6	**Α**
7	**Β**
8	**Β**
9	**C**
10	**Β**

ΕΝΟΤΗΤΑ IV

Ασφαλής και υπεύθυνη χρήση των μέσων κοινωνικής δικτύωσης για ηλικιωμένους

5. Ενότητα IV Ασφαλής και υπεύθυνη χρήση των μέσων κοινωνικής δικτύωσης για ηλικιωμένους

Η ενότητα «Ασφαλής χρήση των μέσων κοινωνικής δικτύωσης» εισάγει τους ηλικιωμένους στην υπεύθυνη και ασφαλή χρήση των πλατφορμών κοινωνικής δικτύωσης, συνδυάζοντας βασικές γνώσεις με πρακτικές οδηγίες. Οι συμμετέχοντες μαθαίνουν πώς να δημιουργούν και να διαχειρίζονται λογαριασμούς, να προσαρμόζουν τις ρυθμίσεις απορρήτου, να αναγνωρίζουν κοινές διαδικτυακές απάτες και να επικοινωνούν με ασφάλεια, ώστε να μπορούν να συμμετέχουν σε ψηφιακούς κοινωνικούς χώρους με μεγαλύτερη αυτοπεποίθηση και έλεγχο.

Η ενότητα περιλαμβάνει πρακτικές δραστηριότητες που βοηθούν τους συμμετέχοντες να αναγνωρίζουν ύποπτα μηνύματα, ψεύτικα προφίλ και παραπλανητικούς συνδέσμους που συναντώνται συχνά στα μέσα κοινωνικής δικτύωσης. Εστιάζει επίσης στην προστασία των προσωπικών πληροφοριών και της ψηφιακής ταυτότητας μέσω της αποτελεσματικής διαχείρισης της ιδιωτικότητας, της περιορισμένης κοινής χρήσης δεδομένων και των πρακτικών ασφαλείας λογαριασμών, όπως ισχυροί κωδικοί πρόσβασης και επαλήθευση δύο παραγόντων. Παρέχονται επίσης οδηγίες για την ασφάλεια των συσκευών, τις ενημερώσεις λογισμικού και τις ασφαλείς συνδέσεις στο διαδίκτυο.

Με την ενσωμάτωση αυτών των στοιχείων, το πρόγραμμα εξασφαλίζει ότι οι ηλικιωμένοι όχι μόνο κατανοούν τους κινδύνους που σχετίζονται με τα μέσα κοινωνικής δικτύωσης, αλλά και αναπτύσσουν πρακτικές δεξιότητες για την αποτελεσματική διαχείρισή τους. Οι συμμετέχοντες ολοκληρώνουν το πρόγραμμα με αυξημένη ψηφιακή ευαισθητοποίηση, αυτοπεποίθηση και ικανότητα να εφαρμόζουν ασφαλείς πρακτικές στα μέσα κοινωνικής δικτύωσης στις καθημερινές διαδικτυακές αλληλεπιδράσεις τους.

5.1 Μαθησιακοί στόχοι

Στόχος αυτού του μαθήματος είναι να βελτιώσει την κατανόηση και τις δεξιότητες των ηλικιωμένων για ασφαλή, υπεύθυνη και ουσιαστική συμμετοχή στα μέσα κοινωνικής δικτύωσης. Μέσω αυτής της εκπαίδευσης, οι ηλικιωμένοι 65 ετών και άνω θα:

- Αποκτήσουν αυτοπεποίθηση στην πλοήγηση σε δημοφιλείς πλατφόρμες κοινωνικών μέσων.
- Κατανοήσουν τη σημασία των ρυθμίσεων απορρήτου και μάθουν πώς να τις προσαρμόζουν αποτελεσματικά.
- Αναγνωρίζουν και αποφεύγουν τις συνήθεις διαδικτυακές απάτες και απειλές στα μέσα κοινωνικής δικτύωσης.
- Αναπτύξουν συνήθειες για την ασφαλή και υπεύθυνη κοινή χρήση προσωπικών πληροφοριών στο διαδίκτυο.
- Ασχολούνται υπεύθυνα με το περιεχόμενο των μέσων κοινωνικής δικτύωσης, διασφαλίζοντας παράλληλα την ασφάλεια και την ευημερία τους.

5.2 Δομή, περιεχόμενο και μαθησιακά αποτελέσματα

Με την επιτυχή ολοκλήρωση αυτού του μοδγλου, οι μαθητές θα είναι σε θέση να:

- Αναγνωρίζουν τα βασικά χαρακτηριστικά και τις χρήσεις δημοφιλών πλατφορμών όπως το Facebook, το Instagram και το LinkedIn.
- Να επιδείξουν την ικανότητα να δημιουργούν λογαριασμούς στα μέσα κοινωνικής δικτύωσης χρησιμοποιώντας ασφαλείς μεθόδους, όπως η επιλογή ισχυρών κωδικών πρόσβασης και η ενεργοποίηση της επαλήθευσης δύο παραγόντων.
- Προσαρμόζουν τις ρυθμίσεις απορρήτου για να ελέγχουν την ορατότητα των προσωπικών πληροφοριών και των αναρτήσεων.
- Διαχειρίζονται τις ρυθμίσεις επαφών για να περιορίζουν τα ανεπιθύμητα μηνύματα και τα αιτήματα σύνδεσης.
- Αναγνωρίζουν προειδοποιητικά σημάδια απάτης, όπως phishing, ψεύτικα προφίλ και ψευδείς συνδέσμους.
- Εφαρμόστε στρατηγικές για την προστασία ευαίσθητων προσωπικών δεδομένων από κακόβουλους χρήστες.
- Ελέγξτε και τροποποιήστε το περιεχόμενο που έχετε μοιραστεί στο παρελθόν, ώστε να συμμορφώνεται με τις βέλτιστες πρακτικές για την ασφάλεια στο διαδίκτυο.
- Αναπτύξτε συνήθειες για την ασφαλή κοινή χρήση πληροφοριών, συμπεριλαμβανομένης της αποφυγής της υπερβολικής κοινοποίησης ή της κοινοποίησης ευαίσθητου περιεχομένου.

5.3 Ατζέντα I Λεπτομερής σχέδιο συνεδρίας

ΕΝΌΤΗΤΑ IV
Ασφαλής και υπεύθυνη χρήση των μέσων κοινωνικής δικτύωσης για ηλικιωμένους

1η Συνεδρία

Καλωσόρισμα
Διάρκεια 5

Μαθησιακοί στόχοι

- Εισαγωγή στο θέμα και δημιουργία φιλόξενου περιβάλλοντος.

Περιεχόμενο/Μέθοδος

- Σύντομη εισαγωγή στη συνεδρία, περιγραφή των στόχων και καθορισμός των προσδοκιών
- Προετοιμασία του πλαισίου για την εκπαίδευση με περιγραφή του ενότητας και της σημασίας της.

Υλικό

- Λευκός πίνακας ή flip chart για τους στόχους της συνεδρίας.
- Μαρκαδόροι.
- Εκτυπωμένη ατζέντα ή διαφάνεια παρουσίασης που περιγράφει τη συνεδρία.

2η Συνεδρία

Δραστηριότητα για το σπάσιμο του πάγου: Μπίνγκο στα μέσα κοινωνικής δικτύωσης
Διάρκεια 5'

Μαθησιακοί στόχοι

- Να ενθαρρύνει την αλληλεπίδραση των συμμετεχόντων και να τους κάνει να αρχίσουν να σκέφτονται τις ψηφιακές τους συνήθειες.

Περιεχόμενο/Μέθοδος

- Καθώς οι συμμετέχοντες παρουσιάζονται, θα σημειώνουν όρους με τους οποίους είναι εξοικειωμένοι. Ο πρώτος συμμετέχων που θα συμπληρώσει μια σειρά στην κάρτα μπίνγκο του θα κερδίσει ένα μικρό βραβείο. Αυτό θα ενθαρρύνει τους συμμετέχοντες να μοιραστούν την εμπειρία τους με τα κοινωνικά μέσα και θα πυροδοτήσει τη συζήτηση γύρω από τις ψηφιακές τους συνήθειες.

Υλικό

- Εκτυπώστε κάρτες με συνήθεις όρους των μέσων κοινωνικής δικτύωσης, όπως «Facebook», «Instagram», «Like», «Hashtag», «Comment», «Follow», «Profile» κ.λπ.
- Στυλό και μολύβια, μαρκαδόροι και/ή αυτοκόλλητα

3η Συνεδρία

Διάλεξη 1: Επισκόπηση των μέσων κοινωνικής δικτύωσης
Διάρκεια *30*

Μαθησιακοί στόχοι

- Να βοηθήσει τους συμμετέχοντες να κατανοήσουν τις βασικές λειτουργίες και τους τύπους των πλατφορμών κοινωνικών μέσων.

Περιεχόμενο/Μέθοδος

- Παρουσίαση μιας επισκόπησης των δημοφιλών πλατφορμών (Facebook, Instagram, Twitter κ.λπ.), με εξήγηση των βασικών χαρακτηριστικών και λειτουργιών τους. Επεξήγηση των χαρακτηριστικών, των πλεονεκτημάτων και των πιθανών κινδύνων τους, καθώς και του τρόπου ασφαλούς δημιουργίας λογαριασμού.

Υλικό

- Διαφάνειες παρουσίασης που καλύπτουν τις δημοφιλείς πλατφόρμες κοινωνικών μέσων, τα χαρακτηριστικά τους και τους κινδύνους ασφαλείας.
- Προβολέας και φορητός υπολογιστής για την παρουσίαση.
- Φυλλάδια που συνοψίζουν τα χαρακτηριστικά και τις συμβουλές ασφαλείας για το Facebook, το Instagram και το Twitter.
- Σύνδεση στο Διαδίκτυο για ζωντανές επιδείξεις των χαρακτηριστικών της πλατφόρμας.

Δραστηριότητα 1: Εξοικείωση με την πλατφόρμα
Διάρκεια 20 λεπτά

Μαθησιακοί στόχοι

- Εξοικείωση των συμμετεχόντων με τον τρόπο πλοήγησης στις πλατφόρμες κοινωνικών μέσων.

Περιεχόμενο/Μέθοδος

- Πρακτική εξερεύνηση των πλατφορμών (π.χ. Facebook, Instagram, Twitter). Οι συμμετέχοντες θα εξασκηθούν στη δημιουργία λογαριασμού στα μέσα κοινωνικής δικτύωσης με έμφαση στην ασφάλεια (π.χ. επιλογή ισχυρών κωδικών πρόσβασης, ενεργοποίηση της επαλήθευσης δύο παραγόντων).

Υλικό

- Υπολογιστές, tablet ή smartphone για να εξερευνήσουν οι συμμετέχοντες τις πλατφόρμες.
- Εκτυπωμένοι οδηγοί για την ασφαλή δημιουργία λογαριασμών, που περιλαμβάνουν: *Οδηγίες για τη δημιουργία ισχυρών κωδικών πρόσβασης. Βήματα για την ενεργοποίηση της επαλήθευσης δύο παραγόντων.*

Διάλειμμα | Διάρκεια *5'*

- **Δώστε χρόνο στους συμμετέχοντες να αναζωογονηθούν και να σκεφτούν.**
- **Σύντομο διάλειμμα για ανανέωση.**

4η Συνεδρία

Διάλεξη 2: Ρυθμίσεις απορρήτου
Διάρκεια *30'*

Μαθησιακοί στόχοι

- Να εξοπλίσει τους συμμετέχοντες με τις δεξιότητες που απαιτούνται για την προσαρμογή των ρυθμίσεων απορρήτου και την προστασία των προσωπικών δεδομένων.

Περιεχόμενο/Μέθοδος

- Διδάξτε πώς να προσαρμόζετε τις ρυθμίσεις απορρήτου στις πλατφόρμες κοινωνικών μέσων για την προστασία των προσωπικών πληροφοριών.

Υλικό

- Διαφάνειες παρουσίασης που εξηγούν τις ρυθμίσεις απορρήτου για κοινές πλατφόρμες.
- Εκτυπωμένοι οδηγοί βήμα προς βήμα για τη ρύθμιση των παραμέτρων απορρήτου για το Facebook, το Instagram και το Twitter.
- Ένας προβολέας και ένας φορητός υπολογιστής για ζωντανές επιδείξεις των ρυθμίσεων απορρήτου.

Δραστηριότητα 2: Ρύθμιση των παραμέτρων απορρήτου
Διάρκεια *20*

Μαθησιακοί στόχοι

- Καθοδήγηση των συμμετεχόντων στην εξάσκηση του τρόπου διαμόρφωσης των ρυθμίσεων απορρήτου στις πλατφόρμες κοινωνικών μέσων.

Περιεχόμενο/Μέθοδος

- Διαδραστική άσκηση όπου οι συμμετέχοντες προσαρμόζουν τις ρυθμίσεις απορρήτου στους δικούς τους λογαριασμούς κοινωνικών μέσων.

Υλικό

- Υπολογιστές, tablet ή smartphone για πρακτική εξάσκηση.
- Προκαθορισμένοι εικονικοί λογαριασμοί (προαιρετικά) για συμμετέχοντες που δεν διαθέτουν προσωπικούς λογαριασμούς.
- Εκτυπωμένα φύλλα εργασίας με χώρο για να σημειώσουν τις ρυθμίσεις απορρήτου που έκαναν.

Διάλειμμα | Διάρκεια *5'*

- **Δώστε χρόνο για ξεκούραση και προετοιμασία για την επόμενη συνεδρία.**
- **Ένα σύντομο διάλειμμα για ανανέωση.**

5η Συνεδρία

Διάλεξη 3: Αναγνώριση απάτης και διαδικτυακών απειλών στα μέσα κοινωνικής δικτύωσης
Διάρκεια *30'*

Μαθησιακοί στόχοι

- Να βοηθήσει τους συμμετέχοντες να αναγνωρίσουν τις απάτες και τις απειλές που αφορούν συγκεκριμένα τα μέσα κοινωνικής δικτύωσης.

Περιεχόμενο/Μέθοδος

- Συζήτηση για τις συνήθεις απάτες στα μέσα κοινωνικής δικτύωσης, όπως το phishing, οι ψευδείς διαφημίσεις, τα ψεύτικα προφίλ και η κλοπή ταυτότητας.

Υλικό

- Διαφάνειες παρουσίασης με παραδείγματα απάτης, όπως ηλεκτρονικά μηνύματα phishing και ψεύτικες αιτήσεις φιλίας.
- Εκτυπωμένα φυλλάδια με λεπτομέρειες για τις συνήθεις απάτες και τα προειδοποιητικά σημάδια που πρέπει να προσέχετε.
- Προβολέας και φορητός υπολογιστής για την προβολή παραδειγμάτων ή βίντεο με απάτες στα μέσα κοινωνικής δικτύωσης.

Δραστηριότητα 3: Άσκηση αναγνώρισης απάτης
Διάρκεια 20

Μαθησιακοί στόχοι

- Ανάπτυξη της ικανότητας να εντοπίζετε απάτες στα μέσα κοινωνικής δικτύωσης και να μαθαίνετε πώς να αποφεύγετε να πέσετε θύματα απατηλών σχεδίων.

Περιεχόμενο/Μέθοδος

- Ομαδική δραστηριότητα όπου οι συμμετέχοντες εντοπίζουν και συζητούν παραδείγματα απάτης στα μέσα κοινωνικής δικτύωσης, όπως ψεύτικες αιτήσεις φιλίας ή μηνύματα ηλεκτρονικού ψαρέματος.

Υλικό

- Κάρτες σεναρίων με παραδείγματα απάτης για ομαδική συζήτηση.
- Φλιπ-χαρτ ή λευκός πίνακας για να σημειώσετε τα ευρήματα της ομάδας.
- Μαρκαδόροι για την καταγραφή των απαντήσεων των συμμετεχόντων.

Διάλειμμα |Διάρκεια 5'

- **Δώστε χρόνο για ξεκούραση και προετοιμασία.**
- **Σύντομο διάλειμμα για ανανέωση.**

6η Συνεδρία

Διάλεξη 4: Ασφαλής και υπεύθυνη συμμετοχή στα μέσα κοινωνικής δικτύωσης
Διάρκεια *30*

Μαθησιακοί στόχοι

- Εξηγήστε τη σημασία της ασφαλούς και υπεύθυνης χρήσης των μέσων κοινωνικής δικτύωσης
- Να διδάξετε στους μαθητές πώς να αναπτύξουν ασφαλείς συνήθειες κοινής χρήσης.

Περιεχόμενο/Μέθοδος

- Παρουσίαση του *θέματος «Γιατί η ασφάλεια στο διαδίκτυο είναι σημαντική για τα άτομα και τους επαγγελματίες;»*. Παραδείγματα πιθανών κινδύνων από μη ασφαλείς πρακτικές κοινής χρήσης (π.χ. κλοπή ταυτότητας, βλάβη της φήμης). Παρουσίαση υποθετικών σεναρίων στους μαθητές (π.χ. κοινή χρήση σχεδίων διακοπών ή επαγγελματικών επιτευγμάτων). Ερώτηση: *«Τι θα μοιραζόσασταν; Πώς θα το μοιραζόσασταν με ασφάλεια;»*. Ομαδική συζήτηση σχετικά με τις απαντήσεις.

Υλικό

- Διαφάνειες με στατιστικά στοιχεία σχετικά με τους κινδύνους στο διαδίκτυο.
- Ενημερωτικό γράφημα που συνοψίζει τους βασικούς κινδύνους και τις συνέπειες των μη ασφαλών πρακτικών.

Δραστηριότητα 4: Ανασκόπηση παλαιότερων αναρτήσεων και πληροφοριών
Διάρκεια *20*

Μαθησιακοί στόχοι

- Να δώσει τη δυνατότητα στους μαθητές να αξιολογήσουν και να τροποποιήσουν τα προφίλ και τις αναρτήσεις τους στα μέσα κοινωνικής δικτύωσης για λόγους ασφάλειας.

Περιεχόμενο/Μέθοδος

- Καθοδηγούμενη εξέταση ενός δείγματος προφίλ κοινωνικών μέσων (φανταστικό ή ανώνυμο παράδειγμα). Προσδιορισμός μη ασφαλούς ή υπερβολικά προσωπικού περιεχομένου (π.χ. αριθμοί τηλεφώνου, τοποθεσίες, ευαίσθητες φωτογραφίες). Επίδειξη του τρόπου διαγραφής ή τροποποίησης αναρτήσεων και προσαρμογής των ρυθμίσεων απορρήτου.

Υλικό

- Παράδειγμα προφίλ κοινωνικών μέσων (έντυπο ή στην οθόνη).
- Οδηγός βήμα προς βήμα για την προσαρμογή των ρυθμίσεων απορρήτου (PDF ή φυλλάδιο).

7η Συνεδρία

Συζήτηση | Διάρκεια 10’

Μαθησιακοί στόχοι

- Ενθάρρυνση μιας προληπτικής νοοτροπίας στην αναγνώριση και αναφορά ύποπτων δραστηριοτήτων στα κοινωνικά μέσα.

Περιεχόμενο/Μέθοδος

- Ομαδική συζήτηση σχετικά με τον τρόπο αντιμετώπισης ύποπτων δραστηριοτήτων στα μέσα κοινωνικής δικτύωσης, όπως ο τρόπος αναφοράς απάτης και αναγνώρισης ψεύτικων λογαριασμών.

Υλικό

- Λευκός πίνακας και μαρκαδόροι για την ανταλλαγή ιδεών σχετικά με τρόπους αναφοράς απάτης και χειρισμού ύποπτων λογαριασμών.
- Εκτυπωμένα υλικά με στοιχεία επικοινωνίας για την αναφορά απάτης (π.χ. συνδέσμους προς κέντρα βοήθειας πλατφορμών).

Σύνοψη | Διάρκεια 5’

Μαθησιακοί στόχοι

- Συνοψίστε την εκπαίδευση και βεβαιωθείτε ότι οι συμμετέχοντες κατανοούν πώς να προστατεύονται από τις απειλές των μέσων κοινωνικής δικτύωσης.

Περιεχόμενο/Μέθοδος

- Επανεξέταση των βασικών σημείων σχετικά με τις απάτες και τις απειλές στα μέσα κοινωνικής δικτύωσης, απάντηση σε εκκρεμείς ερωτήσεις και παροχή πόρων για συνεχή μάθηση.

Υλικό

- Φυλλάδια που συνοψίζουν τα βασικά σημεία που καλύφθηκαν στην ενότητα: ***Λίστα ελέγχου για την ασφάλεια στα μέσα κοινωνικής δικτύωσης***

5.4 Πρόσθετες πληροφορίες

5.4.1 Αυτοαξιολόγηση των εκπαιδευτών

- Μεταβίβασα αποτελεσματικά τη σημασία της ασφάλειας στο διαδίκτυο και της συμμετοχής στα μέσα κοινωνικής δικτύωσης;
- Διασφάλισα ότι οι συμμετέχοντες κατανόησαν τις τεχνικές πτυχές των ρυθμίσεων απορρήτου και της αναγνώρισης απάτης;
- Πώς ενέπλεξα τους συμμετέχοντες στις δραστηριότητες και τις συζητήσεις;
- Ήταν οι πόροι και τα υλικά χρήσιμα για τους συμμετέχοντες;

5.4.2 Αξιολόγηση του προγράμματος από τους εκπαιδευτές

- Είναι το περιεχόμενο της εκπαίδευσης σχετικό και σαφές για τους ηλικιωμένους;
- Ήταν οι δραστηριότητες και οι συζητήσεις αποτελεσματικές στο να βοηθήσουν τους συμμετέχοντες να μάθουν το υλικό;
- Τα αποτελέσματα συνάδουν με τους μαθησιακούς στόχους του μαθήματος;

5.4.3 Υλικό, πρόσθετοι πόροι

Παράρτημα 1 | Δραστηριότητα για το σπάσιμο του πάγου: Μπίνγκο κοινωνικών μέσων

Κάρτα Μπίνγκο κοινωνικών μέσων – Α

Μου αρέσει	**Σχόλιο**	**Facebook**	**Ιστορία**	**Hashtag**
Selfie	Μήνυμα	Instagram	Ετικέτα	Προφίλ
Emoji	Ακολουθούμενοι	ΔΩΡΕΑΝ	Tweet	Μοιραστείτε
Βίντεο	Απόρρητο	LinkedIn	Κατάσταση	Δημοσίευση
Χρονολόγιο	Ειδοποίηση	Twitter	Ομάδα	Reels

Κάρτα μπίνγκο κοινωνικών μέσων – Β

Ετικέτα	**Δημοσίευση**	**Instagram**	**Ιστορία**	**Απόρρητο**
Μήνυμα	Facebook	Χρονολόγιο	Μου αρέσει	Ομάδα
Reels	Hashtag	ΔΩΡΕΑΝ	Κατάσταση	Σχόλιο
Tweet	Μοιραστείτε	LinkedIn	Βίντεο	Selfie
Ακολουθώντας	Ειδοποίηση	Προφίλ	Emoji	Αποκλεισμός

Κάρτα Μπίνγκο κοινωνικών μέσων – C

Κατάσταση	**Μου αρέσει**	**LinkedIn**	**Selfie**	**Κοινή**
Facebook	Emoji	Instagram	Tweet	Reels
Μήνυμα	Απόρρητο	ΔΩΡΕΑΝ	Ομάδα	Ιστορία
Χρονολόγιο	Ετικέτα	Ειδοποίηση	Δημοσίευση	Hashtag
Αποκλεισμός	Ακολουθώντας	Βίντεο	Σχόλιο	Προφίλ

Παράρτημα 2 I Διάλεξη 1: Επισκόπηση των κοινωνικών μέσων

Διαφάνειες για την παρουσίαση:

- **Facebook:** «Αυτή είναι η πιο διαδεδομένη πλατφόρμα για να διατηρείτε επαφή με τους φίλους και την οικογένειά σας. Μπορείτε να μοιράζεστε φωτογραφίες, να σχολιάζετε ενημερώσεις, να συμμετέχετε σε ομάδες ενδιαφέροντος και πολλά άλλα».
- **Instagram:** «Αυτή η πλατφόρμα επικεντρώνεται σε φωτογραφίες και βίντεο. Είναι ιδανική για να μοιράζεστε στιγμές οπτικά, χρησιμοποιώντας λειτουργίες όπως το «Stories», που εξαφανίζονται μετά από 24 ώρες».
- **LinkedIn:** «Σκεφτείτε το ως το επαγγελματικό σας βιογραφικό στο διαδίκτυο. Είναι χρήσιμο για την αναζήτηση εργασίας και τη δικτύωση, αν και δεν χρησιμοποιείται συχνά από τους ηλικιωμένους, εκτός αν εξακολουθούν να είναι ενεργοί στην αγορά εργασίας».
- **Twitter:** «Εδώ, οι χρήστες δημοσιεύουν σύντομα μηνύματα κειμένου που ονομάζονται tweets. Χρησιμοποιείται κυρίως για την παρακολούθηση ειδήσεων και δημόσιων προσώπων».

Σύγκριση πλατφορμών κοινωνικών μέσων

Κατηγορία	Facebook	Instagram	LinkedIn	Twitter	Twitter (διπλή στήλη)
Σκοπός	Σύνδεση με φίλους και οικογένεια	Κοινή χρήση φωτογραφιών και σύντομων βίντεο	Επαγγελματική δικτύωση	Κοινή χρήση σύντομων ενημερώσεων	Κοινή χρήση σύντομων ενημερώσεων
Τύποι δημοσιεύσεων	Κείμενο, φωτογραφίες, βίντεο, σύνδεσμοι, ιστορίες	Φωτογραφίες, βίντεο, reels, ιστορίες	Ενημερώσεις για θέσεις εργασίας, άρθρα, βιογραφικά	Tweets (κείμενο), φωτογραφίες, βίντεο	Δημόσιο, ακόλουθοι
Σχόλια και αντιδράσεις	Φίλοι, ομάδες, κοινό	Ακολουθούμενοι, κοινό	Επαγγελματικές επαφές	Επισημάνσεις "Μου αρέσει", σχόλια	Επισημάνσεις "Μου αρέσει", σχόλια
Μηνύματα	Εφαρμογή Messenger	Επισημάνσεις "Μου αρέσει", σχόλια	Επισημάνσεις "Μου αρέσει", σχόλια	Επισημάνσεις "Μου αρέσει", σχόλια, αναδημοσιεύσεις	Επισημάνσεις "Μου αρέσει", αναδημοσιεύσεις
Ρυθμίσεις απορρήτου	Προσαρμόσιμες: δημόσιες, φίλοι, ομάδες	Περιορισμένες, κυρίως δημόσιες εκτός αν είναι ιδιωτικές	Πιο δημόσια από προεπιλογή	Κυρίως δημόσιο, περιορισμένος έλεγχος	Δημόσιο όνομα και δημοσιεύσεις από προεπιλογή

Ορατότητα προφίλ	Ρυθμιζόμενο: όνομα, φωτογραφίες, βιογραφικό	Περιορισμένος έλεγχος εκτός αν ο λογαριασμός είναι ιδιωτικός	Δημόσιο εκτός αν ρυθμιστεί από προεπιλογή	Δημόσιο όνομα και προσαρμοσμένο	Δημόσιο όνομα και δημοσιεύσεις από προεπιλογή
Κοινές κίνδυνοι	Ψεύτικοι λογαριασμοί, υπερβολική κοινοποίηση πληροφοριών, απάτες	Απάτες σε DM, πλαστοπροσωπία	Μηνύματα phishing, πλαστοπροσωπία	Παρενοχλήσεις, ψεύτικοι σύνδεσμοι, πλαστοπροσωπία	Παράνομη χρήση προσωπικών δεδομένων, ψεύτικοι σύνδεσμοι, πλαστοπροσωπία
Καλό για	✓	✓	✓	✓	✓

Παράρτημα 3 | Δραστηριότητα 1: Εξοικείωση με την πλατφόρμα

Ο εκπαιδευτής καθοδηγεί την ομάδα βήμα προς βήμα:

«Ανοίξτε τον περιηγητή σας στο διαδίκτυο και μεταβείτε στη διεύθυνση www.facebook.com ή www.instagram.com».

«Κάντε κλικ στο "Δημιουργία νέου λογαριασμού" και συμπληρώστε τα στοιχεία σας — όνομα, ημερομηνία γέννησης κ.λπ.».

«Όταν σας ζητηθεί να επιλέξετε έναν κωδικό πρόσβασης, βεβαιωθείτε ότι είναι ισχυρός. Ένας καλός κωδικός πρόσβασης έχει τουλάχιστον 8 χαρακτήρες, χρησιμοποιεί ένα συνδυασμό γραμμάτων και αριθμών και περιλαμβάνει ένα σύμβολο».

Ο εκπαιδευτής προσθέτει:

«Για παράδειγμα, αντί για «maria123», θα μπορούσατε να χρησιμοποιήσετε «Maria!74books».

«Τώρα ας ενεργοποιήσουμε την επαλήθευση δύο παραγόντων — Η επαλήθευση δύο παραγόντων (2FA) προσθέτει ένα επιπλέον επίπεδο ασφάλειας. Αφού εισαγάγετε τον κωδικό πρόσβασής σας, θα σας ζητηθεί ένας κωδικός που θα σταλεί στο κινητό σας τηλέφωνο ή στο email σας.»

Παράρτημα 4 | Λίστα ελέγχου για τη ρύθμιση του λογαριασμού, Λίστα ελέγχου για τη ρύθμιση του λογαριασμού

1. Επιλέξτε μια πλατφόρμα (Facebook, Instagram κ.λπ.)
2. Μεταβείτε στον επίσημο ιστότοπο ή κατεβάστε την επίσημη εφαρμογή.
3. Κάντε κλικ στο «Δημιουργία νέου λογαριασμού».
4. Εισαγάγετε το πραγματικό σας όνομα και την ημερομηνία γέννησής σας.
5. Χρησιμοποιήστε έναν ισχυρό και μοναδικό κωδικό πρόσβασης (βλ. Φυλλάδιο 2).
6. Δώστε τον αριθμό του κινητού σας τηλεφώνου ή τη διεύθυνση email σας.
7. Ενεργοποιήστε την επαλήθευση δύο παραγόντων.
8. Παράλειψε τις περιττές προσωπικές πληροφορίες (όπως τη διεύθυνσή σου).
9. Ελέγξτε τις ρυθμίσεις απορρήτου αμέσως μετά τη δημιουργία του λογαριασμού.
10. Αποσυνδεθείτε όταν χρησιμοποιείτε δημόσια ή κοινόχρηστη συσκευή.

Λίστα ελέγχου για τη ρύθμιση του λογαριασμού

Ένας ισχυρός κωδικός πρόσβασης πρέπει:

- Να έχει μήκος τουλάχιστον 8 χαρακτήρες.
- Περιλαμβάνει συνδυασμό κεφαλαίων και μικρών γραμμάτων.
- Περιλαμβάνει τουλάχιστον έναν αριθμό και έναν ειδικό χαρακτήρα (π.χ. !, @, #, $).
- Να αποφεύγει τη χρήση κοινών λέξεων ή πληροφοριών που μπορούν εύκολα να μαντευτούν (όπως το όνομά σας ή η ημερομηνία γέννησής σας).
- Να είναι μοναδικός για κάθε λογαριασμό που δημιουργείτε.

Παράδειγμα αδύναμου κωδικού πρόσβασης: maria123
Παράδειγμα ισχυρού κωδικού πρόσβασης: M@r!a74Books

Παράρτημα 5 | Διάλεξη 2: Ρυθμίσεις απορρήτου

Λίστα ελέγχου απορρήτου κοινωνικών μέσων

[ ] Έχετε ελέγξει τις ρυθμίσεις ορατότητας του προφίλ σας;

[ ] Οι αναρτήσεις σας περιορίζονται μόνο σε «Φίλους» ή «Ακολουθούς»;

[ ] Έχετε ενεργοποιήσει την επαλήθευση δύο παραγόντων σε όλες τις πλατφόρμες;

[ ] Αποφεύγετε να μοιράζεστε τον αριθμό τηλεφώνου, τη διεύθυνση κατοικίας ή την πλήρη ημερομηνία γέννησής σας;

[ ] Έχετε ελέγξει ποιος μπορεί να σας στέλνει μηνύματα ή αιτήματα φιλίας;

[ ] Ελέγχετε τις φωτογραφίες και τις αναρτήσεις στις οποίες έχετε επισημανθεί πριν εμφανιστούν στο προφίλ σας;

[ ] Είστε προσεκτικοί όταν αποδέχεστε νέες αιτήσεις φιλίας ή παρακολούθησης;

[ ] Έχετε διαγράψει παλιές αναρτήσεις που περιέχουν ευαίσθητες πληροφορίες;

[ ] Ελέγχετε τακτικά τις ρυθμίσεις απορρήτου σας;

[ ] Γνωρίζετε πού να αναφέρετε απάτες και καταχρήσεις σε κάθε πλατφόρμα;

Οδηγός ρυθμίσεων απορρήτου

Σύνδεσμοι και βήματα για την προσαρμογή των ρυθμίσεων απορρήτου σε δημοφιλείς πλατφόρμες:

1. Facebook:

- Μεταβείτε στο Εργαλείο ελέγχου απορρήτου: https://www.facebook.com/privacy/checkup
- Κέντρο απορρήτου: https://www.facebook.com/privacy/center
- Προσαρμόστε ποιος μπορεί να βλέπει τις αναρτήσεις σας, ποιος μπορεί να σας στέλνει αιτήματα φιλίας και ποιος μπορεί να σας αναζητήσει.

2. Instagram:

- Μεταβείτε στο Κέντρο ασφάλειας: https://help.instagram.com/196883487377501
- Πώς να ρυθμίσετε τον λογαριασμό σας στο Instagram ως ιδιωτικό: https://help.instagram.com/448523408565555
- Ορίστε τον λογαριασμό σας ως ιδιωτικό, διαχειριστείτε τα σχόλια και ελέγξτε τις ετικέτες.

3. LinkedIn:

- Μεταβείτε στην επισκόπηση των ρυθμίσεων απορρήτου: https://www.linkedin.com/help/linkedin/answer/66
- Διαχειριστείτε τις ρυθμίσεις του δημόσιου προφίλ σας στο LinkedIn: https://www.linkedin.com/help/linkedin/answer/83
- Επιλέξτε ποιος μπορεί να δει τις συνδέσεις, τις λεπτομέρειες του προφίλ και τη δραστηριότητά σας.

4. Twitter (X):

- Μεταβείτε στις Ρυθμίσεις ασφάλειας: https://help.twitter.com/en/safety-and-security/twitter-privacy-settings
- Ασφάλεια και πρόσβαση στο λογαριασμό: https://help.twitter.com/en/managing-your-account/accessing-your-twitter-data
- Προστατέψτε τα tweets σας, περιορίστε ποιος μπορεί να σας στείλει μηνύματα ή να σας αναφέρει και ελέγξτε την ευρεσιμότητα.

Παράρτημα 6 | Δραστηριότητα 2: Προσαρμογή των ρυθμίσεων απορρήτου

Φύλλο εργασίας προσαρμογής απορρήτου

Χρησιμοποιήστε αυτό το φύλλο εργασίας για να παρακολουθείτε τις αλλαγές που κάνετε στις ρυθμίσεις απορρήτου των κοινωνικών μέσων. Αφού ελέγξετε τον λογαριασμό σας, σημειώστε παρακάτω τις λεπτομέρειες των αλλαγών που έχετε κάνει και τους λόγους για αυτές.

1.

Ρύθμιση που προσαρμόστηκε _____

Νέα τιμή/επιλογή _____

Λόγος αλλαγής _____

2.

Ρύθμιση που προσαρμόστηκε _____

Νέα τιμή/επιλογή _____

Λόγος αλλαγής _____

3.

Ρύθμιση που προσαρμόστηκε _____

Νέα τιμή/επιλογή _____

Λόγος αλλαγής _____

4.

Ρύθμιση που προσαρμόστηκε _____

Νέα τιμή/επιλογή _____

Λόγος αλλαγής _____

5.

Ρύθμιση που προσαρμόστηκε _____

Νέα τιμή/επιλογή _____

Λόγος αλλαγής _____

Παράρτημα 7| Διάλεξη 3: Αναγνώριση απάτης και διαδικτυακών απειλών στα μέσα κοινωνικής δικτύωσης

Βασικά σημεία των πιο συνηθισμένων απάτων:

- **Phishing:** *«Πρόκειται για ψεύτικα μηνύματα που προσπαθούν να σας ξεγελάσουν ώστε να δώσετε τα προσωπικά σας στοιχεία. Για παράδειγμα, ένα μήνυμα που λέει: «Κερδίσατε ένα βραβείο! Κάντε κλικ εδώ για να το διεκδικήσετε».*
- **Ψεύτικες αιτήσεις φιλίας:** *«Μπορεί να λάβετε μια αίτηση από κάποιον που προσποιείται ότι είναι ξάδελφός σας ή γείτονάς σας — πάντα να ελέγχετε δύο φορές».*
- **Ύποπτοι σύνδεσμοι:** *«Αυτοί μπορούν να μολύνουν τη συσκευή σας ή να κλέψουν τους κωδικούς πρόσβασής σας. Αν ο σύνδεσμος φαίνεται περίεργος ή δεν τον περιμένατε, μην κάνετε κλικ».*
- **Απάτες με πλαστοπροσωπία και ρομαντικές απάτες:** *«Μερικοί άνθρωποι μπορεί να ξεκινήσουν μια φιλία ή μια ρομαντική συνομιλία μόνο και μόνο για να ζητήσουν χρήματα αργότερα».*
- **Ψεύτικες ταυτότητες***: «Οι απατεώνες δημιουργούν ψεύτικα προφίλ στο διαδίκτυο για να κερδίσουν την εμπιστοσύνη των θυμάτων και να τα παρασύρουν να τους δώσουν χρήματα ή προσωπικά στοιχεία».*

Παράρτημα 8| Οδηγός αναγνώρισης απάτης

Μάθετε πώς να αναγνωρίζετε τις συνηθισμένες απάτες στα μέσα κοινωνικής δικτύωσης:

1. Μηνύματα ηλεκτρονικού ψαρέματος:
- Αναζητήστε επείγοντα αιτήματα όπως «Ο λογαριασμός σας θα κλειδωθεί!».
- Ελέγξτε το email ή το όνομα χρήστη του αποστολέα — σας φαίνεται ύποπτο;

2. Ψεύτικες αιτήσεις φιλίας:
- Να είστε προσεκτικοί με άτομα που δεν γνωρίζετε.
- Προσέξτε τα διπλά προφίλ που προσποιούνται ότι είναι κάποιος που γνωρίζετε.

3. Απάτες με βραβεία ή λαχειοφόρους αγορές:
- Τα μηνύματα του τύπου «Κερδίσατε!» είναι σχεδόν πάντα απάτες.
- Ποτέ μην παρέχετε τα τραπεζικά σας στοιχεία και μην πληρώνετε για να διεκδικήσετε ένα έπαθλο.

4. Απάτες με ρομαντικές σχέσεις ή φιλίες:
- Οι απατεώνες μπορεί να κερδίσουν την εμπιστοσύνη σας και στη συνέχεια να σας ζητήσουν χρήματα.
- Να είστε προσεκτικοί αν κάποιος γίνεται πολύ προσωπικός πολύ γρήγορα.

5. Ύποπτοι σύνδεσμοι:
- Μην κάνετε κλικ σε άγνωστους συνδέσμους, ειδικά σε αυτούς που αποστέλλονται σε ιδιωτικά μηνύματα.
- Πάντα να ελέγχετε διπλά και να αναφέρετε ύποπτες δραστηριότητες

Παράρτημα 9| Συμβουλές για την ασφάλεια στα μέσα κοινωνικής δικτύωσης

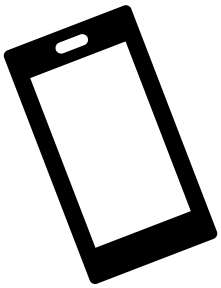
Ακολουθήστε αυτές τις βασικές συμβουλές για να παραμείνετε ασφαλείς στα μέσα κοινωνικής δικτύωσης:

- Ρυθμίστε το προφίλ σας ως ιδιωτικό και ελέγξτε ποιος μπορεί να βλέπει τις αναρτήσεις σας.
- Χρησιμοποιήστε ισχυρούς, μοναδικούς κωδικούς πρόσβασης για κάθε λογαριασμό.
- Ενεργοποιήστε την επαλήθευση δύο παραγόντων για επιπλέον ασφάλεια.
- Μην αποδέχεστε αιτήματα φιλίας από άγνωστους.
- Προσέξτε τι δημοσιεύετε – αποφύγετε να μοιράζεστε ταξιδιωτικά σχέδια ή προσωπικές πληροφορίες.
- Αποσυνδεθείτε όταν χρησιμοποιείτε δημόσιες ή κοινόχρηστες συσκευές.
- Αναφέρετε οτιδήποτε ύποπτο, συμπεριλαμβανομένων απάτες και ψεύτικους λογαριασμούς.
- Ενημερώνετε τις εφαρμογές σας για να προστατεύεστε από νέες απειλές.
- Σκεφτείτε πριν κάνετε κλικ σε συνδέσμους ή κατεβάσετε αρχεία.
- Σε περίπτωση αμφιβολίας, ρωτήστε κάποιον που εμπιστεύεστε ή αναφέρετε το πρόβλημα.

Μείνετε ενημερωμένοι. Μείνετε ασφαλείς.

Παράρτημα 10 | Δραστηριότητα 3: Άσκηση αναγνώρισης απάτης

Σενάριο 1: Κερδίσατε!



Λαμβάνετε ένα μήνυμα από έναν άγνωστο λογαριασμό που λέει:
«Συγχαρητήρια! Κερδίσατε ένα νέο smartphone! Κάντε κλικ στον παρακάτω σύνδεσμο για να διεκδικήσετε το έπαθλο σας».
Το μήνυμα περιλαμβάνει έναν σύνδεσμο και σας ζητά να εισαγάγετε τα προσωπικά σας στοιχεία.

Σενάριο 2: Φίλος σε κίνδυνο

Λαμβάνετε ένα μήνυμα στο Facebook Messenger από έναν φίλο με τον οποίο δεν έχετε μιλήσει εδώ και καιρό. Σας λέει ότι έχει κολλήσει στο εξωτερικό και χρειάζεται να του στείλετε αμέσως 500 ευρώ.

Σας ζητά τον αριθμό τηλεφώνου και τα στοιχεία του τραπεζικού σας λογαριασμού.

Σενάριο 3: Ειδοποίηση από τράπεζα

Ένας λογαριασμός που ισχυρίζεται ότι είναι η τράπεζά σας στέλνει ένα άμεσο μήνυμα στο Instagram:
«Εντοπίσαμε ύποπτη δραστηριότητα στον λογαριασμό σας. Παρακαλούμε επιβεβαιώστε αμέσως τα στοιχεία σύνδεσής σας απαντώντας εδώ».
Το προφίλ του λογαριασμού έχει ως εικόνα το λογότυπο της τράπεζας.

Σενάριο 4: Ευκαιρία εργασίας

Λαμβάνετε ένα αίτημα σύνδεσης στο LinkedIn από κάποιον που ισχυρίζεται ότι είναι υπεύθυνος προσλήψεων. Σας προσφέρει μια θέση εργασίας εξ αποστάσεως με υψηλό μισθό και ευέλικτο ωράριο.
Αφού αποδεχτείτε, σας ζητά το βιογραφικό σας, φωτογραφία ταυτότητας και τον αριθμό κοινωνικής ασφάλισης.

Σενάριο 5: Τοπική κοινοτική ομάδα

Σας προσκαλούν να γίνετε μέλος μιας ομάδας στο Facebook για ηλικιωμένους της περιοχής. Η ομάδα μοιράζεται συμβουλές για την υγεία, ενημερώσεις για εκδηλώσεις και νέα της κοινότητας. Τα μέλη είναι φιλικά και κανείς δεν ζητά προσωπικά δεδομένα.

Παράρτημα 11 | Διάλεξη 4: Ασφαλής και υπεύθυνη συμμετοχή στα μέσα κοινωνικής δικτύωσης

Οδηγίες για ασφαλή κοινή χρήση

Χρησιμοποιήστε τις ακόλουθες οδηγίες για να μοιράζεστε υπεύθυνα στα μέσα κοινωνικής δικτύωσης:

- Σκεφτείτε πριν δημοσιεύσετε: Θα σας πείραζε αν το έβλεπε ένας άγνωστος;
- Αποφύγετε να μοιράζεστε την ακριβή τοποθεσία σας, ειδικά σε πραγματικό χρόνο.
- Μην ανακοινώνετε μακρινά ταξίδια ή πότε θα είναι άδειο το σπίτι σας.
- Μην δημοσιεύετε ποτέ προσωπικά έγγραφα, όπως ταυτότητες, εισιτήρια ή τραπεζικά στοιχεία.
- Να είστε προσεκτικοί όταν μοιράζεστε φωτογραφίες παιδιών – ζητήστε άδεια όταν χρειάζεται.
- Χρησιμοποιήστε τις ρυθμίσεις απορρήτου για να ελέγχετε ποιος βλέπει τις αναρτήσεις σας.
- Αποφύγετε να μοιράζεστε ευαίσθητα θέματα σε δημόσιες αναρτήσεις.
- Μην μοιράζεστε περιεχόμενο όταν είστε συναισθηματικά φορτισμένοι – σταματήστε και σκεφτείτε πρώτα.
- Χρησιμοποιήστε ιδιωτικά μηνύματα για προσωπικές συνομιλίες αντί για δημόσια σχόλια.
- Ελέγχετε τακτικά τις παλιές σας αναρτήσεις και διαγράψτε ό,τι θεωρείτε ότι δεν είναι ασφαλές.

Θυμηθείτε: Μόλις κάτι δημοσιευτεί στο διαδίκτυο, είναι δύσκολο να το ανακαλέσετε.

Παράρτημα 12 | Δραστηριότητα 4: Αναθεώρηση παλαιότερων αναρτήσεων και πληροφοριών

Ο εκπαιδευτής λέει:
«Τώρα θα μπούμε στους λογαριασμούς σας στα μέσα κοινωνικής δικτύωσης και θα δούμε παλιές αναρτήσεις ή φωτογραφίες. Αυτή η άσκηση ονομάζεται «Ψηφιακή καθαριότητα».

Ο εκπαιδευτής καθοδηγεί τα βήματα:

- *«Μεταβείτε στο προφίλ ή στο χρονολόγιό σας».*
- *«Ελέγξτε 3-5 παλαιότερες αναρτήσεις. Ρωτήστε τον εαυτό σας: Είναι κάτι που θα μοιραζόμουν σήμερα; Αποκαλύπτει προσωπικές πληροφορίες;»*
- *«Αν ναι, ας το διαγράψουμε ή ας το επεξεργαστούμε. Θα σας δείξω πώς».*

Ο εκπαιδευτής κάνει επίδειξη στην οθόνη ή στον προβολέα:

- *Πώς να διαγράψετε μια ανάρτηση στο Facebook*
- *Πώς να αφαιρέσετε την επισήμανση από φωτογραφίες*
- *Πώς να αλλάξετε την ορατότητα από «Δημόσια» σε «Φίλοι»*

Παράρτημα 13 | Λίστα ελέγχου ασφάλειας προφίλ

Χρησιμοποιήστε αυτόν τον κατάλογο ελέγχου για να ελέγξετε την ασφάλεια του προφίλ σας στα μέσα κοινωνικής δικτύωσης:

[ ] Η φωτογραφία του προφίλ σας είναι κατάλληλη και δεν σας ταυτοποιεί (δεν περιέχει προσωπικά στοιχεία όπως τη διεύθυνση κατοικίας σας στο φόντο);

[ ] Έχετε αφαιρέσει ή αποκρύψει την ημερομηνία γέννησης, τον αριθμό τηλεφώνου ή τη διεύθυνση κατοικίας σας από το προφίλ σας;

[ ] Οι αναρτήσεις σας έχουν ρυθμιστεί ως «Μόνο για φίλους» ή «Ιδιωτικές» και όχι ως «Δημόσιες»;

[ ] Έχετε ελέγξει ποιος μπορεί να σχολιάζει ή να μοιράζεται τις αναρτήσεις σας;

[ ] Έχετε ελέγξει ποιος μπορεί να σας στείλει αιτήματα φιλίας/ακολούθησης;

[ ] Χρησιμοποιείτε έναν ισχυρό, μοναδικό κωδικό πρόσβασης για τον λογαριασμό σας;

[ ] Έχετε ενεργοποιήσει την επαλήθευση δύο παραγόντων;

[ ] Ελέγχετε τακτικά τις αναρτήσεις σας και διαγράφετε ό,τι είναι παλιό ή μη ασφαλές;

[ ] Έχετε απενεργοποιήσει την κοινή χρήση της τοποθεσίας στις αναρτήσεις σας;

[ ] Ελέγχετε τις αναρτήσεις στις οποίες έχετε επισημανθεί πριν εμφανιστούν στο χρονολόγιό σας;

Συμπληρώστε αυτή τη λίστα ελέγχου κάθε λίγους μήνες για να διατηρήσετε το προφίλ σας ασφαλές.

Παράρτημα 14 | Λίστα ελέγχου για την ασφάλεια στα μέσα κοινωνικής δικτύωσης

[ ] Χρησιμοποιείτε ισχυρούς, μοναδικούς κωδικούς πρόσβασης για κάθε λογαριασμό

[ ] Ενεργοποιήστε την επαλήθευση δύο παραγόντων

[ ] Ελέγχετε και προσαρμόζετε τακτικά τις ρυθμίσεις απορρήτου

[ ] Να είστε προσεκτικοί με τις προσωπικές πληροφορίες που μοιράζεστε δημόσια

[ ] Σκεφτείτε πριν αποδεχτείτε αιτήματα φιλίας ή παρακολούθησης

[ ] Προσέχετε τις απάτες, το phishing και τα ύποπτα μηνύματα

[ ] Να είστε προσεκτικοί όταν κάνετε κλικ σε συνδέσμους ή κατεβάζετε περιεχόμενο

[ ] Αναφέρετε και αποκλείστε ύποπτους ή προσβλητικούς χρήστες

[ ] Περιορίστε την κοινή χρήση της τοποθεσίας και τη γεωγραφική σήμανση

[ ] Διατηρήστε τις εφαρμογές και τις συσκευές σας ενημερωμένες

Παράρτημα 15| Προτάσεις για περαιτέρω ανάγνωση και μάθηση για τους συμμετέχοντες

Ιστοσελίδες για την ασφάλεια στον κυβερνοχώρο: Ευρωπαϊκοί και κυβερνητικοί οργανισμοί που ασχολούνται με την ασφάλεια στον κυβερνοχώρο

1) **ENISA (Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια)**
   Ιστότοπος: https://www.enisa.europa.eu/
   Η ENISA είναι ο οργανισμός της ΕΕ που είναι υπεύθυνος για την κυβερνοασφάλεια. Δημοσιεύει εκθέσεις, οδηγούς και προειδοποιήσεις σχετικά με τις απειλές στον κυβερνοχώρο και παρέχει πρακτικές συμβουλές σε πολίτες και οργανισμούς.
2) **CERT-EU (Ομάδα Αντιμετώπισης Έκτακτων Περιστατικών Πληροφορικής για τα Όργανα της ΕΕ)**
   Ιστότοπος: https://cert.europa.eu/
   Η CERT-EU παρακολουθεί τις απειλές στον κυβερνοχώρο και ανταποκρίνεται σε κυβερνοεπιθέσεις που στοχεύουν ευρωπαϊκά όργανα. Προσφέρει επίσης προειδοποιήσεις και βέλτιστες πρακτικές που μπορούν να εφαρμοστούν από εκπαιδευτές και τελικούς χρήστες.
3) **EC3 – Κέντρο Κυβερνοεγκληματικότητας της Ευρωπόλης**
   Ιστοσελίδα: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cyber-crime
   Το EC3 της Europol παρέχει πληροφορίες σχετικά με την ηλεκτρονική απάτη, τις απάτες και άλλες μορφές εγκληματικότητας στον κυβερνοχώρο. Δημοσιεύει υλικό ευαισθητοποίησης και μελέτες περιπτώσεων που σχετίζονται με τον εντοπισμό κινδύνων στα μέσα κοινωνικής δικτύωσης.
4) **Stay Safe Online – Εθνική Συμμαχία για την Κυβερνοασφάλεια (ΗΠΑ)**
   Ιστοσελίδα: https://staysafeonline.org/
   Ένα κέντρο πόρων με απλές λίστες ελέγχου και εκστρατείες σχετικά με την προστασία της ιδιωτικής ζωής, την ασφάλεια των κωδικών πρόσβασης, το phishing και την ευαισθητοποίηση στα μέσα κοινωνικής δικτύωσης.
5) **Δίκτυο παρακολούθησης απάτης AARP**
   Ιστοσελίδα: https://www.aarp.org/money/scams-fraud/
   Μια προσιτή πρωτοβουλία με έδρα τις ΗΠΑ, η οποία παρέχει ενημερωμένες πληροφορίες σχετικά με απάτες που στοχεύουν ιδιαίτερα τους ηλικιωμένους, προσφέροντας συμβουλές πρόληψης και αναφοράς.
6) **NCSC UK – Οδηγίες για τα μέσα κοινωνικής δικτύωσης**
   Ιστοσελίδα: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/social-media
7) **NCSC UK – Οδηγίες για τους κωδικούς πρόσβασης**
   Ιστοσελίδα: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/pass-words
8) **Βοήθεια LinkedIn – Ρυθμίσεις απορρήτου**

   Ιστοσελίδα: https://www.linkedin.com/help/linkedin/answer/66

5.5 Ενότητα IV – Προ/μετα-τεστ

1. Τι περιλαμβάνουν τα «προσωπικά δεδομένα»;

Α) Μόνο τις αναρτήσεις σας στα μέσα κοινωνικής δικτύωσης
Β) Οποιαδήποτε πληροφορία που μπορεί να σας ταυτοποιήσει, όπως το όνομά σας ή ο αριθμός ταυτότητάς σας
Γ) Μόνο τα στοιχεία του τραπεζικού σας λογαριασμού
Δ) Μόνο τους κωδικούς πρόσβασης που χρησιμοποιείτε στο διαδίκτυο

2. Γιατί είναι σημαντικό να διαβάζετε τις πολιτικές απορρήτου;

Α) Περιέχουν αστεία σχετικά με την ασφάλεια των δεδομένων
Β) Εξηγούν πώς θα συλλέγονται και θα χρησιμοποιούνται τα δεδομένα σας
Γ) Βοηθούν τη συσκευή σας να λειτουργεί πιο γρήγορα
Δ) Είναι νομικά υποχρεωτικές, αλλά δεν έχουν σημασία

3. Ποιο από τα παρακάτω είναι παράδειγμα ευαίσθητων προσωπικών δεδομένων;

Α) Αγαπημένο χρώμα
Β) Διεύθυνση κατοικίας
Γ) Ιατρικό ιστορικό ή βιομετρικά δεδομένα
Δ) Προτιμήσεις αγορών

4. Ποια είναι η βέλτιστη πρακτική κατά την κοινή χρήση φωτογραφιών ή πληροφοριών στο διαδίκτυο;

Α) Να μοιράζεστε όλα τα προσωπικά σας στοιχεία για να είστε ανοιχτοί και κοινωνικοί
Β) Να ελέγχετε ποιος μπορεί να δει τις πληροφορίες πριν τις δημοσιεύσετε
Γ) Δημοσιεύστε συχνά για να παραμείνετε ορατοί
Δ) Να συμπεριλαμβάνετε πάντα την τοποθεσία σας

5. Τι σημαίνει «κρυπτογράφηση δεδομένων»;

Α) Η απόκρυψη αρχείων σε έναν μυστικό φάκελο
Β) Μετατροπή των πληροφοριών σε κωδικό για την προστασία τους από μη εξουσιοδοτημένη πρόσβαση
Γ) Αποθήκευση των αρχείων σας σε μια μονάδα flash
Δ) Διαγραφή όλων των παλαιών δεδομένων

6. Γιατί πρέπει να περιορίζετε την ποσότητα των πληροφοριών που μοιράζεστε στα μέσα κοινωνικής δικτύωσης;

Α) Εξοικονομεί δεδομένα διαδικτύου
Β) Μειώνει τον κίνδυνο κλοπής ταυτότητας και απάτης
Γ) Αυξάνει τον αριθμό των ακολούθων
Δ) Αποτρέπει τους άλλους από το να σχολιάζουν

7. Τι πρέπει να κάνετε πριν παραχωρήσετε σε μια εφαρμογή πρόσβαση στις προσωπικές σας πληροφορίες;

Α) Να αποδεχτείτε αμέσως για να χρησιμοποιήσετε την εφαρμογή πιο γρήγορα
Β) Να διαβάσετε προσεκτικά τις άδειες και να επιτρέψετε μόνο τις απαραίτητες
Γ) Να επιτρέψετε όλες τις άδειες για να αποφύγετε σφάλματα της εφαρμογής
Δ) Να απεγκαταστήσετε αμέσως την εφαρμογή

8. Ποιος είναι ο σκοπός του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR);

Α) Να βοηθήσει τις εταιρείες να συλλέξουν περισσότερα δεδομένα
Β) Να προστατεύσει τα προσωπικά δεδομένα και τα δικαιώματα ιδιωτικότητας των ατόμων
Γ) Να αποτρέψει τους ανθρώπους από τη χρήση των κοινωνικών μέσων
Δ) Να ελέγχει τις δραστηριότητες ηλεκτρονικών αγορών

9. Ποια από τις παρακάτω ενέργειες συμβάλλει στην προστασία των δεδομένων σας σε έναν κοινόχρηστο υπολογιστή;

Α) Να παραμένετε συνδεδεμένοι για λόγους ευκολίας
Β) Να αποσυνδέεστε και να διαγράφετε το ιστορικό του προγράμματος περιήγησης μετά τη χρήση
Γ) Να επιτρέπετε στους περιηγητές να αποθηκεύουν τους κωδικούς πρόσβασής σας
Δ) Να μοιράζεστε τα στοιχεία σύνδεσής σας με μέλη της οικογένειάς σας

10. Τι πρέπει να κάνετε αν υποψιάζεστε ότι τα προσωπικά σας δεδομένα έχουν κλαπεί;

Α) Να το αγνοήσετε και να ελπίζετε ότι θα λυθεί από μόνο του
Β) Να το δημοσιεύσετε στα μέσα κοινωνικής δικτύωσης
Γ) Να το αναφέρετε στις αρμόδιες αρχές και να αλλάξετε αμέσως τους κωδικούς πρόσβασης
Δ) Μην κάνετε τίποτα, εκτός αν έχουν κλαπεί χρήματα

Περίληψη απαντήσεων

1	**B**
2	**B**
3	**C**
4	**B**
5	**B**
6	**B**
7	**B**
8	**B**
9	**B**
10	**C**

ΕΝΟΤΗΤΑ V

Ασφαλής Ψηφιοποίηση των Ηλικιωμένων

6. Ενότητα V - Ασφαλής ψηφιοποίηση των ηλικιωμένων

Η ενότητα 5 εστιάζει στην παροχή στους εκπαιδευτικούς των γνώσεων, των εργαλείων και των μεθόδων εργασίας που απαιτούνται για την αποτελεσματική υποστήριξη των ηλικιωμένων στην ασφαλή χρήση των ψηφιακών τεχνολογιών. Η ενότητα εισάγει τους συμμετέχοντες στα συγκεκριμένα χαρακτηριστικά και τις μαθησιακές ανάγκες των ηλικιωμένων, ιδίως σε σχέση με τη χρήση εφαρμογών διαδικτύου, υπηρεσιών ηλεκτρονικού ταχυδρομείου, πλατφορμών κοινωνικών μέσων και εργαλείων ηλεκτρονικής τραπεζικής.

Ιδιαίτερη έμφαση δίνεται στην ασφάλεια στον κυβερνοχώρο, με ιδιαίτερη προσοχή στην ελαχιστοποίηση των κινδύνων απάτης, εξαπάτησης και παραπληροφόρησης. Οι συμμετέχοντες εξερευνούν τις κοινές διαδικτυακές απειλές που αντιμετωπίζουν οι ηλικιωμένοι και μαθαίνουν πώς να αντιμετωπίζουν αυτούς τους κινδύνους μέσω προληπτικών στρατηγικών, σαφούς επικοινωνίας και πρακτικών οδηγιών προσαρμοσμένων σε αυτήν την ηλικιακή ομάδα.

Επιπλέον, η Ενότητα 5 παρέχει ολοκληρωμένη εκπαιδευτική υποστήριξη για την ψηφιοποίηση των ηλικιωμένων, συνδυάζοντας εργαλεία διδασκαλίας με πρακτικές ασκήσεις. Οι συμμετέχοντες αναπτύσσουν δεξιότητες για την αποτελεσματική και ενσυναίσθητη μεταφορά γνώσεων, την αντιμετώπιση προκλήσεων που σχετίζονται με την ασφάλεια στον κυβερνοχώρο και τον σχεδιασμό προσβάσιμων και υποστηρικτικών μαθησιακών περιβαλλόντων τόσο για ατομικές συνεδρίες καθοδήγησης όσο και για ομαδικές εκπαιδευτικές δραστηριότητες.

6.1 Μαθησιακοί στόχοι

Στόχος αυτού του ενότητας είναι να επιτρέψει στους συμμετέχοντες να αποκτήσουν τις εκπαιδευτικές και πρακτικές δεξιότητες που είναι απαραίτητες για να διδάξουν αποτελεσματικά στους ηλικιωμένους πώς να χρησιμοποιούν με ασφάλεια τις ψηφιακές τεχνολογίες και να τους υποστηρίξουν στην αντιμετώπιση των προκλήσεων της κυβερνοασφάλειας.

- Κατανόηση των συγκεκριμένων αναγκών των ηλικιωμένων όσον αφορά την ψηφιοποίηση.
- Εκμάθηση μεθόδων διδασκαλίας προσαρμοσμένων στους ηλικιωμένους.
- Απόκτηση δεξιοτήτων για τον εντοπισμό και την αντιμετώπιση τυπικών απειλών στον κυβερνοχώρο που στοχεύουν τους ηλικιωμένους.

6.2 Δομή, περιεχόμενο και μαθησιακά αποτελέσματα

Με την επιτυχή ολοκλήρωση αυτού του μαθήματος, οι μαθητές θα είναι σε θέση να:

- Κατανόηση των εμποδίων που αντιμετωπίζουν οι ηλικιωμένοι στην εκμάθηση της τεχνολογίας (ψυχολογικά, γνωστικά και τεχνικά), χρησιμοποιώντας πρακτικές και προσιτές μεθόδους διδασκαλίας, όπως επανάληψη, ασκήσεις σε μικρά βήματα και απλές εξηγήσεις.
- Εκμάθηση μεθόδων για την επικοινωνία των κανόνων ασφαλούς σύνδεσης, την αναγνώριση ασφαλών ιστότοπων και την προστασία προσωπικών δεδομένων, υποστηρίζοντας τους ηλικιωμένους στην ανεξάρτητη και ασφαλή χρήση των διαδικτυακών υπηρεσιών.
- Εξοικειωθείτε με τις πιο συνηθισμένες απειλές στις οποίες οι ηλικιωμένοι είναι ιδιαίτερα ευάλωτοι και μάθετε πώς να μεταφέρετε αυτές τις γνώσεις με απλό τρόπο, ώστε να ενισχύσετε την επαγρύπνηση των ηλικιωμένων.
- Μάθετε πώς να υποστηρίζετε τους ηλικιωμένους στην αναγνώριση των διαδικτυακών απειλών και στην ανάπτυξη ασφαλών συνηθειών μέσω ασκήσεων και σεναρίων κατάστασης.

- ❖ Μάθετε ποιες ενέργειες πρέπει να κάνετε σε περίπτωση απειλής, όπως η άμεση αλλαγή κωδικών πρόσβασης ή η αποσύνδεση μιας συσκευής από το δίκτυο, και κατανοήστε ποια δεδομένα είναι βασικά για την προστασία σε περίπτωση απειλής.
- ❖ Γνωρίστε τις διαδικασίες αναφοράς περιστατικών κυβερνοαπειλών, όπως η επικοινωνία με την τράπεζά σας, την αστυνομία ή εξειδικευμένους οργανισμούς, και μάθετε ποιες πηγές υποστήριξης υπάρχουν για τα θύματα εγκλημάτων στον κυβερνοχώρο.
- ❖ Εξηγήστε τις μεθόδους των κανόνων ασφαλείας σε εφαρμογές άμεσων μηνυμάτων, ηλεκτρονικού ταχυδρομείου και βιντεοκλήσεων και πώς να διεξάγετε ασκήσεις για την αναγνώριση των διαδικτυακών απειλών.
- ❖ Παροχή γνώσεων σχετικά με την προστασία των συσκευών από ιούς και βήμα προς βήμα εκμάθηση της ενημέρωσης των συστημάτων με τρόπο προσιτό και κατανοητό.

6.3 Ατζέντα I Λεπτομερής σχέδιο συνεδρίας

ΕΝΌΤΗΤΑ V
Ασφαλής ψηφιοποίηση των ηλικιωμένων

1η Συνεδρία

Καλωσόρισμα
Διάρκεια 5

Μαθησιακοί στόχοι

- ❖ Δημιουργία μιας ανοιχτής και ελκυστικής ατμόσφαιρας που ενθαρρύνει την ενεργό συμμετοχή.

Περιεχόμενο/Μέθοδος

- ❖ Καλωσόρισμα των συμμετεχόντων, σύντομη παρουσίαση του εκπαιδευτή. Ο εκπαιδευτής παρουσιάζει το πρόγραμμα εκπαίδευσης και τους κανόνες εργασίας.

Υλικό
Δεν απαιτείται πρόσθετο υλικό.

Σχόλια
Μπορεί να είναι χρήσιμο να εξηγηθεί ο στόχος του εργαστηρίου με απλή γλώσσα.

2η Συνεδρία

Δραστηριότητα για το σπάσιμο του πάγου
Διάρκεια 15

Μαθησιακοί στόχοι

- ❖ Δημιουργία φιλικών σχέσεων μεταξύ των συμμετεχόντων, γνωριμία μεταξύ τους και ενεργοποίηση της ομάδας πριν από την έναρξη του ουσιαστικού μέρους.

Περιεχόμενο/Μέθοδος

- Μια σύντομη άσκηση ενεργοποίησης που ξεκινά μια συζήτηση: «Ποιες προκλήσεις αντιμετωπίζουν όταν διδάσκουν νέες τεχνολογίες σε ηλικιωμένους; Πώς τις αντιμετωπίζουν;» Ο εκπαιδευτής μπορεί να προσθέσει υποστηρικτικές ερωτήσεις που θα επηρεάσουν την εξέλιξη της συζήτησης: Τι σας εξέπληξε; Ποιες μέθοδοι αποδείχθηκαν πιο αποτελεσματικές; Πώς μπορεί να προσαρμοστεί ο ρυθμός ή η μορφή των μαθημάτων στις ατομικές ανάγκες των συμμετεχόντων; Κάθε συμμετέχων μπορεί να παρουσιάσει μία πρόκληση.

Υλικό

Δεν απαιτείται πρόσθετο υλικό.

Σχόλια

Είναι χρήσιμο να γράψετε τις απαντήσεις των συμμετεχόντων σε έναν πίνακα ή σε ένα flipchart για να εντοπίσετε τις πιο συνηθισμένες δυσκολίες.

3η Συνεδρία

Διάλεξη 1: Πρακτικές συμβουλές για το πώς να διδάξετε στους ηλικιωμένους την ασφάλεια στον κυβερνοχώρο και τις νέες τεχνολογίες

Διάρκεια *25*

Μαθησιακοί στόχοι

- Ευαισθητοποίηση των εκπαιδευτικών σχετικά με τα εμπόδια που αντιμετωπίζουν οι ηλικιωμένοι κατά την εκμάθηση της χρήσης νέων τεχνολογιών και παροχή αποτελεσματικών εργαλείων διδασκαλίας για την υποστήριξη της μαθησιακής διαδικασίας.
- Παροχή γνώσεων και μεθόδων στους εκπαιδευτικούς για τη διδασκαλία των αρχών της ασφαλούς χρήσης των διαδικτυακών εφαρμογών στους ηλικιωμένους, ενισχύοντας την αίσθηση ασφάλειας και τις ψηφιακές τους ικανότητες.

Περιεχόμενο/Μέθοδος

- Η διάλεξη χωρίζεται σε δύο θεματικές ενότητες:

Θέμα 1: Μέθοδοι αποτελεσματικής διδασκαλίας των ηλικιωμένων στον τομέα της κυβερνοασφάλειας και των νέων τεχνολογιών

Περιεχόμενο/Μέθοδοι:

- Προσδιορισμός ψυχολογικών εμποδίων (π.χ. φόβος της τεχνολογίας, χαμηλή αυτοπεποίθηση), γνωστικών εμποδίων (π.χ. βραδύτερη επεξεργασία πληροφοριών, δυσκολία συγκέντρωσης) και τεχνικών εμποδίων (έλλειψη εμπειρίας με συσκευές).
- Συζήτηση των αρχών της φιλικής επικοινωνίας με τους ηλικιωμένους.

Υλικό:

Διδακτικό βοήθημα για εκπαιδευτικούς: Πρακτικές μέθοδοι διδασκαλίας ηλικιωμένων – υλικό ασκήσεων για εκπαιδευτικούς (Παράρτημα 1)

Θέμα 2: Προετοιμασία των εκπαιδευτικών για τη διδασκαλία των αρχών της ασφαλούς χρήσης των διαδικτυακών εφαρμογών (τραπεζικές συναλλαγές, αγορές, ιστότοποι κοινωνικής δικτύωσης) σε ηλικιωμένους

Περιεχόμενο / Μέθοδοι:

- Ανασκόπηση δημοφιλών διαδικτυακών εφαρμογών που χρησιμοποιούν οι ηλικιωμένοι.
- Εκμάθηση αναγνώρισης ασφαλών ιστότοπων και εφαρμογών (πιστοποιητικά, διευθύνσεις URL, εμφάνιση φορμών σύνδεσης).
- Συζήτηση σχετικά με τις αρχές δημιουργίας ασφαλών κωδικών πρόσβασης και αποθήκευσης δεδομένων σύνδεσης.
- Πρακτικές ασκήσεις σε εικονικούς λογαριασμούς: σύνδεση, έλεγχος της ασφάλειας του ιστότοπου, προσομοίωση ηλεκτρονικών αγορών.

Υλικό:

Διδακτικό βοήθημα για εκπαιδευτικούς: Πρακτικές ασκήσεις – διδασκαλία των αρχών της ασφάλειας στον κυβερνοχώρο για ηλικιωμένους σε εκπαιδευτικούς (Παράρτημα 2)

Σχόλια

Είναι χρήσιμο να γράφετε τις απαντήσεις των συμμετεχόντων σε έναν πίνακα ή σε ένα flipchart για να εντοπίσετε τις πιο συνηθισμένες δυσκολίες.

Δραστηριότητα 1: Προσδιορισμός των εμποδίων στη μάθηση των ηλικιωμένων
Διάρκεια 15

Μαθησιακοί στόχοι

- Αύξηση της ευαισθητοποίησης σχετικά με τη μαθησιακή διαδικασία των ηλικιωμένων.
- Αναγνώριση των εμποδίων στη μάθηση των ηλικιωμένων.

Περιεχόμενο/Μέθοδος

- Η άσκηση πραγματοποιείται ατομικά ή σε ζευγάρια, ανάλογα με τις προτιμήσεις των συμμετεχόντων.
- Οι συμμετέχοντες λαμβάνουν φύλλα εργασίας (Παράρτημα 3), τα οποία περιέχουν μια εργασία που συνίσταται στην ανάλυση των πιθανών εμποδίων στη μαθησιακή διαδικασία των ηλικιωμένων.
- Οι συμμετέχοντες καλούνται να εντοπίσουν παραδείγματα ψυχολογικών, γνωστικών και τεχνικών εμποδίων που μπορεί να εμφανιστούν στους ηλικιωμένους κατά τη διάρκεια της μάθησής τους.
- Στη συνέχεια, προτείνουν τρόπους για να ξεπεραστούν αυτά τα εμπόδια και περιγράφουν πώς μπορεί να επηρεάσουν τη μαθησιακή διαδικασία των ηλικιωμένων.
- Η άσκηση ολοκληρώνεται με μια συζήτηση υπό την καθοδήγηση του συντονιστή, κατά τη διάρκεια της οποίας οι συμμετέχοντες μοιράζονται τα συμπεράσματά τους και τις εμπειρίες τους.

Υλικό

- Φύλλο εργασίας – Προσδιορισμός εμποδίων στη μάθηση των ηλικιωμένων (Παράρτημα 3)

Σχόλια

Αξίζει να ενθαρρύνετε τους συμμετέχοντες να συμμετάσχουν ενεργά στη συζήτηση.

Διάλειμμα | Διάρκεια *5'*

- **Δώστε χρόνο στους συμμετέχοντες να αναζωογονηθούν και να σκεφτούν.**
- **Σύντομο διάλειμμα για ανανέωση.**

4η Συνεδρία

Διάλεξη 2: Εισαγωγή στην κυβερνοασφάλεια για ηλικιωμένους
Διάρκεια *35'*

Μαθησιακοί στόχοι

- Εξοικείωση με τις πιο συνηθισμένες απειλές στις οποίες είναι ιδιαίτερα ευάλωτοι οι ηλικιωμένοι και εκμάθηση του τρόπου με τον οποίο μπορείτε να μεταδώσετε αυτές τις γνώσεις με προσιτό και αποτελεσματικό τρόπο, ώστε να ενισχύσετε την επαγρύπνηση των ηλικιωμένων και να αυξήσετε την ασφάλειά τους στο Διαδίκτυο.
- Απόκτηση γνώσεων σχετικά με τον τρόπο υποστήριξης των ηλικιωμένων στην αναγνώριση των διαδικτυακών απειλών και τον τρόπο διαμόρφωσης συνηθειών ασφαλούς χρήσης του Διαδικτύου, αυξάνοντας έτσι την ψηφιακή τους ευαισθητοποίηση.

Περιεχόμενο/Μέθοδος

- Η διάλεξη χωρίζεται σε δύο θεματικές ενότητες:

Θέμα 1: Συνηθισμένες ψηφιακές απειλές και οι ανάγκες των ηλικιωμένων

Περιεχόμενο/Μέθοδοι:

- Συζήτηση για τις κοινές διαδικτυακές απειλές, όπως το phishing, η διαδικτυακή απάτη, η κλοπή δεδομένων, τα ψευδή νέα.
- Προσδιορισμός συγκεκριμένων κινδύνων στους οποίους οι ηλικιωμένοι είναι πιο ευάλωτοι.
- Συμβουλές για τον αποτελεσματικό τρόπο ενημέρωσης των ηλικιωμένων σχετικά με αυτές τις απειλές, χωρίς να προκαλείται άσκοπος φόβος.
- Παραδείγματα διαδικτυακών απάτων που ενδέχεται να αντιμετωπίσουν οι ηλικιωμένοι και πώς να τις αναγνωρίσουν.

Υλικό:

Διδακτικό βοήθημα για εκπαιδευτικούς: Ασφαλής χρήση του Διαδικτύου από ηλικιωμένους (Παράρτημα 4)

Θέμα 2: Ανάπτυξη ψηφιακής ευαισθητοποίησης μεταξύ των ηλικιωμένων

Περιεχόμενο/Μέθοδοι:

- Συζήτηση μεθόδων για την υποστήριξη των ηλικιωμένων στην εκμάθηση του τρόπου αναγνώρισης ύποπτων καταστάσεων στο Διαδίκτυο.
- Παραδείγματα ασκήσεων που βοηθούν τους ηλικιωμένους να θυμούνται τις αρχές της ασφάλειας στον κυβερνοχώρο.
- Προσομοιώσεις καταστάσεων στο Διαδίκτυο στις οποίες οι ηλικιωμένοι ενδέχεται να κάνουν λάθη και τρόποι για να τους βοηθήσετε αποτελεσματικά να μάθουν να αποφεύγουν αυτά τα λάθη.

Υλικό:

Διδακτικό βοήθημα για εκπαιδευτικούς: Αναγνώριση απειλών στο Διαδίκτυο (Παράρτημα 5)

Σχόλια

Ενθαρρύνετε τους συμμετέχοντες να μοιραστούν εμπειρίες από τη συνεργασία τους με ηλικιωμένους και παραδείγματα αποτελεσματικών μεθόδων για την εξήγηση δύσκολων θεμάτων.

Δραστηριότητα 2: Άσκηση προσομοίωσης: συζήτηση με έναν ηλικιωμένο για την ασφάλεια στον κυβερνοχώρο

Διάρκεια *15*

Μαθησιακοί στόχοι

- Να δοθεί η δυνατότητα στον εκπαιδευτικό να μιλήσει με τον ηλικιωμένο, βοηθώντας τον να κατανοήσει πώς να αποφεύγει τις διαδικτυακές απειλές.

Περιεχόμενο/Μέθοδος

- Η άσκηση πραγματοποιείται σε ζευγάρια, στα οποία οι συμμετέχοντες εναλλάσσονται μεταξύ των ρόλων του εκπαιδευτικού και του ηλικιωμένου. Στόχος της άσκησης είναι η διεξαγωγή μιας προσομοίωσης εκπαιδευτικής συζήτησης σχετικά με τις απειλές στο Διαδίκτυο, λαμβάνοντας υπόψη πραγματικές καταστάσεις που ενδέχεται να αντιμετωπίσουν οι ηλικιωμένοι. Κάθε ζευγάρι λαμβάνει μια περιγραφή που παρουσιάζει μια συγκεκριμένη απειλή (Παράρτημα 6).
- Ο ρόλος του εκπαιδευτικού συνίσταται σε μια ήρεμη, κατανοητή εξήγηση του τι είναι μια δεδομένη απειλή, πώς να την αναγνωρίσετε και πώς να αντιδράσετε. Ο ρόλος του ηλικιωμένου σας επιτρέπει να αναλάβετε τον ρόλο ενός ατόμου που μπορεί να έχει περιορισμένες ψηφιακές γνώσεις και χρειάζεται σαφείς, φιλικές οδηγίες. Η άσκηση τελειώνει με μια κοινή συζήτηση που συντονίζει ο ηγέτης, κατά τη διάρκεια της οποίας οι συμμετέχοντες μοιράζονται τα συναισθήματα, τα συμπεράσματα και τις σκέψεις τους σχετικά με την αποτελεσματική εκπαιδευτική επικοινωνία με τους ηλικιωμένους.

Υλικό

- Άσκηση προσομοίωσης: Συζήτηση με έναν ηλικιωμένο για την ασφάλεια στον κυβερνοχώρο (Παράρτημα 6)

Σχόλια

Αξίζει να δοθεί προσοχή στη σαφήνεια της γλώσσας και να αποφεύγεται η τεχνική ορολογία.

Διάλειμμα | Διάρκεια *5'*

- **Δώστε χρόνο για ξεκούραση και προετοιμασία για την επόμενη συνεδρία.**
- **Ένα σύντομο διάλειμμα για να αναζωογονηθείτε.**

5η Συνεδρία

Διάλεξη 3: Αντιμετώπιση των απειλών στον κυβερνοχώρο
Διάρκεια *30*

Μαθησιακοί στόχοι

- Προετοιμασία των εκπαιδευτικών ώστε να παρέχουν αποτελεσματικά στους ηλικιωμένους γνώσεις σχετικά με τις ψηφιακές απειλές και τον τρόπο αποφυγής τους.
- Ανάπτυξη των δεξιοτήτων των εκπαιδευτικών στη διεξαγωγή μαθημάτων με ηλικιωμένους σχετικά με την αντιμετώπιση των απειλών στον κυβερνοχώρο.
- Ενίσχυση των ικανοτήτων των εκπαιδευτικών στη χρήση μεθόδων ενεργοποίησης και μεθόδων προσαρμοσμένων στις ανάγκες των ηλικιωμένων.

Περιεχόμενο/Μέθοδος

- Η διάλεξη χωρίζεται σε δύο θεματικές ενότητες:

Θέμα 1: Μέτρα που πρέπει να ληφθούν σε περίπτωση υποψίας κυβερνοεπίθεσης
Περιεχόμενο/Μέθοδοι:
Ο εκπαιδευτής συζητά:

- τα πιο συνηθισμένα συμπτώματα μιας πιθανής κυβερνοεπίθεσης (π.χ. παράξενη συμπεριφορά της συσκευής, ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα σφάλματος, ξαφνικές αποσυνδέσεις)
- βασικούς κανόνες ασφάλειας - πώς να αντιδράσετε σε περίπτωση υποψίας επίθεσης: άμεση αποσύνδεση από το δίκτυο, αλλαγή κωδικών πρόσβασης, μη άνοιγμα ύποπτων συνημμένων ή συνδέσμων
- τη σημασία της διατήρησης της ψυχραιμίας και της αποφυγής βεβιασμένων ενεργειών (π.χ. μη επανάκληση άγνωστων αριθμών, μη κλικ σε προειδοποιήσεις για phishing)
- τρόπους δημιουργίας ασφαλών κωδικών πρόσβασης και ενημέρωσής τους - συμπεριλαμβανομένης της αποφυγής γενεθλίων και απλών συνδυασμών.

Θέμα 2: Πώς να αναφέρετε ψηφιακές απειλές και πού να ζητήσετε βοήθεια
Περιεχόμενο/Μέθοδοι:
Ο εκπαιδευτής συζητά:

- ιδρύματα και μέρη όπου μπορείτε να αναφέρετε απειλές στον κυβερνοχώρο (π.χ. CERT Polska, τηλεφωνικές γραμμές τραπεζών, τοπική αστυνομία, οργανώσεις που υποστηρίζουν ηλικιωμένους)
- πότε και πώς να επικοινωνήσετε με την τράπεζα - π.χ. όταν υποψιάζεστε ότι έχει γίνει παραβίαση του λογαριασμού σας ή μη εξουσιοδοτημένη συναλλαγή

- πώς να προετοιμαστείτε για την αναφορά - σημειώνοντας την ημερομηνία, την ώρα, το περιεχόμενο του μηνύματος, λαμβάνοντας ένα screenshot, αποθηκεύοντας ύποπτα μηνύματα
- το ρόλο της συναισθηματικής και ενημερωτικής υποστήριξης - πώς και πού να την αναζητήσετε (τηλεφωνικές γραμμές, συμβουλευτικά κέντρα, αγαπημένα πρόσωπα)
- η σημασία της αναφοράς απόπειρας απάτης, ακόμη και αν δεν έχουν προκύψει απώλειες - για το καλό των άλλων χρηστών.

Υλικό

- Διδακτικό βοήθημα για εκπαιδευτικούς: Προσομοιώσεις σεναρίων (Παράρτημα 7)

Σχόλια

Αξίζει να ενθαρρύνετε τους συμμετέχοντες να συμμετάσχουν στη συζήτηση.

Δραστηριότητα 3: Άσκηση αναγνώρισης απάτης
Διάρκεια 20

Μαθησιακοί στόχοι

- Απόκτηση γνώσεων σχετικά με τον τρόπο με τον οποίο μπορείτε να βοηθήσετε τους ηλικιωμένους να παραμείνουν ψύχραιμοι και ήρεμοι σε καταστάσεις που ενέχουν απειλές στο διαδίκτυο (π.χ. απόπειρες απάτης, ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου, άγνωστες τηλεφωνικές κλήσεις).
- Ανάπτυξη της ικανότητας λήψης ορθολογικών αποφάσεων, αποφυγής βιαστικών ενεργειών και επικοινωνίας με τα κατάλληλα άτομα και φορείς.

Περιεχόμενο/Μέθοδος

- Η άσκηση συνίσταται στην προσομοίωση μιας συνομιλίας μεταξύ ενός ηλικιωμένου και ενός εκπαιδευτικού.
- Οι συμμετέχοντες εργάζονται σε ζεύγη, αναλαμβάνοντας τους ρόλους που τους έχουν ανατεθεί: εκπαιδευτικός και ηλικιωμένος. Οι συμμετέχοντες έχουν πρόσβαση σε συμβουλές και θέματα προσομοίωσης (Παράρτημα 8), τα οποία τους βοηθούν να διεξάγουν μια ρεαλιστική συνομιλία σχετικά με τις απειλές στον κυβερνοχώρο. Μετά το τέλος της προσομοίωσης, ο συντονιστής διευθύνει τη συζήτηση. Κάθε ζεύγος μοιράζεται τις σκέψεις του με την ομάδα, συζητώντας τις δυσκολίες που αντιμετώπισε, τα συναισθήματα και τις αποτελεσματικές στρατηγικές επικοινωνίας. Η συζήτηση βοηθά στην καλύτερη κατανόηση των μεθόδων υποστήριξης των ηλικιωμένων στην αναγνώριση των απειλών και στην εκμάθηση του τρόπου κατάλληλης αντίδρασης σε αυτές.

Υλικό

- Άσκηση προσομοίωσης: Δείγματα αναφορών για απειλές στον κυβερνοχώρο (Παράρτημα 8)

Σχόλια

Είναι σημαντικό οι εκπαιδευτικοί να είναι καλά προετοιμασμένοι για να προσελκύσουν τους ηλικιωμένους και να τους παρακινήσουν να συμμετάσχουν ενεργά στη μάθηση, χρησιμοποιώντας παραδείγματα από την καθημερινή τους ζωή.

Διάλειμμα | Διάρκεια 5'

- **Δώστε χρόνο για ξεκούραση και προετοιμασία.**
- **Σύντομο διάλειμμα για ανανέωση.**
- **Σύντομο διάλειμμα για αναζωογόνηση και χαλάρωση.**

6η Συνεδρία

Διάλεξη 4: Εκπαίδευση ηλικιωμένων στη χρήση ηλεκτρονικών συσκευών και διαδικτυακών εφαρμογών – οδηγός για εκπαιδευτικούς
Διάρκεια *20'*

Μαθησιακοί στόχοι

- Εξοπλισμός των εκπαιδευτικών με εργαλεία και μεθόδους που επιτρέπουν την αποτελεσματική διδασκαλία των ηλικιωμένων σχετικά με τις αρχές της ασφαλούς χρήσης εφαρμογών επικοινωνίας, όπως το ηλεκτρονικό ταχυδρομείο, τα προγράμματα άμεσων μηνυμάτων (π.χ. Messenger, WhatsApp) και οι εφαρμογές βιντεοκλήσεων (π.χ. Zoom).
- Προετοιμασία των εκπαιδευτικών για τη διεξαγωγή μαθημάτων σχετικά με την προστασία των ψηφιακών συσκευών των ηλικιωμένων – από τη βασική χρήση προγραμμάτων προστασίας από ιούς έως την εκμάθηση του τρόπου ενημέρωσης του λειτουργικού συστήματος και των εφαρμογών.

Περιεχόμενο/Μέθοδος

- Η διάλεξη χωρίζεται σε δύο θεματικές ενότητες:

Θέμα 1: Πώς να διδάξετε στους ηλικιωμένους την ασφαλή χρήση των εφαρμογών επικοινωνίας
Περιεχόμενο/μέθοδοι:

- Τρόποι εξήγησης των βασικών λειτουργιών των εφαρμογών επικοινωνίας με απλή, καθημερινή γλώσσα.
- Παραδείγματα ασκήσεων που βοηθούν στην αναγνώριση επικίνδυνων μηνυμάτων (spam, phishing), π.χ. ανάλυση πραγματικών και ψεύτικων μηνυμάτων ηλεκτρονικού ταχυδρομείου.
- Πρακτικές επιδείξεις των ρυθμίσεων απορρήτου και ασφάλειας στις εφαρμογές - αποκλεισμός άγνωστων επαφών, αλλαγή κωδικών πρόσβασης, ρυθμίσεις απορρήτου.
- Μέθοδοι ενεργοποίησης: εργασία με λίστα ελέγχου, προσομοιώσεις επικίνδυνων καταστάσεων, από κοινού επίλυση σεναρίων.

Υλικό:
Διδακτικό βοήθημα για εκπαιδευτικούς: Πώς να διδάξετε στους ηλικιωμένους την ασφαλή χρήση των εφαρμογών επικοινωνίας (Παράρτημα 9)

Θέμα 2: Πώς να διδάξετε στους ηλικιωμένους να χρησιμοποιούν antivirus και ενημερώσεις συστήματος
Περιεχόμενο/μέθοδοι:

- Πώς να εξηγήσετε στους ηλικιωμένους με κατανοητό τρόπο τις έννοιες: ιός υπολογιστή, ενημέρωση, σάρωση συστήματος.

- Ομαδικές ασκήσεις σχετικά με την εγκατάσταση και τη χρήση δωρεάν προγραμμάτων προστασίας από ιούς (π.χ. Avast, AVG).
- Βήμα προς βήμα: πώς να δείξετε στους ηλικιωμένους πώς να εκτελούν ενημερώσεις συστήματος και εφαρμογών.

Υλικό:
Διδακτικό βοήθημα για εκπαιδευτικούς: Πώς να διδάξετε στους ηλικιωμένους τη χρήση των αντιϊικών προγραμμάτων και των ενημερώσεων συστήματος (Παράρτημα 10)

Σχόλια
Κατά τη διάρκεια της συζήτησης, είναι σημαντικό να εξασφαλιστεί η ανταλλαγή ιδεών μεταξύ των συμμετεχόντων.

Δραστηριότητα 4: Πρακτικές συμβουλές και τεχνικές για ηλικιωμένους
Διάρκεια *30*

Μαθησιακοί στόχοι

- Ανάπτυξη της ικανότητας παροχής απλών και αποτελεσματικών συμβουλών στους ηλικιωμένους σχετικά με την ασφαλή χρήση του Διαδικτύου.
- Ανάπτυξη της ικανότητας αναγνώρισης και εφαρμογής διδακτικών τεχνικών που είναι κατανοητές και προσβάσιμες στους ηλικιωμένους.
- Ανταλλαγή καλών πρακτικών και πραγματικών εμπειριών από τη συνεργασία με ηλικιωμένους, που μπορούν να αποτελέσουν πηγή έμπνευσης για άλλους εκπαιδευτικούς.

Περιεχόμενο/Μέθοδος

- Η άσκηση αποτελείται από δύο στάδια εργασίας: ατομικό και ομαδικό. Στο πρώτο στάδιο, οι συμμετέχοντες συμπληρώνουν ανεξάρτητα το φύλλο εργασίας (Παράρτημα 11), καταγράφοντας τις δικές τους σκέψεις, παρατηρήσεις και ιδέες σχετικά με αποτελεσματικές μεθόδους διδασκαλίας των ηλικιωμένων για την ασφάλεια στον κυβερνοχώρο. Στο δεύτερο στάδιο, οι συμμετέχοντες μοιράζονται τις σκέψεις τους στο φόρουμ ολόκληρης της ομάδας, το οποίο διευκολύνει την ανταλλαγή εμπειριών και την αναζήτηση εμπνευσμένων λύσεων και αποδεδειγμένων πρακτικών. Η κοινή συζήτηση επιτρέπει τη συμπλήρωση των γνώσεων, τον εμπλουτισμό των προοπτικών και την αναγνώριση διαφορετικών στυλ εκπαιδευτικής εργασίας με ηλικιωμένους. Στο τέλος της άσκησης, ο συντονιστής ξεκινά μια συζήτηση με στόχο την εμβάθυνση του θέματος.

Υλικό

- Φύλλο εργασίας: Ασφαλής χρήση του Διαδικτύου: Πρακτικές συμβουλές και τεχνικές για ηλικιωμένους (Παράρτημα 11)

Σχόλια
Αξίζει να ενθαρρύνετε τους συμμετέχοντες να κάνουν ερωτήσεις κατά τη διάρκεια της άσκησης.

7η Συνεδρία

Συζήτηση | Διάρκεια 10’

Μαθησιακοί στόχοι

- Να δοθεί η ευκαιρία στους συμμετέχοντες να μοιραστούν τις εμπειρίες και τις παρατηρήσεις τους μετά τη συνεδρία.
- Προσδιορισμός των προκλήσεων που σχετίζονται με τη διδασκαλία ηλικιωμένων.
- Διοργάνωση συλλογικής συνεδρίας ανταλλαγής ιδεών για τη βελτίωση της εργασίας με ομάδες ηλικιωμένων.

Περιεχόμενο/Μέθοδος

- Ο εκπαιδευτής ξεκινά μια ανοιχτή συζήτηση με ερωτήσεις όπως: «Ποιο ήταν το πιο δύσκολο μέρος;», «Ποιοι τομείς χρειάζονται περαιτέρω ανάπτυξη;», «Πώς μπορεί να απλοποιηθεί η διδασκαλία σε ηλικιωμένους;» Οι συμμετέχοντες μοιράζονται τις σκέψεις, τις πρακτικές και τα συμπεράσματά τους από τη συνεδρία. Τα συμπεράσματα γράφονται σε ένα flipchart ή σε έναν πίνακα, ώστε να είναι πιο εύκολο να συνοψιστούν και να χρησιμοποιηθούν ενδεχομένως στο μέλλον.

Υλικό

- Πίνακας παρουσιάσεων ή λευκός πίνακας
- Μαρκαδόροι

Σύνοψη | Διάρκεια 5’

Μαθησιακοί στόχοι

- Σύνοψη των βασικών πληροφοριών, απάντηση στις τελευταίες ερωτήσεις των συμμετεχόντων και αναφορά σε πηγές για περαιτέρω μάθηση.

Περιεχόμενο/Μέθοδος

- Σύντομη υπενθύμιση των πιο σημαντικών θεμάτων που καλύφθηκαν κατά τη διάρκεια της εκπαίδευσης.
- Αναφορά σε πρόσθετες πηγές γνώσης (π.χ. εκπαιδευτικοί ιστότοποι, βίντεο).
- Ευχαριστίες στους συμμετέχοντες για τη συμμετοχή τους και λήξη της συνεδρίας.

Υλικό

- Διδακτικό βοήθημα για εκπαιδευτικούς: Ιστοσελίδες για την ασφαλή χρήση της τεχνολογίας (Παράρτημα 12).

Σχόλια

Στο τέλος, είναι καλή ιδέα να διεξαχθεί μια σύντομη έρευνα αξιολόγησης.

6.4 Πρόσθετες πληροφορίες

6.4.1 Αυτοανασκόπηση των εκπαιδευτών

- Ποιο ήταν το πιο δύσκολο πράγμα για τους συμμετέχοντες να κατανοήσουν σχετικά με την ασφάλεια στον κυβερνοχώρο;
- Ποιες μέθοδοι ήταν πιο αποτελεσματικές κατά τη διάρκεια της εκπαίδευσης;
- Ποιες αλλαγές θα μπορούσαν να βελτιώσουν την εμπειρία των συμμετεχόντων κατά τη διάρκεια της άσκησης;
- Αισθάνθηκαν οι συμμετέχοντες άνετα να μοιραστούν τις εμπειρίες και τις ανησυχίες τους σχετικά με τη μάθηση των ηλικιωμένων;

6.4.2 Αξιολόγηση του προγράμματος από τους εκπαιδευτές

- Επιτεύχθηκαν οι στόχοι της εκπαίδευσης;
- Ποια θέματα απαιτούν επέκταση ή τροποποίηση στο μέλλον;
- Ποιες διδακτικές τεχνικές ήταν πιο αποτελεσματικές με αυτή την ομάδα συμμετεχόντων;

6.4.3 Υλικό, πρόσθετοι πόροι

Παράρτημα 1 | Πρακτικές μέθοδοι διδασκαλίας ηλικιωμένων – Υλικό ασκήσεων για εκπαιδευτικούς

Συμπληρώστε τις ασκήσεις του εκπαιδευτικού για κάθε μέθοδο (π.χ. δημιουργήστε οδηγούς, προτείνετε αναλογίες, σχεδιάστε οπτικά βοηθήματα ή περιγράψτε απαντήσεις).

Επανάληψη και ασκήσεις βήμα προς βήμα

- **Περιγραφή μεθόδου:** Σύντομες, επαναλαμβανόμενες οδηγίες, κάθε δραστηριότητα χωρίζεται σε απλά βήματα.
- **Άσκηση για εκπαιδευτικούς:** Αναπτύξτε έναν οδηγό βήμα προς βήμα για τη σύνδεση σε μια πλατφόρμα κοινωνικών μέσων ή ένα σύστημα ηλεκτρονικής τραπεζικής (χρησιμοποιώντας απλή και σαφή γλώσσα).
- **Στόχος:** Να αναπτύξετε την ικανότητα να διατυπώνετε εργασίες με λογική και εύκολη στην κατανόηση δομή.

Χρήση οπτικοποιήσεων και παραδειγμάτων από την πραγματική ζωή

- **Περιγραφή μεθόδου:** Σύνδεση αφηρημένων τεχνολογικών εννοιών με τις καθημερινές εμπειρίες των ηλικιωμένων (π.χ. σύγκριση ενός κωδικού πρόσβασης με ένα κλειδί σπιτιού).
- **Άσκηση για εκπαιδευτικούς:** Προτείνετε 3 αναλογίες για να εξηγήσετε στους ηλικιωμένους τα εξής: κωδικός πρόσβασης, ασφαλής ιστότοπος και phishing.
- **Στόχος:** Να βοηθήσετε τους ηλικιωμένους να κατανοήσουν σύνθετες έννοιες μέσω αναφορών σε οικείες καταστάσεις.

Χρήση υλικού με μεγάλα γράμματα

- **Περιγραφή μεθόδου:** Χρήση μεγεθυμένων γραμμάτων, χρωμάτων υψηλής αντίθεσης, εικονογραμμάτων και διαγραμμάτων.
- **Άσκηση για τον εκπαιδευτικό:** Προετοιμάστε ένα παράδειγμα κάρτας οπτικής βοήθειας για ηλικιωμένους που περιλαμβάνει τις αρχές της δημιουργίας ενός ασφαλούς κωδικού πρόσβασης.
- **Στόχος:** Να αναπτύξετε δεξιότητες στη δημιουργία υλικού προσαρμοσμένου στις οπτικές και γνωστικές ανάγκες των ηλικιωμένων.

Διδασκαλία με ρυθμό προσαρμοσμένο στην ομάδα

- **Περιγραφή μεθόδου:** Παρατήρηση των αντιδράσεων των συμμετεχόντων, υποβολή ερωτήσεων ελέγχου και διατήρηση ευελιξίας στο ρυθμό των μαθημάτων.
- **Άσκηση για τον εκπαιδευτικό:** Περιγράψτε πώς θα αντιδρούσατε αν το ήμισυ της ομάδας δεν καταλάβαινε τη λειτουργία μιας εφαρμογής που συζητάτε – ποια μέτρα θα λαμβάνατε;
- **Στόχος:** Ανάπτυξη μιας αναστοχαστικής διδακτικής προσέγγισης και ευελιξίας κατά την εργασία με μια ομάδα με διαφορετικούς ρυθμούς μάθησης.

  Πώς να χρησιμοποιήσετε το παράρτημα:

  Το παράρτημα μπορεί να χρησιμοποιηθεί κατά τη διάρκεια των εργαστηρίων για εκπαιδευτικούς ως σύνολο ατομικών και ομαδικών ασκήσεων, υλικό για προσομοιώσεις συνεδριών κατάρτισης ηλικιωμένων και ως αφετηρία για τη δημιουργία εξατομικευμένων σχεδίων μαθήματος.

Παράρτημα 2 | Πρακτικές ασκήσεις – Διδάσκοντας στους εκπαιδευτικούς τις αρχές της ασφάλειας στον κυβερνοχώρο για ηλικιωμένους με γνώσεις πληροφορικής

Ολοκληρώστε τις πρακτικές ασκήσεις για κάθε θέμα (π.χ. ελέγξτε τις εφαρμογές, ελέγξτε την ασφάλεια του ιστότοπου, δημιουργήστε ασφαλείς κωδικούς πρόσβασης και εξασκηθείτε με δοκιμαστικούς λογαριασμούς).

Περιεχόμενο και μέθοδοι για τη συνεργασία με εκπαιδευτικούς:

1. Επισκόπηση δημοφιλών διαδικτυακών εφαρμογών που χρησιμοποιούνται από ηλικιωμένους
   - **Εργασία του εκπαιδευτικού:** Εξοικειωθείτε με τις διεπαφές εφαρμογών όπως ιστότοποι αγορών όπως το Allegro, πλατφόρμες κοινωνικών μέσων όπως το Facebook και κινητή τραπεζική.
   - **Μέθοδος:** Ανάλυση στιγμιότυπων οθόνης, αναθεώρηση διεπαφών σε κινητές συσκευές και υπολογιστές.
   - **Στόχος:** Να αναγνωρίσετε κοινά στοιχεία και πιθανές δυσκολίες που αντιμετωπίζουν οι ηλικιωμένοι.

2. Μάθηση αναγνώρισης ασφαλών ιστότοπων και εφαρμογών
   - **Πρακτική εργασία:** Εξετάστε 5 παραδείγματα ιστότοπων – προσδιορίστε ποιοι είναι ασφαλείς. Υποδείξτε το πιστοποιητικό SSL, την αξιολόγηση της διεύθυνσης URL, τις ύποπτες φόρμες σύνδεσης.
   - **Μέθοδος:** Συγκριτική ανάλυση (ασφαλείς έναντι μη ασφαλών ιστότοπων), διαδραστικό κουίζ.
   - **Στόχος:** Να διδάξει την κριτική ανάλυση της ασφάλειας των ιστότοπων.

3. Αρχές δημιουργίας ασφαλών κωδικών πρόσβασης και αποθήκευσης δεδομένων σύνδεσης
   - **Άσκηση:** Δημιουργήστε 3 ασφαλείς κωδικούς πρόσβασης χρησιμοποιώντας τον κανόνα 3C (πολυπλοκότητα, δυνατότητα αλλαγής, ευκολία απομνημόνευσης). Προτείνετε έναν ασφαλή τρόπο αποθήκευσης των στοιχείων σύνδεσης (π.χ. διαχειριστές κωδικών πρόσβασης, σημειωματάριο εκτός σύνδεσης).
   - **Μέθοδος:** Ανταλλαγή ιδεών, συζήτηση + μίνι εργαστήριο για τη δημιουργία κωδικών πρόσβασης.
   - **Στόχος:** Να κατανοήσετε και να μεταδώσετε τις αρχές ασφάλειας με απλό και πειστικό τρόπο.

4. Πρακτικές ασκήσεις με χρήση φανταστικών λογαριασμών
   - **Εργασία:** Συνδεθείτε σε έναν δοκιμαστικό τραπεζικό λογαριασμό ή λογαριασμό ηλεκτρονικού καταστήματος (προσομοίωση), πραγματοποιήστε μια ασφαλή «αγορά» και ελέγξτε τα στοιχεία ασφαλείας στον ιστότοπο.
   - **Μέθοδος:** Εργασία σε ζεύγη με υπολογιστές/ταμπλέτες, σενάρια κατάστασης.
   - **Στόχος:** Να μετατρέψετε τις θεωρητικές γνώσεις σε πρακτικές δεξιότητες που οι εκπαιδευτικοί μπορούν να μεταδώσουν στους ηλικιωμένους.

Παράρτημα 3 | Φύλλο εργασίας: Προσδιορισμός των εμποδίων στη μάθηση των ηλικιωμένων

Συμπληρώστε το φύλλο εργασίας εντοπίζοντας τα εμπόδια (ψυχολογικά, γνωστικά, τεχνικά)

Ψυχολογικά εμπόδια	Παράδειγμα	Πώς να τα ξεπεράσετε	Επίδραση στη μάθηση
Φόβος αποτυχίας			
Έλλειψη αυτοπεποίθησης			
Περιορισμένη κινητοποίηση			
Γνωστικά εμπόδια	Παράδειγμα	Πώς να το λύσετε	Επίδραση στη μάθηση
Αργότερη απομνημόνευση			
Δυσκολίες συγκέντρωσης			
Προβλήματα βραχυπρόθεσμης μνήμης			
Τεχνικά εμπόδια	Παράδειγμα	Πώς να το λύσετε	Επίδραση στη μάθηση
Δυσκολίες στη χρήση της τεχνολογίας			
Έλλειψη εμπειρίας στη χρήση του Διαδικτύου			
Προβλήματα στη χρήση νέων εκπαιδευτικών πλατφορμών			

Παράρτημα 4 | Ασφαλής χρήση του Διαδικτύου από ηλικιωμένους

Παρουσιάστε παραδείγματα, συζητήστε πραγματικές απειλές και πραγματοποιήστε διαδραστικές ασκήσεις για να διδάξετε στους ηλικιωμένους την ασφάλεια στο Διαδίκτυο.

1. Παρουσιάσεις με παραδείγματα διαδικτυακών απάτων

- **Περιγραφή:** Οι παρουσιάσεις πρέπει να περιλαμβάνουν ρεαλιστικά παραδείγματα διαδικτυακών απάτων που στοχεύουν συνήθως τους ηλικιωμένους, όπως phishing, ψεύτικες δημοπρασίες ή δόλια μηνύματα ηλεκτρονικού ταχυδρομείου. Οι εκπαιδευτικοί μπορούν να προετοιμάσουν διαφάνειες ή οπτικό υλικό που απεικονίζει συγκεκριμένες περιπτώσεις, δείχνοντας πώς να αναγνωρίζουν τα επικίνδυνα στοιχεία.
- **Στόχος:** Να ευαισθητοποιήσει τους ηλικιωμένους σχετικά με τις πιο συνηθισμένες απειλές στο διαδίκτυο. Να διδάξει την αναγνώριση των απάτων και άλλων μορφών διαδικτυακής κακοποίησης στις οποίες οι ηλικιωμένοι μπορεί να είναι ιδιαίτερα ευάλωτοι.
- **Παραδείγματα απάτης προς συζήτηση:**
  Phishing: ψεύτικα μηνύματα ηλεκτρονικού ταχυδρομείου ή ιστότοποι που προσπαθούν να κλέψουν τα στοιχεία σύνδεσης.
  Απάτες σε διαδικτυακές δημοπρασίες: ψεύτικες προσφορές πώλησης προϊόντων.
  Ψεύτικα SMS και ηλεκτρονικά μηνύματα: μηνύματα που προσποιούνται ότι προέρχονται από ιδρύματα, όπως τράπεζες.

2. Συζήτηση για τις πραγματικές απειλές στην καθημερινή ζωή των ηλικιωμένων

- **Περιγραφή:** Μετά την παρουσίαση παραδειγμάτων απάτης, είναι σημαντικό ο εκπαιδευτικός να καθοδηγήσει μια συζήτηση που θα επιτρέψει στους συμμετέχοντες να μοιραστούν τις εμπειρίες και τις γνώσεις τους σχετικά με τις διαδικτυακές απειλές που αντιμετωπίζουν οι ηλικιωμένοι. Οι εκπαιδευτικοί πρέπει να ενθαρρύνουν τους ηλικιωμένους να μιλήσουν για τις δικές τους εμπειρίες και τις δυσκολίες που αντιμετωπίζουν κατά τη χρήση της τεχνολογίας.
- **Στόχος**: Να κατανοήσουμε τους πραγματικούς κινδύνους που αντιμετωπίζουν οι ηλικιωμένοι στην καθημερινή τους ζωή. Να προσδιορίσουμε τα εμπόδια στη χρήση του διαδικτύου από τους ηλικιωμένους, όπως η έλλειψη ψηφιακών δεξιοτήτων ή οι φόβοι που σχετίζονται με την ασφάλεια.
- **Δείγματα ερωτήσεων για συζήτηση**
  - Τι είδους διαδικτυακές απάτες έχετε συναντήσει ή έχετε ακούσει;
  - Ποια είναι τα κύρια προβλήματα ασφάλειας στο διαδίκτυο που απασχολούν τους ηλικιωμένους;
  - Ποια είναι η μεγαλύτερη πρόκληση για τους ηλικιωμένους όταν μαθαίνουν να χρησιμοποιούν το διαδίκτυο;

3. Διαδραστικές ασκήσεις και προσομοιώσεις για τον εντοπισμό διαδικτυακών απειλών

- **Περιγραφή:** Οι ασκήσεις και οι προσομοιώσεις βοηθούν στην εφαρμογή των γνώσεων για την ασφάλεια στο διαδίκτυο στην πράξη. Οι ηλικιωμένοι μπορούν να συμμετάσχουν σε δραστηριότητες όπου πρέπει να εντοπίσουν ποιοι ιστότοποι ή μηνύματα είναι ασφαλείς και ποιοι μπορεί να είναι επικίνδυνοι. Οι εκπαιδευτικοί μπορούν να χρησιμοποιήσουν παραδείγματα όπως έναν φανταστικό τραπεζικό λογαριασμό, ένα ηλεκτρονικό κατάστημα ή ένα προφίλ κοινωνικών μέσων για να δείξουν σε πραγματικό χρόνο πώς να αναγνωρίζουν ύποπτα στοιχεία.
- **Στόχος:** Να ενισχυθεί η ικανότητα αναγνώρισης των απειλών στο διαδίκτυο μέσω πρακτικής εξάσκησης. Να αναπτυχθεί η ικανότητα των ηλικιωμένων να λαμβάνουν τεκμηριωμένες αποφάσεις σχετικά με την ασφάλειά τους στο διαδίκτυο.

❖ **Δείγματα ασκήσεων**

- *Άσκηση αναγνώρισης phishing:* Οι συμμετέχοντες λαμβάνουν δείγματα email και πρέπει να υποδείξουν ποια από αυτά ενδέχεται να είναι απόπειρες phishing.
- *Προσομοίωση ηλεκτρονικών αγορών:* Ομαδική ανάλυση ενός ιστότοπου ηλεκτρονικού εμπορίου, έλεγχος του τρόπου αναγνώρισης ψεύτικων προσφορών και των στοιχείων που υποδηλώνουν ότι ένας ιστότοπος είναι ασφαλής.
- *Αξιολόγηση της ασφάλειας ιστότοπων:* Επισκόπηση ιστότοπων και αναγνώριση ύποπτων στοιχείων, όπως η απουσία πιστοποιητικών SSL ή αμφίβολα έντυπα σύνδεσης.

Παράρτημα 5 | Αναγνώριση απειλών στο Διαδίκτυο

Διδάξτε στους ηλικιωμένους να αναγνωρίζουν τις διαδικτυακές απειλές και να εξασκούνται με μηνύματα ηλεκτρονικού ταχυδρομείου, συνδέσμους και κωδικούς πρόσβασης.

1. Επισκόπηση μεθόδων για την υποστήριξη των ηλικιωμένων στην αναγνώριση ύποπτων καταστάσεων στο διαδίκτυο

❖ **Περιγραφή**

Οι εκπαιδευτικοί πρέπει να χρησιμοποιούν διάφορες μεθόδους που επιτρέπουν στους ηλικιωμένους να αναγνωρίζουν ύποπτες καταστάσεις στο Διαδίκτυο. Ο κύριος στόχος είναι να δημιουργηθεί η συνειδητοποίηση ότι δεν είναι όλα όσα φαίνονται αξιόπιστα και στην πραγματικότητα είναι. Σαφείς και απλές οδηγίες μπορούν να βοηθήσουν τους ηλικιωμένους να αξιολογήσουν ανεξάρτητα εάν μια δεδομένη κατάσταση είναι ασφαλής.

❖ **Μέθοδοι**

- Βασικές αρχές για τον εντοπισμό ύποπτων καταστάσεων: Διδάξτε στους ηλικιωμένους πώς να εντοπίζουν ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα SMS ή ψεύτικους ιστότοπους. Παραδείγματα: έλλειψη πιστοποιητικού SSL, ορθογραφικά λάθη στα μηνύματα, ασυνεπείς διευθύνσεις URL.
- Ο κανόνας «μην εμπιστεύεσαι το άγνωστο»: Συζήτηση σχετικά με καταστάσεις στις οποίες οι ηλικιωμένοι ενδέχεται να λάβουν ύποπτες προσφορές (π.χ. ψεύτικες επενδυτικές ευκαιρίες, κέρδη σε διαγωνισμούς ή άγνωστα αιτήματα για προσωπικά δεδομένα).
- Εκπαίδευση μέσω αναλογιών: Σύγκριση καταστάσεων στο διαδίκτυο με σενάρια της πραγματικής ζωής, όπως η αναγνώριση ενός ύποπτου πωλητή σε μια αγορά.

2. Παραδείγματα ασκήσεων που βοηθούν τους ηλικιωμένους να θυμούνται τους κανόνες ασφάλειας στον κυβερνοχώρο

❖ **Περιγραφή**

Οι πρακτικές ασκήσεις που εμπλέκουν τους ηλικιωμένους βοηθούν στην ενίσχυση των αρχών της κυβερνοασφάλειας και της προσεκτικής συμπεριφοράς στο διαδίκτυο. Οι ηλικιωμένοι είναι πιο πιθανό να θυμούνται αυτούς τους κανόνες όταν έχουν την ευκαιρία να τους εφαρμόσουν σε ένα ασφαλές και ελεγχόμενο περιβάλλον.

❖ **Ασκήσεις**

- Αναγνώριση ψεύτικων μηνυμάτων ηλεκτρονικού ταχυδρομείου: Οι συμμετέχοντες λαμβάνουν διάφορα παραδείγματα μηνυμάτων ηλεκτρονικού ταχυδρομείου (αυθεντικά και

ψεύτικα). Ο στόχος τους είναι να προσδιορίσουν ποια μηνύματα ηλεκτρονικού ταχυδρομείου μπορεί να είναι απάτες και ποια είναι ασφαλή.

- Ανίχνευση επικίνδυνων συνδέσμων: Οι ηλικιωμένοι εξασκούνται στον εντοπισμό ύποπτων συνδέσμων σε μηνύματα ηλεκτρονικού ταχυδρομείου ή SMS, μαθαίνοντας πώς να επαληθεύουν αν μια διεύθυνση URL είναι αξιόπιστη.
- Άσκηση ασφάλειας κωδικών πρόσβασης: Οι συμμετέχοντες δημιουργούν παραδείγματα ισχυρών και αδύναμων κωδικών πρόσβασης. Μαθαίνουν τις αρχές της δημιουργίας ασφαλών κωδικών πρόσβασης και πώς να τους αποθηκεύουν με ασφάλεια.

3. Προσομοιώσεις διαδικτυακών καταστάσεων στις οποίες οι ηλικιωμένοι ενδέχεται να κάνουν λάθη — και πώς να τους βοηθήσετε να μάθουν να τα αποφεύγουν

❖ **Περιγραφή**

Οι διαδικτυακές προσομοιώσεις είναι πρακτικές ασκήσεις που επιτρέπουν στους ηλικιωμένους να μάθουν μέσω της εμπειρίας πώς να αναγνωρίζουν και να αποφεύγουν τα λάθη. Οι προσομοιώσεις βοηθούν τους συμμετέχοντες να αισθάνονται πιο σίγουροι και ενημερωμένοι κατά τη χρήση του διαδικτύου.

❖ **Μέθοδοι**

- **Προσομοίωση ηλεκτρονικού ψαρέματος (phishing):** Ο εκπαιδευτής παρουσιάζει ένα σενάριο στο οποίο ένας ηλικιωμένος λαμβάνει ένα email που μοιάζει με αυθεντικό μήνυμα από τράπεζα, στο οποίο ζητούνται τα στοιχεία σύνδεσης. Οι ηλικιωμένοι μαθαίνουν πώς να μην εξαπατώνται και ποια στοιχεία στο email πρέπει να τους κάνουν να υποψιάζονται.
- **Προσομοίωση ηλεκτρονικών αγορών:** Οι ηλικιωμένοι επισκέπτονται ιστότοπους που μιμούνται ηλεκτρονικά καταστήματα. Ο στόχος τους είναι να εντοπίσουν ύποπτα στοιχεία, όπως υπερβολικά χαμηλές τιμές, έλλειψη πιστοποιητικού SSL ή παράξενες μεθόδους πληρωμής.
- **Προσομοίωση ψεύτικης ανακοίνωσης βραβείου:** Οι εκπαιδευτές παρουσιάζουν μια κατάσταση στην οποία ένας ηλικιωμένος λαμβάνει ένα μήνυμα σχετικά με τη νίκη σε έναν διαγωνισμό που στην πραγματικότητα είναι απάτη. Οι ηλικιωμένοι μαθαίνουν να αναγνωρίζουν τέτοιες απάτες και πώς να αντιδρούν.

Παράρτημα 6 | Άσκηση προσομοίωσης: Συζήτηση με έναν ηλικιωμένο για την ασφάλεια στον κυβερνοχώρο

Διεξάγετε ένα παιχνίδι ρόλων σχετικά με το phishing, τις απάτες, την ασφάλεια των λογαριασμών και τα μέσα κοινωνικής δικτύωσης, με τον εκπαιδευτικό να καθοδηγεί και τον ηλικιωμένο να εξασκείται.

Σενάριο εργασίας

Ο εκπαιδευτικός και ο ηλικιωμένος συνομιλούν για τις διαδικτυακές απειλές, μαθαίνοντας πώς να αναγνωρίζουν και να αποφεύγουν επικίνδυνες καταστάσεις. Κάθε σενάριο παρουσιάζει διαφορετικές κοινές απειλές που μπορεί να αντιμετωπίσουν οι ηλικιωμένοι στο διαδίκτυο.

Παραδείγματα θεμάτων προς συζήτηση κατά τη διάρκεια της άσκησης

- Phishing (ψεύτικα μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα) Πώς μπορεί να αναγνωριστεί το phishing σε μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα SMS και ιστότοπους; Ποια είναι τα τυπικά σημάδια των ψεύτικων μηνυμάτων και συνδέσμων;

- Ψεύτικα βραβεία και απάτες σε διαγωνισμούς Ποια είναι τα συνηθισμένα απάτη που αφορούν βραβεία και κέρδη σε διαγωνισμούς; Πώς πρέπει να αντιδράσει κανείς σε προσφορές που απαιτούν προκαταβολή;
- Ασφάλεια διαδικτυακών λογαριασμών Ποιες είναι οι ορθές πρακτικές για την ασφάλεια των λογαριασμών σε τράπεζες, ηλεκτρονικά καταστήματα και μέσα κοινωνικής δικτύωσης; Τι κάνει έναν κωδικό πρόσβασης ασφαλή και γιατί είναι σημαντική η επαλήθευση δύο παραγόντων;
- Ασφαλής χρήση των μέσων κοινωνικής δικτύωσης Πώς μπορείτε να αναγνωρίσετε ψεύτικα προφίλ και απατεώνες στα μέσα κοινωνικής δικτύωσης; Ποιες πληροφορίες πρέπει να προστατεύονται και ποιες δεν πρέπει να κοινοποιούνται στο διαδίκτυο;

Κατάτμηση ρόλων στην άσκηση (σε ζευγάρια)

- **Ρόλος του εκπαιδευτικού (εκπαιδευτής προσομοίωσης):**
  Ο εκπαιδευτικός έχει ως αποστολή να καθοδηγήσει τη συζήτηση, βοηθώντας τους ηλικιωμένους να κατανοήσουν τις διαδικτυακές απειλές και διδάσκοντάς τους πώς να τις αναγνωρίζουν.
  Ο εκπαιδευτικός πρέπει να χρησιμοποιεί απλή και σαφή γλώσσα, να εξηγεί υπομονετικά τις απειλές και να κάνει ερωτήσεις για να ενθαρρύνει τον ηλικιωμένο να συμμετέχει ενεργά στη συζήτηση.
  Ο εκπαιδευτικός είναι επίσης υπεύθυνος να υπενθυμίζει στον ηλικιωμένο τους κανόνες ασφάλειας στο διαδίκτυο και να διασφαλίζει ότι έχει κατανοήσει το υλικό.
- **Ρόλος του ηλικιωμένου**
  Ο ηλικιωμένος συμμετέχει ενεργά στη συζήτηση, μοιράζεται τις εμπειρίες του σχετικά με τη χρήση του διαδικτύου. Μπορεί να εκφράσει τυχόν αμφιβολίες ή ανησυχίες σχετικά με την ασφάλεια στο διαδίκτυο.
  Ο ηλικιωμένος απαντά στις ερωτήσεις του εκπαιδευτικού, μοιράζεται την άποψή του και προσπαθεί να λύσει τα προβλήματα που παρουσιάζονται σχετικά με τις διαδικτυακές απειλές.

- **Phishing (ψεύτικα μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα)**

Πώς μπορεί να αναγνωριστεί το phishing σε μηνύματα ηλεκτρονικού ταχυδρομείου, SMS και ιστότοπους;

Ποια είναι τα τυπικά σημάδια των ψεύτικων μηνυμάτων και συνδέσμων;

- **Ψεύτικα βραβεία και απάτες σε διαγωνισμούς**

Ποια είναι τα συνηθισμένα απάτη που αφορούν βραβεία και κέρδη σε διαγωνισμούς;

Πώς πρέπει να αντιδράσει κανείς σε προσφορές που απαιτούν προκαταβολή;

- **Ασφάλεια των διαδικτυακών λογαριασμών**

Ποιες είναι οι ορθές πρακτικές για την ασφάλεια των λογαριασμών σε τράπεζες, ηλεκτρονικά καταστήματα και μέσα κοινωνικής δικτύωσης;

Τι κάνει έναν κωδικό πρόσβασης ασφαλή και γιατί είναι σημαντική η επαλήθευση δύο παραγόντων;

- **Ασφαλής χρήση των μέσων κοινωνικής δικτύωσης**

Πώς μπορεί κανείς να αναγνωρίσει ψεύτικα προφίλ και απατεώνες στα μέσα κοινωνικής δικτύωσης;

Ποιες πληροφορίες πρέπει να προστατεύονται και ποιες δεν πρέπει να κοινοποιούνται στο διαδίκτυο;

Παράρτημα 7 | Προσομοιώσεις σεναρίων

Διεξάγετε προσομοιώσεις σεναρίων όπου οι ηλικιωμένοι αντιμετωπίζουν απατηλές κλήσεις, μηνύματα ηλεκτρονικού ταχυδρομείου ή SMS. Ρωτήστε τους πώς θα αντιδρούσαν, συζητήστε τα συναισθήματα και τις ασφαλείς αντιδράσεις και εξασκηθείτε σε τεχνικές χαλάρωσης, όπως η αναπνοή.

Περιεχόμενο της άσκησης

Προετοιμασία για την άσκηση
Ξεκινήστε τη συνεδρία με μια σύντομη συζήτηση σχετικά με τη σημασία της διατήρησης της ηρεμίας σε δύσκολες καταστάσεις. Τονίστε ότι οι απατεώνες συχνά προσπαθούν να δημιουργήσουν πανικό ή αίσθημα επείγοντος για να πιέσουν τους ηλικιωμένους να λάβουν γρήγορες, απερίσκεπτες αποφάσεις.

Προσομοιώσεις σεναρίων απειλής

- **Σενάριο 1**
  Ένας ηλικιωμένος λαμβάνει τηλεφώνημα από έναν «υπάλληλο τράπεζας» που ισχυρίζεται ότι ο λογαριασμός του έχει μπλοκαριστεί και του ζητά να εγκαταστήσει μια εφαρμογή. Τι κάνει ο ηλικιωμένος;
- **Σενάριο 2**
  Ένας ηλικιωμένος λαμβάνει ένα email σχετικά με τη νίκη του σε έναν διαγωνισμό και του ζητείται να παράσχει προσωπικές πληροφορίες και να κάνει κλικ σε έναν σύνδεσμο. Τι κάνει ο ηλικιωμένος;
- **Σενάριο 3**
  Ένας ηλικιωμένος λαμβάνει ένα SMS με ένα ύποπτο μήνυμα σχετικά με την ανάγκη να πληρώσει επιπλέον για ένα πακέτο. Τι κάνει ο ηλικιωμένος;

Μετά από κάθε σενάριο:

- Ζητήστε από τους ηλικιωμένους να μοιραστούν εν συντομία πώς θα αντιδρούσαν σε μια τέτοια κατάσταση.
- Κάντε ερωτήσεις που προκαλούν προβληματισμό, όπως
  Τι αισθάνεστε όταν λαμβάνετε τέτοια μηνύματα;
  Ποια συναισθήματα σας προκαλούν;
  Ποιες σκέψεις επηρεάζουν τις αποφάσεις σας;

Στη συνέχεια, συζητήστε ως ομάδα ποια μέτρα πρέπει να λάβετε για να παραμείνετε ψύχραιμοι: μην πανικοβληθείτε, μην ενεργείτε παρορμητικά, σταματήστε και μιλήστε με κάποιον κοντινό σας πρόσωπο, επαληθεύστε τις πληροφορίες.

Άσκηση συνειδητοποίησης των συναισθημάτων:
Ζητήστε από τους ηλικιωμένους να κλείσουν τα μάτια τους και να θυμηθούν μια κατάσταση στην οποία ένιωσαν απειλημένοι στο διαδίκτυο (π.χ. έλαβαν ένα ύποπτο email).
Ρωτήστε: *Τι συναισθήματα νιώσατε εκείνη τη στιγμή; Τι σωματικά σημάδια έστελνε το σώμα σας (π.χ. αυξημένος καρδιακός ρυθμός, αίσθημα ανησυχίας);*
Ενθαρρύνετέ τους να βρουν τρόπους για να ελέγχουν αυτά τα συναισθήματα σε μια απειλητική κατάσταση, όπως η χρήση τεχνικών αναπνοής που έχουν συζητηθεί προηγουμένως.

Περίληψη της άσκησης:
Τονίστε πόσο σημαντικό είναι να κάνετε μια παύση πριν λάβετε οποιαδήποτε απόφαση όταν αντιμετωπίζετε μια πιθανή απειλή.
Επισημάνετε ότι δεν είναι πάντα απαραίτητο να ενεργείτε αμέσως. Είναι σοφό να ζητήσετε βοήθεια ή να συμβουλευτείτε τους αγαπημένους σας ή επαγγελματίες πριν προβείτε σε οποιαδήποτε ενέργεια.

Συμβουλές για τον εκπαιδευτικό:

- **Να είστε υπομονετικοί:** Οι ηλικιωμένοι μπορεί να χρειάζονται περισσότερο χρόνο για να κατανοήσουν τις απειλές και να αντιδράσουν κατάλληλα. Εξηγήστε υπομονετικά κάθε απειλή και προτείνετε πιθανές λύσεις.
- **Προσαρμόστε το ρυθμό:** Βεβαιωθείτε ότι όλοι οι συμμετέχοντες κατανοούν κάθε άσκηση και έχουν την ευκαιρία να κάνουν ερωτήσεις.
- **Να είστε προσεκτικοί με τα συναισθήματα:** Είναι σημαντικό να κατανοήσετε πώς τα συναισθήματα επηρεάζουν τη λήψη αποφάσεων. Γι' αυτό είναι σημαντικές οι ασκήσεις χαλάρωσης και η αναγνώριση των συναισθημάτων.

Ασκηθείτε τακτικά
Αυτές οι συνεδρίες πρέπει να επαναλαμβάνονται τακτικά, ώστε οι ηλικιωμένοι να αισθάνονται πιο σίγουροι και να γνωρίζουν πώς να αντιδρούν όταν αντιμετωπίζουν απειλές.

Παράρτημα 8 | Άσκηση προσομοίωσης: Δείγματα αναφορών απειλών στον κυβερνοχώρο

Διεξάγετε παιχνίδια ρόλων με δείγματα απειλών στον κυβερνοχώρο, εξηγήστε, προσδιορίστε τους κινδύνους και εξασκηθείτε σε ασφαλείς αντιδράσεις.

Σενάριο εργασίας
Οι συμμετέχοντες εργάζονται σε ζεύγη, αναλαμβάνοντας τους ρόλους του εκπαιδευτικού και του ηλικιωμένου.
Κάθε ζευγάρι λαμβάνει μια περιγραφή ενός από τα τέσσερα δείγματα αναφορών για απειλές στον κυβερνοχώρο.
Ο εκπαιδευτικός έχει ως αποστολή να διεξάγει μια ήρεμη και σαφή εκπαιδευτική συζήτηση με τον ηλικιωμένο, κατά τη διάρκεια της οποίας:

- εξηγούν τη φύση της απειλής,
- βοηθά τον ηλικιωμένο να κατανοήσει πώς να αναγνωρίζει τα σημάδια κινδύνου,
- συνεργάζονται με τον ηλικιωμένο για να βρουν λύσεις και ασφαλείς απαντήσεις στην κατάσταση.

Οι συμμετέχοντες μπορούν να αλλάξουν ρόλους και να εργαστούν με μια νέα αναφορά.

Παραδείγματα τεσσάρων αναφορών για απειλές στον κυβερνοχώρο που μπορεί να αφορούν ηλικιωμένους

Αναφορά 1: SMS που ζητά επιπλέον πληρωμή για ένα δέμα
Περιγραφή της κατάστασης: Ο ηλικιωμένος έλαβε ένα SMS που τον ενημέρωνε ότι ένα δέμα περιμένει παράδοση, αλλά απαιτείται επιπλέον πληρωμή 2 ευρώ. Το μήνυμα περιείχε έναν ύποπτο σύνδεσμο που οδηγούσε σε έναν άγνωστο ιστότοπο.

Αναφορά 2: Ψεύτικο τηλεφώνημα από την τράπεζα
Περιγραφή της κατάστασης: Ο ηλικιωμένος έλαβε τηλεφώνημα από κάποιον που ισχυριζόταν ότι ήταν υπάλληλος της τράπεζας. Ο απατεώνας ισχυρίστηκε ότι ο λογαριασμός είχε μπλοκαριστεί και πρότεινε την εγκατάσταση μιας εφαρμογής για την προστασία του.

Αναφορά 3: Ηλεκτρονικό μήνυμα σχετικά με υποτιθέμενο έπαθλο
Περιγραφή της κατάστασης: Ο ηλικιωμένος έλαβε ένα email που ισχυριζόταν ότι είχε κερδίσει έναν διαγωνισμό. Το email ζητούσε προσωπικά δεδομένα και ζητούσε από τον ηλικιωμένο να κάνει κλικ σε έναν σύνδεσμο που οδηγούσε σε έναν ύποπτο ιστότοπο.

Αναφορά 4: Κατάληψη λογαριασμού Facebook
Περιγραφή της κατάστασης: Οι φίλοι του ηλικιωμένου έλαβαν περίεργα μηνύματα από τον λογαριασμό του, τα οποία περιείχαν συνδέσμους ή αιτήματα για δάνειο. Ο ηλικιωμένος δεν έστειλε αυτά τα μηνύματα, γεγονός που υποδηλώνει ότι ο λογαριασμός του είχε παραβιαστεί από έναν απατεώνα.

Προτάσεις για εκπαιδευτικούς σχετικά με τον τρόπο συζήτησης των απειλών:

- **Κατανόηση της κατάστασης:** Χρησιμοποιήστε απλή γλώσσα και αναλογίες για να εξηγήσετε τις απειλές. Οι ηλικιωμένοι συχνά κατανοούν καλύτερα όταν οι καταστάσεις παρουσιάζονται στο πλαίσιο της καθημερινής ζωής (π.χ. συγκρίνοντας την ηλεκτρονική απάτη με τις παραδοσιακές τηλεφωνικές απάτες).
- **Παραδείγματα και προσομοιώσεις:** Διεξάγετε τακτικά ασκήσεις χρησιμοποιώντας προσομοιώσεις τηλεφωνικών συνομιλιών ή αναλύοντας παραδείγματα ύποπτων μηνυμάτων ηλεκτρονικού ταχυδρομείου. Αυτό βοηθά τους ηλικιωμένους να ανταποκρίνονται πιο αποτελεσματικά σε πραγματικές απειλές.
- **Βοήθεια στην αναφορά περιστατικών:** Βοηθήστε τους ηλικιωμένους να αναφέρουν τις απειλές στον κυβερνοχώρο στις αρμόδιες αρχές, όπως το CERT Poland, τις τράπεζες ή την αστυνομία. Αυτό μπορεί να εξασκηθεί κατά τη διάρκεια της εκπαίδευσης για να ενισχυθεί η αυτοπεποίθησή τους.
- **Έμφαση στην επαλήθευση δύο παραγόντων:** Δώστε οδηγίες για την ενεργοποίηση της επαλήθευσης δύο παραγόντων, η οποία μπορεί να βοηθήσει τους ηλικιωμένους να ασφαλίσουν τους διαδικτυακούς τους λογαριασμούς, ειδικά όταν χρησιμοποιούν τα μέσα κοινωνικής δικτύωσης.
- **Διατήρηση της ψυχραιμίας:** Οι εκπαιδευτικοί πρέπει να διδάξουν στους ηλικιωμένους να παραμένουν ψύχραιμοι σε απειλητικές καταστάσεις και να αποφεύγουν παρορμητικές ενέργειες, όπως η εγκατάσταση άγνωστων εφαρμογών ή η κοινοποίηση προσωπικών πληροφοριών.
- **Εκπαίδευση σχετικά με τα εργαλεία ασφάλειας:** Αξίζει να εισαχθεί η χρήση λογισμικού προστασίας από ιούς, η ασφάλεια των διαδικτυακών λογαριασμών και η επαλήθευση της αξιοπιστίας των πηγών πληροφοριών (π.χ. έλεγχος των επίσημων τηλεφωνικών αριθμών των τραπεζών).

Παράρτημα 9 | Πώς να διδάξετε στους ηλικιωμένους την ασφαλή χρήση των εφαρμογών επικοινωνίας

Διδάξτε την ασφαλή χρήση των εφαρμογών με απλή γλώσσα, εξασκηθείτε με εικονίδια και αναγνωρίστε τα μηνύματα spam ή phishing.

Περιεχόμενο και μέθοδοι διδασκαλίας

1. Επεξήγηση των βασικών λειτουργιών των εφαρμογών επικοινωνίας με καθημερινή γλώσσα

Συστάσεις για τον εκπαιδευτικό

- Αποφύγετε την τεχνική ορολογία – αντί να λέτε «συνδεθείτε στον λογαριασμό σας», πείτε «πληκτρολογήστε το όνομα και τον κωδικό πρόσβασής σας για να ανοίξετε το γραμματοκιβώτιό σας».
- Αντί για «ρυθμίσεις απορρήτου», πείτε «όπου μπορείτε να επιλέξετε ποιος μπορεί να σας δει και ποιος μπορεί να σας στείλει μήνυμα».
- Χρησιμοποιήστε αναλογίες, π.χ. «ένα πρόγραμμα ανταλλαγής μηνυμάτων είναι σαν ένα τηλέφωνο με μηνύματα και εικόνες».

Παράδειγμα άσκησης

- Μοιράστε κάρτες με εικονίδια δημοφιλών εφαρμογών (π.χ. email, WhatsApp, Messenger, Zoom).
- Ζητήστε από τους συμμετέχοντες να τις περιγράψουν με δικά τους λόγια.
- Δημιουργήστε μαζί έναν απλό ορισμό για κάθε μία.

Υποστηρικτικό υλικό

- Δημιουργήστε ένα έντυπο γλωσσάριο με απλούς όρους (π.χ. «μήνυμα», «βιντεοκλήση», «συνημμένο»).

2. Ασκήσεις αναγνώρισης επικίνδυνων μηνυμάτων (Spam, Phishing)

Συστάσεις για τον εκπαιδευτικό

- Χρησιμοποιείτε πάντα πραγματικά παραδείγματα για να δείξετε τόσο τα ασφαλή όσο και τα ψεύτικα μηνύματα.
- Συζητήστε πώς μοιάζει μια ύποπτη διεύθυνση ηλεκτρονικού ταχυδρομείου, τι σημαίνει «κάντε κλικ σε αυτόν τον σύνδεσμο», πώς να εντοπίσετε την απάτη «εγγονός στο εξωτερικό».

Παράδειγμα άσκησης

- Χωρίστε τους συμμετέχοντες σε ομάδες και δώστε τους τρία εκτυπωμένα email:
  - Μια πραγματική πρόσκληση για συνομιλία
  - Ένα ψεύτικο email με σύνδεσμο προς ένα «τιμολόγιο»
  - Ένα μήνυμα με γραμματικά λάθη και αίτημα για προσωπικά δεδομένα
- Εργασία: Προσδιορίστε ποια μηνύματα είναι ύποπτα και γιατί.

Υποστηρικτικό υλικό

- Δημιουργήστε φύλλα εργασίας με δείγματα email για ανάλυση
- Εισάγετε 5 βασικές ερωτήσεις για κάθε μήνυμα:
  - Γνωρίζω τον αποστολέα;
  - Το μήνυμα έχει νόημα;
  - Υπάρχουν λάθη;
  - Η διεύθυνση ηλεκτρονικού ταχυδρομείου φαίνεται σωστή;
  - Ο σύνδεσμος φαίνεται ύποπτος;

3. Επίδειξη ρυθμίσεων απορρήτου και ασφάλειας

Συστάσεις για τον εκπαιδευτικό

- Επιδείξτε κάθε εργασία βήμα προς βήμα σε μια μεγάλη οθόνη ή προβολέα.
- Να θυμάστε: οι ηλικιωμένοι συχνά μαθαίνουν με την επανάληψη – προγραμματίστε να ολοκληρώσετε κάθε βήμα μαζί.

Παράδειγμα άσκησης

Για να ολοκληρώσετε μαζί με τους συμμετέχοντες:

- Μεταβείτε στις ρυθμίσεις του WhatsApp → «Απόρρητο» → «Φωτογραφία προφίλ» → επιλέξτε «Οι επαφές μου»
- Στο Messenger: δείξτε πώς να αποκλείσετε έναν άγνωστο

Υποστηρικτικό υλικό

- Δημιουργήστε εικονογραφημένες κάρτες με οδηγίες βήμα προς βήμα, π.χ.:
    - «Πώς να αλλάξετε τον κωδικό πρόσβασής σας»
    - «Πώς να ρυθμίσετε την ιδιωτικότητα»
    - «Πώς να αποκλείσετε έναν χρήστη»

4. Διαδραστικές μέθοδοι – Ενίσχυση των γνώσεων και αντιμετώπιση απειλών

Συστάσεις για τον εκπαιδευτικό:

- Οι προσομοιώσεις είναι αποτελεσματικές – οι ηλικιωμένοι μαθαίνουν καλύτερα μέσω ρεαλιστικών σεναρίων.
- Χρησιμοποιήστε ζευγάρια ή μικρές ομάδες για να ενισχύσετε την αυτοπεποίθηση και την ομαδική εργασία.

Παραδείγματα ασκήσεων:

- Προσομοίωση 1: «Έλαβα ένα παράξενο μήνυμα από την τράπεζα» – τι να κάνω;
- Προσομοίωση 2: «Δεν μπορώ να συνδεθώ με την κόρη μου στο Zoom» – πώς να ελέγξω τις ρυθμίσεις;
- Παιχνίδι ρόλων: ο εκπαιδευτικός παίζει τον ρόλο του απατεώνα, ο συμμετέχων παίζει τον ρόλο του ηλικιωμένου – στη συνέχεια, αλλάζουν ρόλους.

Υποστηρικτικό υλικό:

- Δημιουργία σεναρίων προσομοίωσης
- Κάρτες ρόλων: εκπαιδευτικός/συμμετέχων/απατεώνας
- Κάρτες υπενθύμισης για το σπίτι με συμβουλές ασφαλείας (π.χ. για να κολλήσετε στο ψυγείο)

Παράρτημα 10 | Πώς να διδάξετε στους ηλικιωμένους να χρησιμοποιούν antivirus και ενημερώσεις συστήματος

Διδάξτε στους ηλικιωμένους τι είναι οι ιοί και οι ενημερώσεις, δείξτε τους πώς να χρησιμοποιούν τα προγράμματα προστασίας από ιούς και εξασκηθείτε μαζί τους στη διεξαγωγή σαρώσεων και στην εγκατάσταση ενημερώσεων συστήματος βήμα προς βήμα.

Περιεχόμενο και μέθοδοι διδασκαλίας

1. Εισαγωγή – Τι είναι οι ιοί, οι ενημερώσεις και οι λειτουργίες ασφαλείας

Συστάσεις για τον εκπαιδευτικό:

- Θυμηθείτε να χρησιμοποιείτε αναλογίες όταν εξηγείτε σύνθετα θέματα.
- Εξηγήστε τι είναι οι «ιούς υπολογιστών» – χρησιμοποιήστε συγκρίσεις με ένα κρυολόγημα ή μια λοίμωξη που μπορεί να προσβάλει έναν υπολογιστή.
- Διευκρινίστε ότι οι ενημερώσεις είναι σαν «φάρμακα» για έναν υπολογιστή – βοηθούν στην πρόληψη βλαβών και επιθέσεων.

Παράδειγμα άσκησης

- Κάντε στους συμμετέχοντες τις ακόλουθες ερωτήσεις:
  - Έχετε ακούσει ποτέ για «ιούς υπολογιστών»;
  - Τι σας έρχεται στο μυαλό όταν ακούτε τη λέξη «ενημέρωση»;

2. Επίδειξη λογισμικού προστασίας από ιούς

Συστάσεις για τον εκπαιδευτικό:

- Χρησιμοποιήστε ένα ασφαλές και διαισθητικό πρόγραμμα (π.χ. Windows Defender, δωρεάν έκδοση του Avast).
- Ακολουθήστε τη διαδικασία βήμα προς βήμα: άνοιγμα του προγράμματος, έλεγχος για ενημερώσεις, εκτέλεση γρήγορης σάρωσης. Μπορείτε να επιδείξετε τη διαδικασία χρησιμοποιώντας έναν προβολέα.

Παράδειγμα άσκησης:

- Ζητήστε από τους συμμετέχοντες να ανοίξουν το λογισμικό προστασίας από ιούς στις δικές τους συσκευές (ή σε κοινόχρηστο φορητό υπολογιστή).
- Εκτελέστε μια σάρωση μαζί. Συζητήστε τι σημαίνουν τα αποτελέσματα: «δεν βρέθηκαν απειλές» έναντι «εντοπίστηκαν απειλές».

3. Μάθετε πώς να ενημερώνετε το λειτουργικό σύστημα

Συστάσεις για τον εκπαιδευτικό:

- Δείξτε πώς να εντοπίζετε τις ρυθμίσεις ενημέρωσης (π.χ. στα Windows: Ρυθμίσεις → Ενημέρωση και ασφάλεια).
- Επισημάνετε ότι οι ενημερώσεις εμφανίζονται συνήθως αυτόματα – ο χρήστης χρειάζεται απλώς να κάνει κλικ στο «Εγκατάσταση τώρα».

Παράδειγμα άσκησης:

- **Κάθε συμμετέχων λαμβάνει μια λίστα ελέγχου:**
  - Ανοίξτε τις «Ρυθμίσεις»
  - Βρείτε το «Windows Update»
  - Ελέγξτε για διαθέσιμες ενημερώσεις
  - Εγκαταστήστε την ενημέρωση, εάν είναι διαθέσιμη

- **Σημείωση: Εάν χρησιμοποιείτε κοινόχρηστο υπολογιστή, η άσκηση μπορεί να πραγματοποιηθεί ως επίδειξη με σχολιασμό.**

4. Μέθοδοι ενίσχυσης – λίστες ελέγχου, παιχνίδια ρόλων, συζητήσεις

Συστάσεις για τον εκπαιδευτικό:

- Παρουσιάστε μια ανακεφαλαίωση του υλικού με τη μορφή παιχνιδιού ή κουίζ.
- Ενθαρρύνετε τους συμμετέχοντες να κάνουν ερωτήσεις και να μοιραστούν τις δικές τους εμπειρίες.

Παραδείγματα ασκήσεων:

- Λίστα ελέγχου ασφάλειας: Ο συμμετέχων ελέγχει βήμα προς βήμα αν ο υπολογιστής/το smartphone του είναι προστατευμένο (κωδικοί πρόσβασης, ενημερώσεις, σαρώσεις).
- Προσομοίωση τηλεφωνικής κλήσης: Ο εκπαιδευτικός υποδύεται έναν απατεώνα που λέει: «Ο υπολογιστής σας κινδυνεύει – κατεβάστε το πρόγραμμά μας». Ο ηλικιωμένος πρέπει να αναγνωρίσει την απειλή και να απαντήσει: «Πρώτα θα ελέγξω τις ρυθμίσεις του antivirus μου».

Υποστηρικτικό υλικό:

- Έτοιμοι προς χρήση κατάλογοι ελέγχου: «Ασφαλής υπολογιστής – Έχω όλα όσα χρειάζομαι;»

Παράρτημα 11 | Φύλλο εργασίας: Ασφαλής χρήση του Διαδικτύου: Πρακτικές συμβουλές και τεχνικές για ηλικιωμένους

Συμπληρώστε το φύλλο εργασίας απαντώντας σε ερωτήσεις σχετικά με την ασφαλή αγορά, την ασφάλεια των συσκευών, την προστασία της ιδιωτικής ζωής στο διαδίκτυο και την υπέρβαση του φόβου για την τεχνολογία.

Ασφαλείς διαδικτυακές αγορές	
Ποια στοιχεία μιας διαδικτυακής προσφοράς πρέπει να επισημανθούν στους ηλικιωμένους ως δυνητικά επικίνδυνα ή ύποπτα;	
Πώς να καθοδηγήσετε τους ηλικιωμένους στη διαδικασία των διαδικτυακών αγορών – πώς να μιλήσετε, τι να δείξετε και τι να αναζητήσετε για να τους κάνετε να νιώσουν ασφαλείς;	
Ασφάλεια συσκευών	
Ποιες τεχνικές βοηθούν τους ηλικιωμένους να κατανοήσουν πώς να ρυθμίζουν τις συσκευές τους με ασφάλεια;	
Ποιες εφαρμογές και ρυθμίσεις είναι απαραίτητες για την προστασία των συσκευών των ηλικιωμένων	
Προστασία της ιδιωτικής ζωής στο διαδίκτυο	
Ποιες μεθόδους θα χρησιμοποιήσετε για να βοηθήσετε τους ηλικιωμένους να κατανοήσουν καλύτερα την έννοια της προστασίας της ιδιωτικής ζωής στο διαδίκτυο, ειδικά στο πλαίσιο της χρήσης εφαρμογών επικοινωνίας όπως το WhatsApp;	
Ξεπερνώντας τον φόβο της τεχνολογίας	
Ποια στοιχεία εκπαίδευσης βοηθούν τους ηλικιωμένους να ξεπεράσουν τον φόβο της τεχνολογίας και να ενισχύσουν την αυτοπεποίθησή τους κατά τη χρήση του διαδικτύου;	
Ποιες μέθοδοι ενίσχυσης της αυτοπεποίθησης αξίζει να χρησιμοποιηθούν για να κάνουν τους ηλικιωμένους να αισθάνονται άνετα στον κόσμο των νέων τεχνολογιών;	

Παράρτημα 12 | Προτάσεις για περαιτέρω ανάγνωση και μάθηση για τους συμμετέχοντες

Ιστοσελίδες για την ασφάλεια στον κυβερνοχώρο: Ευρωπαϊκοί και κυβερνητικοί οργανισμοί που ασχολούνται με την ασφάλεια στον κυβερνοχώρο

1) **ENISA – Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια**
   Ιστότοπος: https://www.enisa.europa.eu
   Η ENISA προσφέρει οδηγούς, εκθέσεις και εκπαιδευτικές εκστρατείες για την κυβερνοασφάλεια. Περιλαμβάνει εκπαιδευτικό υλικό για μεμονωμένους χρήστες, συμπεριλαμβανομένων των ηλικιωμένων, σχετικά με την ασφαλή χρήση ηλεκτρονικού ταχυδρομείου, κωδικών πρόσβασης, smartphone και ηλεκτρονικής τραπεζικής.
2) **Ευρωπαϊκή Επιτροπή – Ασφαλέστερο Διαδίκτυο**
   Ιστότοπος: https://digital-strategy.ec.europa.eu/en/policies/safer-internet
   Πρόγραμμα της Ευρωπαϊκής Επιτροπής για την προώθηση της ασφαλούς χρήσης του διαδικτύου για όλες τις ηλικιακές ομάδες, συμπεριλαμβανομένων των ηλικιωμένων. Ο ιστότοπος περιέχει ενημερωτικές εκστρατείες και συνδέσμους προς εθνικές πρωτοβουλίες.
3) **Δίκτυο Ευρωπαϊκών Κέντρων Καταναλωτών (ECC-Net)**
   Ιστοσελίδα: https://www.eccnet.eu
   Δίκτυο κέντρων καταναλωτών στην ΕΕ, το οποίο προσφέρει συμβουλές για ασφαλείς διαδικτυακές αγορές, προστασία προσωπικών δεδομένων και αποφυγή διαδικτυακής απάτης, οι οποίες μπορεί να είναι ιδιαίτερα χρήσιμες για τους ηλικιωμένους.
4) **Cyberprofilaktyka – Πρόγραμμα ψηφιακής πρόληψης**
   Ιστοσελίδα: https://cyberprofilaktyka.pl/
   Ένα πρόγραμμα ψηφιακής πρόληψης που περιλαμβάνει μια ενότητα με συμβουλές για ηλικιωμένους σχετικά με τον τρόπο αποφυγής των διαδικτυακών απειλών. Περιλαμβάνει επίσης εκπαιδευτικό υλικό, ενημερωτικά γραφικά και παραδείγματα πραγματικών περιπτώσεων απάτης, τα οποία βοηθούν στην καλύτερη κατανόηση των ψηφιακών κινδύνων.

6.5 Ενότητα V – Προ/Μετα-τεστ

1. Ποιος είναι ο κύριος στόχος της Ενότητας 5;

Α) Να διδάξει στους ηλικιωμένους πώς να χρησιμοποιούν τα μέσα κοινωνικής δικτύωσης για διασκέδαση
Β) Να εκπαιδεύσει τους εκπαιδευτικούς ώστε να υποστηρίζουν αποτελεσματικά τους ηλικιωμένους στην ασφαλή ψηφιοποίηση
Γ) Να βελτιώσει τις γνώσεις των ηλικιωμένων σχετικά με την τεχνητή νοημοσύνη
Δ) Να αναπτύξει τις δεξιότητες προγραμματισμού των ηλικιωμένων

2. Ποιο από τα παρακάτω αποτελεί ένα κοινό εμπόδιο για τους ηλικιωμένους κατά την εκμάθηση ψηφιακών δεξιοτήτων;

Α) Η περιέργεια για τις νέες τεχνολογίες
Β) Ο φόβος της αποτυχίας ή η έλλειψη αυτοπεποίθησης
Γ) Η υπερβολική χρήση των μέσων κοινωνικής δικτύωσης
Δ) Οι ισχυρές τεχνικές γνώσεις

3. Ποια είναι μια αποτελεσματική μέθοδος διδασκαλίας για ηλικιωμένους;

Α) Χρήση περίπλοκων τεχνικών όρων για να ακούγεται επαγγελματίας
Β) Διεξαγωγή μαθημάτων με γρήγορο ρυθμό
Γ) Χωρισμός των οδηγιών σε μικρά, απλά βήματα
Δ) Εστίαση μόνο στις θεωρητικές γνώσεις

4. Τι πρέπει να τονίζουν οι εκπαιδευτικοί όταν διδάσκουν για τις ηλεκτρονικές τραπεζικές συναλλαγές και τις αγορές στο διαδίκτυο;

Α) Πώς να ξοδεύουν τα χρήματά τους πιο γρήγορα
Β) Πώς να αναγνωρίζουν ασφαλείς ιστότοπους και να προστατεύουν τα προσωπικά τους δεδομένα
Γ) Πώς να αυξήσετε την ορατότητα στο διαδίκτυο
Δ) Πώς να απενεργοποιήσετε το λογισμικό προστασίας από ιούς

5. Ποιο από τα παρακάτω είναι ένα καλό παράδειγμα απόπειρας ηλεκτρονικού ψαρέματος (phishing);

Α) Ένας φίλος σας στέλνει έναν γνωστό σύνδεσμο
Β) Ένα email από την τράπεζά σας που σας ζητάει το όνομα χρήστη και τον κωδικό πρόσβασής σας
Γ) Μια ενημέρωση από ένα αξιόπιστο πρόγραμμα λογισμικού
Δ) Μια υπενθύμιση από την εφαρμογή ημερολογίου

6. Όταν ένας ηλικιωμένος λαμβάνει μια ύποπτη τηλεφωνική κλήση από έναν «υπάλληλο τράπεζας», τι πρέπει να κάνει πρώτα;

Α) Να εγκαταστήσει αμέσως την προτεινόμενη εφαρμογή
Β) Να κλείσει το τηλέφωνο και να καλέσει την τράπεζά του στον επίσημο αριθμό
Γ) Να δώσει τα στοιχεία ταυτότητας και τα στοιχεία του λογαριασμού του
Δ) Να αγνοήσει εντελώς την κλήση

7. Ποιος είναι ο καλύτερος τρόπος για τους εκπαιδευτικούς να βοηθήσουν τους ηλικιωμένους να κατανοήσουν τα προγράμματα προστασίας από ιούς;

Α) Να εξηγήσουν χρησιμοποιώντας αναλογίες, όπως η σύγκριση των ιών με τις ασθένειες
Β) Να αποφύγουν εντελώς τις τεχνικές εξηγήσεις
Γ) Να παραλείψουν τα θέματα που αφορούν τα προγράμματα προστασίας από ιούς, επειδή είναι πολύ προχωρημένα
Δ) Να παρουσιάζουν μόνο εξηγήσεις με βάση κείμενο

8. Τι σημαίνει «ψηφιακή ευαισθητοποίηση» για τους ηλικιωμένους;

Α) Να γνωρίζουν πώς να κάνουν πιο γρήγορα αγορές στο διαδίκτυο
Β) Να κατανοούν και να αναγνωρίζουν τις διαδικτυακές απειλές
Γ) Αποφυγή κάθε χρήσης της τεχνολογίας
Δ) Να μάθουν πώς να σχεδιάζουν ιστοσελίδες

9. Τι πρέπει να κάνει ένας εκπαιδευτικός αν ένας ηλικιωμένος δεν καταλαβαίνει μια εφαρμογή κατά τη διάρκεια του μαθήματος;

Α) Να προχωρήσει στο επόμενο θέμα
Β) Να επαναλάβει και να απλοποιήσει την εξήγηση με υπομονή
Γ) Να ζητήσει από έναν άλλο ηλικιωμένο να τον διδάξει
Δ) Να αγνοήσει το πρόβλημα

10. Τι πρέπει να κάνουν οι ηλικιωμένοι αν υποψιάζονται ότι ο λογαριασμός τους έχει υποστεί κυβερνοεπίθεση;

Α) Να περιμένουν να δουν αν το πρόβλημα θα επιλυθεί από μόνο του
Β) Να το αναφέρουν στην τράπεζα ή στις αρχές και να αλλάξουν αμέσως τους κωδικούς πρόσβασης
Γ) Να μοιραστούν την είδηση στα μέσα κοινωνικής δικτύωσης
Δ) Να διαγράψουν όλους τους λογαριασμούς τους

Περίληψη απαντήσεων

1	**B**
2	**B**
3	**C**
4	**B**
5	**B**
6	**B**
7	**A**
8	**B**
9	**B**
10	**B**

7. Έρευνα αξιολόγησης

Οι πληροφορίες που παρέχετε σε αυτή την έρευνα θα χρησιμεύσουν ως κατευθυντήριες γραμμές για τη βελτίωση του επιπέδου της εκπαίδευσης στην οποία συμμετέχετε, καθώς και του επιπέδου αποτελεσματικότητας και ελκυστικότητας των επόμενων εκπαιδευτικών προγραμμάτων σας.

Παρακαλούμε συμπληρώστε την έρευνα απαντώντας οι ίδιοι ή σύμφωνα με την παρακάτω κλίμακα βαθμολόγησης, όπου 1 είναι η χαμηλότερη βαθμολογία και 5 η υψηλότερη.

I. **Αξιολόγηση εργαστηρίου:**

- Πρόγραμμα εκπαίδευσης ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Μέθοδοι διεξαγωγής των μαθημάτων ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Ατμόσφαιρα κατά τη διάρκεια των μαθημάτων ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Χρησιμότητα της εκπαίδευσης ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Προετοιμασία του εκπαιδευτή ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Επιλογή του περιεχομένου της εκπαίδευσης ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Οι στόχοι της εκπαίδευσης ήταν σαφώς καθορισμένοι ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1

1. **Ποια θέματα σας φάνηκαν χρήσιμα και σίγουρα θα χρησιμοποιήσετε;**
   .....
   .....

2. **Ποια θέματα ήταν λιγότερο χρήσιμα για εσάς;**
   .....
   .....

3. **Ποια από τα θέματα που δεν καλύφθηκαν στην τάξη πιστεύετε ότι θα έπρεπε να είχαν συμπεριληφθεί στο πρόγραμμα και γιατί;**
   .....
   .....

4. **Πιστεύετε ότι υπάρχουν θέματα που θα έπρεπε να προστεθούν ή να αφαιρεθούν από το εκπαιδευτικό πρόγραμμα; Εξηγήστε γιατί.**
   .....
   .....

II. **Αξιολόγηση εκπαιδευτικού υλικού:**

- Περιεχόμενο 54321 ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Προσβασιμότητα των πληροφοριών ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Ευανάγνωστη ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Χρησιμότητα υλικών ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1

III. **Πρόσθετες πληροφορίες:**

1. **Συνολική αξιολόγηση της εκπαίδευσης** ☐ **ΘΕΤΙΚΗ** ☐ **ΑΡΝΗΤΙΚΗ**

2. **Η εκπαίδευση ανταποκρίθηκε στις προσδοκίες και τις απαιτήσεις σας - επιτεύχθηκαν οι επιδιωκόμενοι στόχοι, τα αποτελέσματα και τα αποτελέσματα;**
   ☐ **ΝΑΙ** ☐ **ΟΧΙ**

3. **Πιστεύετε ότι άξιζε τον κόπο να οργανωθεί μια τέτοια εκπαίδευση (και γιατί);**
   .....
   .....

4. **Πρόσθετα σχόλια και παρατηρήσεις:**
   .....
   .....

5. **Πώς μάθατε για την εκπαίδευση;**
   .....
   .....

www.cybersafesenior.eu

Cyber-Safe-Senior

Funded by
the European Union

CYBER SAFE
SENIOR

Instytut
Nowych Technologii

iED

ILKSENOL
DERNEĞİ

SIMBIOZA
MED GENERACIJAMI

«Χρηματοδοτείται από την ΕΕ. Οι απόψεις και οι γνώμες που εκφράζονται είναι αυτές του/των συγγραφέα/ων και δεν αντικατοπτρίζουν απαραίτητα τις απόψεις της Ευρωπαϊκής Ένωσης ή του Εθνικού Οργανισμού Erasmus+.»
Η Ευρωπαϊκή Ένωση ούτε ο χορηγός δεν φέρουν ευθύνη γι' αυτά.