VARNOST
V DIGITALNEM SVETU

Program usposabljanja z gradivi in scenariji, namenjen izobraževalcem za izvedbo delavnic o kibernetski varnosti starejših.

VSEBINA

1. Uvod

„Cyber Safe Senior“ je projekt, ki ga financira Evropska unija in katerega cilj je izboljšati digitalno pismenost, varnost na spletu in splošno digitalno opolnomočenje oseb starejših od 65 let. V današnjem vse bolj digitalnem svetu se starejši ljudje pri uporabi spleta soočajo s posebnimi ovirami, saj pogosto niso seznanjeni z novimi tehnologijami, tveganji na spletu in varnim ravnanjem v digitalnem okolju. Ob zavedanju tega si pobuda Cyber Safe Senior prizadeva zapolniti ključne vrzeli v digitalnem znanju in kompetencah z organiziranim večstranskim pristopom.

Projekt vključuje pripravo informativne e-knjige, ki vsebuje študije primerov internetnih kaznivih dejanj iz resničnega življenja, praktične nasvete za varnost in podrobna navodila za varno spletno ravnanje. Poleg tega pobuda ponuja virtualna predavanja, interaktivne vaje na podlagi scenarijev in pilotna usposabljanja, ki so posebej prilagojena potrebam starejših udeležencev. Cyber Safe Senior si prizadeva odpraviti digitalno izključenost, izboljšati zaupanje v uporabo tehnologije in omogočiti starejšim osebam, da neodvisno in varno sodelujejo v digitalnih okoljih, pri čemer se osredotoča na starejše, ki imajo nekaj osnovnih digitalnih izkušenj, vendar nimajo zavesti o varnosti na spletu.

Program usposabljanja za izobraževalce in trenerje zagotavlja informacije, metodologijo in praktična orodja, ki jih potrebujejo za kakovostno izobraževanje starejših o varnosti na internetu. Trenerji so pripravljeni ne le poučevati osnovne koncepte kibernetske varnosti, ampak tudi vključevati udeležence v interaktivne dejavnosti, scenarije iz resničnega življenja in vaje, ki poudarjajo posebne težave, s katerimi se starejše osebe lahko srečujejo v digitalnem svetu. To zagotavlja, da je usposabljanje praktično in neposredno povezano z vsakdanjim življenjem udeležencev.

Projekt izvaja konzorcij partnerjev iz Poljske, Slovenije, Turčije in Grčije, ki združuje znanje iz izobraževalnih ustanov, skupnostnih organizacij, knjižnic, kulturnih centrov in skupnosti starejših. S pomočjo teh lokalnih mrež lahko Cyber Safe Senior doseže starejše v mestnih in podeželskih območjih ter jim zagotovi enakopraven dostop do gradiva in podpore za digitalno pismenost.

S tem, da starejše osebe nauči, kako samozavestno uporabljati spletne platforme, varovati svoje osebne podatke, prepoznati spletna tveganja in se aktivno vključiti v digitalno družbo, projekt želi ustvariti varnejše in prijaznejše digitalno okolje. Cyber Safe Senior združuje učna gradiva, praktične dejavnosti in vključevanje skupnosti, da bi ustvaril okolje, v katerem imajo starejše osebe informacije, sposobnosti in samozavest, ki jih potrebujejo za varno, samostojno in produktivno uporabo digitalnih orodij.

Ključni dopolnilni del izobraževalnega programa Cyber Safe Senior je niz interaktivnih študij primerov Improve, razvitih z uporabo Genially. Ti scenariji so popolnoma usklajeni s temami posameznih izobraževalnih modulov in so zasnovani tako, da simulirajo resnične digitalne situacije, s katerimi se starejši ljudje pogosto srečujejo. S pomočjo vodene odločitve, praktičnih nalog in vizualne interakcije študije primerov Improve utrjujejo teoretično znanje in podpirajo izkustveno učenje, s čimer postanejo zapleteni koncepti spletne varnosti dostopnejši in zanimivejši za starejše učence.

Vsak modul usposabljanja sledi strukturirani obliki, ki je skladna z vmesnikom modula, vključno z učnimi cilji, načrtovanjem sej, dodatnimi viri, samoocenjevanjem izvajalcev usposabljanja in elementi ocenjevanja. Pred in po vsakem modulu se izvedejo predhodni in naknadni testi, da se oceni pridobljeno znanje in napredek pri učenju. Poleg tega se z ocenjevalnimi anketami zbirajo povratne informacije udeležencev in izvajalcev usposabljanja, kar podpira zagotavljanje kakovosti in nenehno izboljševanje programa usposabljanja.

1.1 Cilj programa usposabljanja

Program usposabljanja Cyber Safe Senior je bil razvit, da bi zadovoljil naraščajoče potrebe po digitalni pismenosti in varnosti na internetu med starejšimi odraslimi, starimi 65 let in več. Starejši imajo v današnjem digitalnem svetu težave z uporabo spleta, ker običajno nimajo veliko znanja o možnih grožnjah, varnostnih ukrepih na spletu in varnih digitalnih navadah. Cilj tega programa usposabljanja je zapolniti te vrzeli s tem, da starejšim zagotovi orodja, ki jih potrebujejo za varno in samozavestno uporabo digitalnih tehnologij v učinkovitem, praktičnem in zanimivem učnem okolju.

Njegovi cilji so povečati znanje starejših o varnosti na internetu, jim zagotoviti potrebna znanja in spodbuditi njihovo samozavest pri varni uporabi digitalnih tehnologij. Poleg praktičnih ukrepov za zaščito osebnih podatkov in zasebnosti program usposabljanja ponuja jasno ozaveščenost o prevladujočih spletnih grožnjah in kako jih prepoznati, nasvete o varnem spletnem ravnanju ter vpogled v realne scenarije, ki ponazarjajo možne grožnje in rešitve. S petimi obsežnimi tečaji, ki trajajo po štiri ure, in desetimi interaktivnimi primeri IMPROVE, ki simulirajo ad hoc odzive na spletne grožnje, program močno poudarja praktično učenje s preučevanjem primerov nevarnosti kibernetske varnosti iz resničnega življenja. Vsebina, temeljite vaje z navodili ter orodja in viri, potrebni za izvedbo tega programa usposabljanja, so vključeni v vsako sejo.

Ti viri učiteljem ponujajo koristne dejavnosti, pripomočke in metode za spodbujanje zanimanja starejših za interaktivno učenje in njihovo vključevanje vanj. Učitelji, ki bodo uspešno zaključili ta program, bodo usposobljeni za pomoč starejšim pri razvoju njihove digitalne usposobljenosti in samozavesti.

1.2.1 Ključni cilji programa

Povečati ozaveščenost starejših o spletnih grožnjah
Udeleženci bodo pridobili celovito razumevanje najpogostejših spletnih groženj, kot so zlonamerna programska oprema, lažno predstavljanje, prevare, kraja identitete in nevarne spletne strani. Program udeležence nauči, kako prepoznati opozorilne znake, in ponazarja možne nevarnosti s primeri iz resničnega življenja.

Razviti praktične digitalne veščine
Udeleženci bodo pridobili celovito razumevanje, kako pravilno opravljati tipične internetne naloge, kot so uporaba družbenih medijev, spletno bančništvo, nakupovanje in brskanje. Poudarek je na varnem upravljanju podatkov, dvofaktorski avtentikaciji in močnih geslih.

Spodbujanje varnega spletnega vedenja
Program poudarja sprejetje najboljših praks za zaščito zasebnosti, varno komunikacijo in etično digitalno sodelovanje. Starejši bodo razumeli, kako upravljati osebne podatke, prepoznati lažna sporočila in se ustrezno odzvati na sumljive dejavnosti.

Oskrba izobraževalcev s strokovnim znanjem
Usposabljanje izobraževalcev in moderatorjev je temeljni del programa. Izobraževalci bodo pridobili znanja, vire in tehnike, potrebne za izvajanje spletnega usposabljanja o varnosti, namenjenega starejšim. To vključuje nasvete o upravljanju dinamike skupine, učenju na podlagi scenarijev in interaktivnih tehnikah poučevanja.

Zmanjšajte digitalno izključenost
Program si prizadeva zmanjšati socialno in tehnološko izključenost starejših, zlasti tistih, ki živijo zunaj mestnih območij, s povečanjem digitalne pismenosti in znanja o varnosti na spletu. V današnjem digitalnem svetu bodo udeleženci lažje uporabljali digitalne naprave sami, kar bo spodbudilo večjo vključenost.

1.2.2 Pričakovani rezultati

- Starejši bodo pridobili znanje in praktične spretnosti, potrebne za varno uporabo internetnega okolja.
- Izobraževalci bodo dobro opremljeni, da bodo starejšim državljanom lahko ponudili zanimiva in koristna navodila o kibernetski varnosti.
- Starejši z digitalno opolnomočenostjo, ki se lahko varno ukvarjajo z dejavnostmi in storitvami na spletu, bodo koristili svojim skupnostim.

Program usposabljanja združuje teorijo z interaktivnimi vajami, ki temeljijo na scenarijih, študijami primerov in skupinskimi dejavnostmi, da se zagotovi, da se udeleženci učijo z delom. Vsak modul vsebuje strukturirane informacije, praktične naloge in možnosti za razpravo, kar starejšim omogoča, da svoje znanje takoj uporabijo in pridobijo samozavest v realnih situacijah. Program vključuje tudi komponente ocenjevanja in refleksije, ki zagotavljajo doseganje učnih rezultatov, hkrati pa nudijo povratne informacije tako izobraževalcem kot udeležencem, da se lahko nenehno razvijajo.

1.2.3 Analiza primerov

Primeri so interaktivne vaje, zasnovane na scenarijih, ki dopolnjujejo izobraževalne module programa Cyber Safe Senior. Ti scenariji so neposredno povezani z moduli I–V in prikazujejo dejanske spletne situacije, s katerimi se lahko starejši ljudje srečujejo v vsakdanjih digitalnih interakcijah, kot so lažna sporočila, prevare pri spletnih nakupih, nevarna uporaba javnih Wi-Fi omrežij in lažne naložbe. Scenariji, ki so na voljo prek interaktivnih vsebin Genially, udeležencem omogočajo, da prepoznajo potencialne nevarnosti, sprejemajo ozaveščene odločitve in razumejo posledice tveganih dejanj na internetu. Primeri spodbujajo praktično učenje s ponazoritvijo dejanskih digitalnih nevarnosti, kar starejšim omogoča pridobivanje praktičnih veščin za varno uporabo interneta.

Primeri so prilagojeni izobraževalnim modulom v skladu z njihovo tematiko in učnimi cilji, določenimi v programu.

- **Modul I – Osnove kibernetske varnosti: zaščita računalnika, elektronske pošte in osebnih podatkov:** smishing; dilema javnega Wi-Fi-ja.
- **Modul II – Tipične spletne prevare, usmerjene v starejše:** Prevara z vnukom; Past dobrodelne prevare.
- **Modul III – Varnost spletnega bančništva in spletnih nakupov:** prevare v zvezi s spletnimi nakupi; phishing prevare v e-pošti; kripto-miraž: iluzija takojšnjega obogatitve; zlati dobički – cena zaupanja.
- **Modul IV – Varna in odgovorna raba družbenih omrežij s strani starejših:** Deepfake prevare; Prevare v zvezi s spletnimi storitvami.
- **Modul V – Varna digitalizacija starejših:** obravnavana prečno v okviru splošne vsebine usposabljanja in vaj.

Dostopi do Improvizacijskih primerov:

- KRIPTO ILUZIJA: IZGUBA HITREGA BOGASTVA
- PREVARA PRI SPLETNEM NAKUPOVANJU
- PAST DOBRODELNE PREVARE
- SMISHING
- TVEGANJA UPORABE JAVNEGA WI-FI-JA
- PREVARA PREKO E-POŠTE (PHISHING)
- PERVARA STARIH STARŠEV
- PREVARA S SPLETNIMI STORITVAMI
- DEEPFAKE PREVARA
- ZLATI DONOSI - CENA ZAUPANJA: PRIMER NALOŽBENE PREVARE

MODUL I

Osnove kibernetske varnosti

2. Modul I – Osnove kibernetske varnosti: zaščita računalnikov, e-pošte in osebnih podatkov

Modul „Osnove kibernetske varnosti“ ponuja celovit pregled digitalne varnosti, ki združuje teoretično znanje s praktičnimi aplikacijami. Udeleženci bodo pridobili temeljito razumevanje bistvenih načel računalniške varnosti, zasebnosti e-pošte in varstva osebnih podatkov. Modul zajema pomembne podteme, kot so računalniška varnost in upravljanje e-pošte, v katerih se bodo udeleženci naučili, kako vzdrževati operacijski sistem in programsko opremo, uporabljati protivirusne programe in požarne zidove ter prepoznati potencialne kibernetske grožnje. Osredotoča se tudi na varnost in upravljanje gesel, kjer se uporabniki naučijo, kako ustvariti močna gesla in uspešno uporabljati upravitelje gesel.

Na voljo so praktične vaje za varnost e-pošte, ki udeležencem naučijo, kako prepoznati poskuse phishinga, identificirati sumljive povezave ali datoteke in spremljati svoje poštne predale za nepooblaščeno dejavnost, vključno z uporabo dvofaktorskega preverjanja pristnosti za večjo varnost. Program obravnava tudi, kako zavarovati osebne naprave, kot so računalniki, mobilni telefoni in tablični računalniki, vključno s taktikami za zaklepanje zaslona, spremljanje izgubljenih naprav, preprečevanje nepooblaščenega fizičnega dostopa in posodabljanje programske opreme za zaščito pred nastajajočimi grožnjami. Nazadnje se program osredotoča na upravljanje osebnih podatkov in zasebnost na spletu, udeležence pa nauči, kako spremeniti nastavitve zasebnosti na družbenih omrežjih, zaščititi kritične informacije in varno uporabljati javna omrežja Wi-Fi z uporabo VPN-jev.

S kombinacijo teh podtem se usposabljanje zagotovi, da starejši ne le razumejo potencialne grožnje v digitalnem okolju, ampak se tudi naučijo praktičnih metod za svojo zaščito. Udeleženci bodo modul zaključili z večjo ozaveščenostjo, samozavestjo pri obravnavanju vprašanj kibernetske varnosti in sposobnostjo za izvajanje pridobljenih rešitev v realnih scenarijih.

2.1 Cilji učenja

Glavni cilj tega modula je udeležencem posredovati praktično znanje in veščine, potrebne za učinkovito zaščito računalnikov, e-poštnih računov in osebnih podatkov pred grožnjami v kibernetskem prostoru. Udeleženci se bodo naučili, kako prepoznati potencialne grožnje, zmanjšati tveganja in izvajati strategije za izboljšanje digitalne varnosti v zasebnem in poklicnem življenju.

- Razumeti temeljna načela kibernetske varnosti, ki pomagajo preprečevati napade in zaščititi podatke pred nepooblaščenim dostopom.
- Razviti veščine za ustvarjanje močnih gesel in njihovo varno shranjevanje, s čimer se poveča odpornost proti kršitvam.
- Prepoznati in se izogniti napadom phishinga, ki so ena najpogostejših metod spletnega goljufanja.
- Učinkovito zavarujte osebne naprave in podatke, shranjene na njih, z uporabo orodij, kot so šifriranje, zaklepanje zaslona in funkcije sledenja lokacije.
- Zavestno upravljati nastavitve zasebnosti na platformah družbenih medijev, da se zmanjša tveganje za uhajanje osebnih podatkov.
- Pridobite znanje in veščine za varno uporabo javnih omrežij Wi-Fi z uporabo VPN-jev in drugih zaščitnih orodij.

2.2 Struktura, vsebina in učni izidi

Po uspešnem zaključku tega modula bodo udeleženci sposobni:

- Uvod v osnovno varnost računalnika: kako posodobiti operacijski sistem in programsko opremo, uporabljati protivirusne programe in požarne zidove, kako prepoznati znake morebitnih napadov na računalnik in kako zmanjšati tveganje za njihov nastanek.
- Ustvarjanje varnih gesel in njihovo shranjevanje: kako ustvariti močna gesla, sestavljena iz edinstvenih kombinacij črk, številk in simbolov, kako uporabljati upravitelje gesel, da se izognete shranjevanju gesel na nevarn način, npr. na papirju.
- Praktični scenariji za odkrivanje lažnih e-poštnih sporočil: analiza vzorčnih lažnih sporočil in učenje, kako prepoznati sumljive povezave, priloge ali jezikovne napake, kako prijaviti sumljive e-poštne sporočile ustreznim službam.
- Spremljanje in zaščita poštnega predala pred nepooblaščenim dostopom: kako nastaviti dvofazno preverjanje, spremljati nenavadne dejavnosti v poštnem predalu in se odzvati na poskuse hekanja.
- Zaščita osebnih naprav (računalnikov, pametnih telefonov, tabličnih računalnikov): kako zakleniti zaslon in uporabljati aplikacije, ki omogočajo lociranje izgubljenih naprav, kako zaščititi naprave pred fizičnim dostopom nepooblaščenih oseb.
- Zaščita osebnih naprav (računalnikov, pametnih telefonov, tabličnih računalnikov): kako zakleniti zaslon in uporabljati aplikacije, ki omogočajo iskanje izgubljenih naprav, kako zaščititi naprave pred fizičnim dostopom nepooblaščenih oseb.
- Redne posodobitve programske opreme za večjo varnost: zakaj so redne posodobitve potrebne za zaščito vaših naprav pred novimi grožnjami in kako nastaviti sistem za samodejne posodobitve.
- Zaščita vaše zasebnosti na družbenih omrežjih: kako prilagoditi nastavitve zasebnosti na priljubljenih platformah družbenih omrežij, katere informacije je treba ohraniti zasebne in kako se izogniti deljenju podatkov, ki bi jih lahko uporabili na neželen način.
- Pravila za varno uporabo javnih omrežij Wi-Fi: tveganja pri uporabi odprtih omrežij Wi-Fi in kako uporabiti VPN za zaščito podatkov pri povezovanju z internetom na javnih mestih.

2.3 Dnevni red | Podroben načrt seje

MODUL I
Osnove kibernetske varnosti | Zaščita računalnikov, e-pošte in osebnih podatkov

1. seja

Dobrodošli
Trajanje *5 min*

Cilji

- Ustvarjanje odprtega in privlačnega vzdušja, ki spodbuja aktivno sodelovanje.

Vsebina/metoda

- Pozdrav udeležencev in kratek predstavitev izvajalca usposabljanja.

- Predstavitev programa usposabljanja in delovnih pravil.
- Spodbujanje udeležencev, da se predstavijo (ime in ena beseda, povezana s kibernetskimi grožnjami).

Material
Ni dodatnega gradiva.

Komentar
Lahko je koristno, da namen delavnice predstavite v preprostem jeziku.

2. Srečanje

Dejavnost za spoznavanje: „Osnove kibernetske varnosti“
Trajanje *15 min*

Cilji

- Učenje in razumevanje osnovnih izrazov s področja kibernetske varnosti.
- Krepitev znanja o kibernetski varnosti.

Vsebina/metoda

- Izvedba vaje, ki vključuje povezovanje pojmov z definicijami.
- Udeleženci prejmejo delovni list (Priloga 1). Naloga udeležencev je, da vsak pojem pravilno povežejo z ustrezno definicijo. Vaja je individualna ali skupinska, odvisno od odločitve vodje. Po zaključku naloge vodja vodi kratko razpravo, med katero se obravnavajo odgovori, pojasnijo morebitne nejasnosti in raziskujejo vprašanja, povezana s temo vaje. Spodbujanje udeležencev, da se predstavijo (ime in ena beseda, povezana s kibernetskimi grožnjami).

Gradivo

- Delovni list, Icebreaker: „Osnove kibernetske varnosti“ (Priloga 1)

Komentar
Ta naloga uvaja temo in vam omogoča, da ocenite začetno raven znanja udeležencev.

3. seja

Predavanje 1: Varnost računalnikov in e-pošte
Trajanje *20 min*

Cilji

- Razumeti pomen rednega posodabljanja sistema in programske opreme.
- Prepoznati različne vrste kibernetskih groženj, vključno z zlonamerno programsko opremo, vohunsko programsko opremo in izsiljevalsko programsko opremo.
- Razumeti vlogo protivirusne programske opreme pri zagotavljanju varnosti.

- Pridobiti znanje in veščine za varno uporabo javnih omrežij Wi-Fi z uporabo VPN-jev in drugih varnostnih orodij.

Vsebina/metoda

- Predavanje, ki pojasnjuje osnovne koncepte: zakaj so redne posodobitve sistema ključnega pomena, kako zlonamerna programska oprema prodre v sisteme, kakšna je vloga protivirusne programske opreme in kako prepoznati varno Wi-Fi omrežje.
- Uporaba primerov iz resničnega življenja (npr. znani napadi izsiljevalske programske opreme) za ponazoritev tveganj, povezanih z zastarelimi sistemi in nezavarovanimi napravami.
- Poudarjanje najboljših praks, kot so omogočanje samodejnih posodobitev in izogibanje sumljivim prenosom. Za izvedbo predavanja ima izvajalec na voljo predloge tem iz Priloge 2.

Gradivo

- Predlogi tem za razpravo (priloga 2)

Komentar

Udeležence je vredno spodbuditi k aktivni udeležbi na predavanju, tako da jim omogočite, da postavljajo vprašanja.

Dejavnost 1 „Kviz: Res/Neresnično“
Trajanje *20 min*

Cilji

- Utrjevanje znanja iz predavanja, razvoj zavesti o grožnjah.

Vsebina/metoda

- Tečaj vključuje vajo v obliki kviza z naslovom „Resnično ali napačno?“, ki se izvaja na podlagi delovnega lista (Priloga 3), ki ga udeleženci prejmejo od izvajalca.
- Udeleženci imajo 5 minut časa, da samostojno označijo svoje odgovore. Po zaključku te faze vodja tečaja vodi kratko razpravo, med katero se z udeleženci pogovori o pravilnih odgovorih, pojasni pomembna vprašanja in popravi morebitna napačna prepričanja. Na koncu vodja tečaja povzame ključne vsebine, obravnavane v kvizu, s čimer okrepi razumevanje in utrdi dobre prakse v zvezi z digitalno varnostjo.

Gradivo

- Delovni list Kviz: Resnično/Neresnično (Priloga 3)

Komentar

Po kvizu povzemite ključne točke, da okrepite razumevanje udeležencev o bistvenih varnostnih praksah.

Odmor | Trajanje *5’*

- **Udeležencem omogočite čas za počitek in razmislek.**
- **Kratek odmor za osvežitev.**

- **Udeležence spodbudite, da se raztegnejo ali si privoščijo pijačo, da si pred naslednjim predavanjem napolnijo baterije.**

4. Srečanje

Predavanje 2: Praktične vaje v zvezi z varnostjo e-pošte
Trajanje *30 min*

Cilji

- Spoznajte najboljše prakse za ustvarjanje močnih in varnih gesel (npr. uporaba velikih in malih črk, posebnih znakov in številk).
- Razumevanje tveganj slabe shranjevanja gesel in spoznavanje upraviteljev gesel.

Vsebina/metoda

- Pojasnite „pravilo treh komponent“ (dolžina, zapletenost, edinstvenost) za ustvarjanje močnih gesel. Prikažite, kako delujejo upravitelji gesel, in razpravljajte o njihovih prednostih (npr. večja varnost, udobnost). Izpostavite pogoste napake, kot so ponovna uporaba gesel ali njihovo shranjevanje v nezavarovanih datotekah.

Gradivo

- Predlog tem za razpravo (Priloga 4)

Komentar

Dajte praktične nasvete, s katerimi se lahko udeleženci poistovetijo, npr. ustvarjanje gesla na podlagi enostavne, a edinstvene fraze.

Dejavnost 2: Ustvarjanje močnih gesel
Trajanje *20 min*

Cilji učenja

- Uporabite navodila, ki so bila obravnavana, in ustvarite močna, edinstvena gesla.

Vsebina/metoda

- Vaja poteka v dveh fazah – najprej posamezno, nato v parih. Za vajo je pripravljen delovni list (Priloga 5).
- Udeleženci samostojno ustvarijo vsaj tri močna gesla v skladu z varnostnimi načeli in jih zapišejo na kartice. Nato jih pokažejo svojemu partnerju iz para, ki oceni njihovo dolžino, zapletenost in edinstvenost ter poda povratne informacije in morebitne predloge za izboljšanje. Na koncu vodja usposabljanja razloži značilnosti varnega gesla in sproži razpravo z vsemi udeleženci, ki omogoča izmenjavo mnenj in dobrih praks.

Gradivo

- Delovni list Ustvarjanje močnih gesel (Priloga 5)

Komentar

Udeležence je vredno spodbuditi, naj v skladu z navodili izvajalca vadbe preverijo, ali so gesla, ki jih trenutno uporabljajo, varna.

Odmor | Trajanje *5 min*

- **Omogočite čas za počitek in pripravo.**
- **Kratek odmor za osvežitev.**
- **Kratek odmor za osvežitev in sprostitev.**

5. Srečanje

Predavanje 3: Zaščita osebnih naprav in podatkov

Trajanje *30 min*

Cilji

- Pridobiti znanje o prepoznavanju lažnih e-poštnih sporočil.
- Razumeti, kako konfigurirati osnovne varnostne nastavitve e-pošte.

Vsebina/metoda

- Pojasni značilne znake lažnih e-poštnih sporočil, kot so pravopisne napake, neznani naslovi pošiljateljev in nujna sporočila. Pokaže, kako prilagoditi varnostne nastavitve e-pošte na platformah, kot sta Gmail in Outlook. Pokaže primere lažnih e-poštnih sporočil in razloži, kako prepoznati opozorilne znake.

Material

Dodatni materiali niso potrebni.

Komentar

Prikaz resničnih primerov phishinga iz priljubljenih storitev (npr. PayPal, Amazon), da bi vsebina bila privlačnejša.

Dejavnost 3: Analiza lažnih e-poštnih sporočil

Trajanje *20 min*

Cilji učenja

- Praktična analiza e-pošte – odkrivanje nepravilnosti.

Vsebina/metoda

- Izobraževalec ima na voljo niz predlog za e-pošto (Priloga 6), ki jih je treba pred razdelitvijo udeležencem dopolniti s podrobnostmi, kot so vzorčne povezave, imena znanih podjetij (npr. banke, kurirske službe ali nakupovalne platforme).
- Vaja se izvaja v parih ali manjših skupinah. Udeleženci analizirajo pripravljene e-pošte iz delovnega lista (Priloga 6) in identificirajo ter označijo sumljive elemente. Po končani analizi sledi skupinska razprava, ki jo vodi vodja.

Predlagana vprašanja za razpravo:

- Kakšni opozorilni signali so v tem e-sporočilu?
- Kako se lahko zaščitite pred takšnim napadom?
- Kaj naj storite, če prejmete sumljivo e-poštno sporočilo te vrste?
- Pripravite se na razpravo o odgovorih s skupino.

Gradivo

❖ Delovni list, Analiza lažnega e-poštnega sporočila (Priloga 6)

Komentar

Povzetek rezultatov skupinske analize, ki poudarja ključne razlike med pravimi in ponarejenimi e-poštnimi sporočili.

Odmor

Trajanje 5 min

❖ **Čas za počitek in pripravo.**

❖ **Kratek odmor za osvežitev.**

❖ **Kratek odmor za osvežitev in sprostitev.**

6. Srečanje

Predavanje 4: Upravljanje osebnih podatkov in zasebnost na spletu

Trajanje *30 min*

Cilji

❖ Sporazumevanje o pravilih zasebnosti, nastavitvah zasebnosti, zaklepanju in posodabljanju. Sporazumevanje o osnovnih varnostnih nastavitvah za zaščito naprav (npr. omogočanje zaklepanja zaslona in samodejnih posodobitev).

❖ Razumevanje, kako učinkovito upravljati nastavitve zasebnosti na spletu.

Vsebina/metoda

❖ Razprava o načinih zaščite podatkov na družbenih omrežjih (Instagram, Facebook), nastavitvah zasebnosti na pametnih telefonih in omejitvah deljenja aplikacij.

❖ Izobraževalec razpravlja o ključnih varnostnih nastavitvah na pametnih telefonih in računalnikih, kot so zaklepanje zaslona, šifriranje podatkov, upravljanje aplikacij in nastavitve dovoljenj na sistemih Android in iOS.

❖ Razpravljajte o upravljanju zasebnosti na spletu – kako nastaviti nastavitve zasebnosti na platformah družbenih medijev, nadzorovati, kdo lahko vidi objave, osebne podatke in katere aplikacije imajo dostop do vaših podatkov.

❖ Pogovorite se o načelih preverjanja varnosti Wi-Fi – kako prepoznati nezavarovane povezave, zakaj se je treba izogibati nezavarovanim javnim omrežjem in kako povečati varnost domačega internetnega omrežja.

❖ Poudarite pomen rednega pregledovanja nastavitev zasebnosti – pomen rednega pregledovanja in posodabljanja nastavitev zasebnosti, da se prilagodite spreminjajočim se potrebam in novim spletnim grožnjam.

Material

Dodatno gradivo ni potrebno.

Komentar

Osredotočite se na praktične, enostavno izvedljive korake za izboljšanje varnosti in zasebnosti naprav.

Dejavnost 4: Varna konfiguracija naprave
Trajanje *20 min*

Cilji

- Uporaba znanja pri konfiguraciji varnostnih nastavitev na osebnih napravah.

Vsebina/metoda

- Udeleženci se naučijo nastaviti zaklepanje zaslona, omogočiti dvofazno preverjanje in prilagoditi nastavitve zasebnosti. Izvajalec usposabljanja po potrebi nudi individualno podporo.

Material

- Pametni telefoni in/ali računalniki.

Komentar

Udeležence spodbujajte, naj med nastavljanjem naprav rešujejo težave in postavljajo vprašanja.

7. Srečanje

Razprava
Trajanje *10 min*

Cilji učenja

- Razmislite o ključnih spoznanjih.
- Udeležence spodbudite, da delijo svoje najbolj dragocene spoznanje in preostala vprašanja.

Vsebina/metoda

- Moderirana razprava, v kateri udeleženci delijo svoje opažanja, izkušnje in vprašanja, ki zahtevajo pojasnilo. Izobraževalec povzame ključne točke in odgovori na vprašanja.

Material

Dodatni materiali niso potrebni.

Komentar

Udeležence spodbujajte, naj naučene koncepte povežejo s svojim vsakdanjim spletnim vedenjem.

Zaključek
Trajanje *5 min*

Cilji učenja

- Povzemite ključne točke učenja in zagotovite vire za nadaljnje učenje.

- ❖ Zahvalite se udeležencem in zaključite sejo.

Vsebina/metoda

- ❖ Povzetek ključnih točk učenja iz usposabljanja.
- ❖ Deljenje dodatnih virov (npr. spletne strani o kibernetski varnosti, članki).
- ❖ Zahvalite se udeležencem za njihovo sodelovanje in jih spodbudite, naj nadaljujejo z izboljševanjem svojih praks na področju kibernetske varnosti.

Gradivo

- ❖ Priporočila za nadaljnje branje in učenje za udeležence (Priloga 7)
- ❖ Spletne strani o kibernetski varnosti: evropske in vladne organizacije za kibernetsko varnost

Komentar

Na koncu je smiselno izvesti kratko evalvacijsko anketo.

2.4 Dodatne informacije

2.4.1 Samorefleksija izobraževalcev

- ➢ Ali sem udeležencem jasno in učinkovito posredoval pomen spletne varnosti in zavestne uporabe družbenih medijev?
- ➢ Ali sem uporabil praktične primere, ki so pomagali bolje razumeti digitalne grožnje?
- ➢ Ali sem zagotovil, da so udeleženci razumeli tehnične vidike nastavitev zasebnosti in prepoznavanja prevar?
- ➢ Ali sem zagotovil, da so udeleženci razumeli tehnične vidike nastavitev zasebnosti in so bili sposobni prepoznati prevare, kot je phishing?
- ➢ Ali sem prilagodil podane informacije ravni napredka udeležencev?
- ➢ Kako sem udeležence vključil v dejavnosti in razprave?
- ➢ Ali sem spodbujal aktivno sodelovanje, izmenjavo izkušenj in zastavljanje vprašanj?
- ➢ Ali so bili uporabljeni materiali in viri (npr. predstavitve, kvizi, praktične vaje) koristni in primerni za udeležence?
- ➢ Ali so bili pripravljeni materiali jasni in lahko razumljivi?

2.4.2 Ocena programa s strani izobraževalcev

- ➢ Je bila vsebina usposabljanja ustrezna potrebam starejših in primerno prilagojena njihovi ravni znanja in izkušenj?
- ➢ So imeli udeleženci priložnost razumeti osnovna načela kibernetske varnosti in zasebnosti na spletu?
- ➢ So dejavnosti, kot so kvizi, praktične vaje in analiza primerov phishinga, podpirale učni proces udeležencev?
- ➢ So razprave omogočile poglobitev znanja in spodbudile razmišljanje o digitalni varnosti?
- ➢ Ali so doseženi rezultati (npr. razumevanje digitalnih groženj, sposobnost konfiguriranja varnostnih nastavitev) v skladu z nameravanimi izobraževalnimi cilji modula?
- ➢ So udeleženci osvojili ključne veščine, kot so ustvarjanje močnih gesel, prepoznavanje goljufij in upravljanje zasebnosti na spletu?

2.4.3 Gradivo, dodatni viri

Priloga 1 | Delovni list Uvodna dejavnost: „Osnove kibernetske varnosti“
Povežite pojem s pravilno definicijo:

Phishing	**goljufiva metoda, pri kateri se nekdo izdaja za zaupanja vredno osebo, da bi ukradel občutljive podatke.**
Izsiljevalska programska oprema	**zlonamerna programska oprema, ki šifrira podatke in zahteva odkupnino za njihovo sprostitev.**
Dvostopenjska avtentikacija (2FA)	**dodatna varnostna plast, ki zahteva drugi avtentifikacijski faktor.**
Gesla in Upravitelji gesel	**za upravljanje močnih in edinstvenih gesel za različne storitve.**
Požarni zid	**varnostni sistem, ki ščiti pred nepooblaščenim dostopom do omrežja.**
Šifriranje podatkov	**metoda zaščite podatkov pred nepooblaščenim dostopom s pretvorbo v nečitljivo kodo.**
VPN (Virtualna zasebna omrežja)	**tehnologija, ki zagotavlja varne in zasebne internetne povezave.**
Varna e-pošta	**praksa zaščite e-poštnih sporočil pred napadi, kot sta filtriranje neželene pošte in šifriranje.**
SOC (Center za varnostne operacije)	**operativni center, odgovoren za spremljanje in odzivanje na grožnje kibernetski varnosti.**

Priloga 1 | Delovni list Uvodna aktivnost: „Osnove kibernetske varnosti“
Pravilni odgovori

1. **Phishing** – goljufiva metoda, pri kateri se nekdo izdaja za zaupanja vredno osebo, da bi ukradel občutljive podatke.
2. **Ransomware** – zlonamerna programska oprema, ki šifrira podatke in zahteva odkupnino za njihovo sprostitev.
3. **Dvostopenjska avtentikacija (2FA)** – dodatna varnostna plast, ki zahteva drugi avtentikacijski faktor.
4. **Gesla in upravitelji gesel** – strategije za upravljanje močnih in edinstvenih gesel za različne storitve.
5. **Požarni zid** – varnostni sistem, ki ščiti pred nepooblaščenim dostopom do omrežja.
6. **Šifriranje podatkov** – metoda zaščite podatkov pred nepooblaščenim dostopom s pretvorbo v nečitljivo kodo.
7. **Zlonamerna programska oprema** – programska oprema, zasnovana za škodovanje uporabnikom ali računalniškim sistemom.
8. **VPN (Virtual Private Network)** – tehnologija, ki zagotavlja varne in zasebne internetne povezave.
9. **Varna e-pošta** – prakse za zaščito e-poštnih sporočil pred napadi, kot so filtriranje spamov in šifriranje.
10. **SOC (varnostni operativni center)** – operativni center, odgovoren za spremljanje in odzivanje na grožnje kibernetski varnosti.

Priloga 2 | Predlagane teme za razpravo Predavanje 1 | Varnost računalnikov in e-pošte

- Pomen rednih posodobitev operacijskih sistemov in aplikacij.
- Tveganja zastarelih sistemov in nezavarovanih naprav.
- Vrste zlonamerne programske opreme: virusi, trojanski konji, izsiljevalska programska oprema in kako delujejo.
- Mehanizmi, ki omogočajo zlonamerni programski opremi, da se infiltrira v sisteme.
- Vloga protivirusne programske opreme pri zaščiti pred kibernetskimi grožnjami.
- Uporaba požarnih zidov za zaščito pred napadi.
- Prakse upravljanja gesel, vključno z uporabo upraviteljev gesel.
- Pravila za izogibanje nevarnim prilogam in sumljivim povezavam v e-pošti.
- Pomen šifriranja podatkov za zaščito zasebnosti in varnosti.
- Samodejne posodobitve kot najboljša praksa za zagotavljanje varnosti.
- VPN-ji in njihova vloga pri zaščiti zasebnosti na spletu.
- Zakaj niso vsa brezplačna omrežja Wi-Fi varna?
- Osnovna zaščita e-pošte pred lažnim predstavljanjem in neželeno pošto.
- Najboljše prakse za ustvarjanje močnih gesel in njihov vpliv na varnost.
- Varnost mobilnih naprav in aplikacij.
- Pomen izobraževanja in ozaveščanja uporabnikov pri preprečevanju kibernetskih napadov.

Priloga 3 | Delovni list Kviz: Res/Neresnično

Označite, katere trditve so pravilne in katere napačne.

- Redne posodobitve operacijskega sistema in aplikacij so potrebne le za nove naprave. **Res/Neresnično**
- Zlonamerna programska oprema, kot so virusi ali trojanski konji, lahko prodira v sisteme prek zastarele programske opreme in varnostnih ranljivosti. **Res/Neresnično**
- Protivirusna programska oprema ni potrebna, če se sistem redno posodablja. **Res/Neresnično**
- Požarni zid se uporablja le za zaščito pred fizičnimi napadi na naprave. **Res/Neresnično**
- Upravljanje gesel in uporaba upraviteljev gesel sta ključnega pomena za ohranjanje močnih, edinstvenih gesel za različne storitve. **Res/Neresnično**
- Izogibanje sumljivim prilogam v e-pošti ni pomembno, če je nameščena protivirusna programska oprema. **Res/Neresnično**
- Šifriranje podatkov pomaga zaščititi zasebnost in varnost pred nepooblaščenim dostopom. **Res/Neresnično**
- Samodejne posodobitve so neobvezne, ker je za zagotovitev varnosti vedno dovolj ročno posodabljanje sistema. **Res/Neresnično**
- VPN (Virtual Private Network) omogoča varno povezavo z internetom in skriva naše spletne aktivnosti. **Res/Neresnično**
- Phishing je tehnika napada, ki vključuje krajo gesel prek navidezno zaupanja vrednih e-poštnih sporočil. **Res/Neresnično**
- Močno geslo naj bi bilo sestavljeno samo iz črk in naj bi bilo enostavno za zapomniti, da ga ni težko uporabljati. Mobilne naprave zahtevajo manj varnostnih ukrepov kot namizni računalniki, saj so manj dovzetne za napade. **Res/Neresnično**
- Mobilne naprave zahtevajo manj varnostnih ukrepov kot namizni računalniki, saj so manj dovzetne za napade. **Res/Neresnično**
- Znanje uporabnikov o spletnih grožnjah je bistveno za preprečevanje kibernetskih napadov.
- Ransomware je programska oprema, ki blokira dostop do sistema ali datotek in zahteva odkupnino za njihovo odklepanje. **Res/Neresnično**
- Zastareli operacijski sistem je varen, ker starejše različice programske opreme redko postanejo tarča napadov. **Res/Neresnično**

Priloga 3 | Delovni list Kviz: Res/Neresnično
Pravilni odgovori

1. Redne posodobitve operacijskega sistema in aplikacij so potrebne le za nove naprave. **Neresnično**
2. Zlonamerna programska oprema, kot so virusi ali trojanski konji, lahko prodira v sisteme prek zastarele programske opreme in varnostnih ranljivosti. **Res**
3. Protivirusna programska oprema ni potrebna, če se sistem redno posodablja. **Neresnično**
4. Požarni zid se uporablja le za zaščito pred fizičnimi napadi na naprave. **Neresnično**
5. Upravljanje gesel in uporaba upraviteljev gesel sta ključnega pomena za ohranjanje močnih, edinstvenih gesel za različne storitve. **Res**
6. Izogibanje sumljivim prilogam v e-pošti ni pomembno, če je nameščena protivirusna programska oprema. **Neresnično**
7. Šifriranje podatkov pomaga zaščititi zasebnost in varnost pred nepooblaščenim dostopom. **Res**
8. Samodejne posodobitve so neobvezne, ker je za zagotovitev varnosti vedno dovolj ročno posodabljanje sistema. **Neresnično**
9. VPN (Virtual Private Network) omogoča varno povezavo z internetom in skriva naše spletne dejavnosti. **Res**
10. Phishing je tehnika napada, ki vključuje krajo gesel prek navidezno zaupanja vrednih e-poštnih sporočil. **Res**
11. Močno geslo naj bi bilo sestavljeno samo iz črk in naj bi bilo enostavno za zapomniti, da ga ni težko uporabljati. **Neresnično**
12. Mobilne naprave zahtevajo manj varnostnih ukrepov kot namizni računalniki, saj so manj dovzetne za napade. **Neresnično**
13. Znanje uporabnikov o spletnih grožnjah je bistveno za preprečevanje kibernetskih napadov. **Res**
14. Ransomware je programska oprema, ki blokira dostop do sistema ali datotek in zahteva odkupnino za njihovo odklepanje. **Neresnično**
15. Zastareli operacijski sistem je varen, ker starejše različice programske opreme redko postanejo tarča napadov. **Neresnično**

Priloga 4 | Predlagane teme za predavanje 2 „Varnost e-pošte – praktične vaje”

- Ustvarjanje varnih gesel – načela za ustvarjanje močnih gesel, ki jih je težko razvozlati, vključno z uporabo različnih vrst znakov (velike črke, male črke, številke, posebni znaki).
- Upravljanje gesel – kako se izogniti shranjevanju gesel na nezavarovanih mestih, kot so papirnate beležke, in kako uporabljati upravitelje gesel za varno shranjevanje.
- Načelo treh komponent – razlaga, zakaj mora biti geslo ustrezne dolžine, zapletenosti in edinstvenosti, da se zagotovi visoka varnost.
- Vloga upraviteljev gesel – razprava o tem, kako delujejo upravitelji gesel in kakšne prednosti ponujajo, na primer varnost in udobje pri upravljanju več gesel.
- Pogoste napake pri upravljanju gesel – kako nevarno je ponovno uporabljati ista gesla v različnih storitvah ali jih shranjevati v nezavarovanih datotekah.
- Varnostne prakse pri e-pošti – kako se izogibati sumljivim povezavam in prilogam ter kako uporabljati dodatne metode zaščite, kot je šifriranje.

Priloga 5 | Delovni list „Ustvarjanje močnih gesel“
Ustvarite močna in varna gesla na podlagi naslednjih načel:

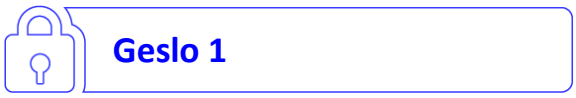
- **Ustrezna dolžina (najmanj 12 znakov),**
- **Zapletenost (velike in male črke, številke, posebni znaki),**
- **Edinstvenost (brez očitnih vzorcev, kot je datum rojstva).**

Individualno delo: Napišite vsaj tri različna gesla:

Dodatek 5 | Delovni list | Ustvarjanje močnih gesel

Delajte v parih:

· Po končanem individualnem delu se združite z drugim udeležencem.
· Pokažite jim svoja gesla.
· Prosite ga, naj označi (npr. s plusom), ali gesla izpolnjujejo vsa merila.
· Izobraževalec lahko poda komentarje in predloge za morebitne izboljšave.



Dolžina

Zapletenost

Vsestranskost

Opombe

Dolžina

Zapletenost

Vsestranskost

Opombe

Dolžina

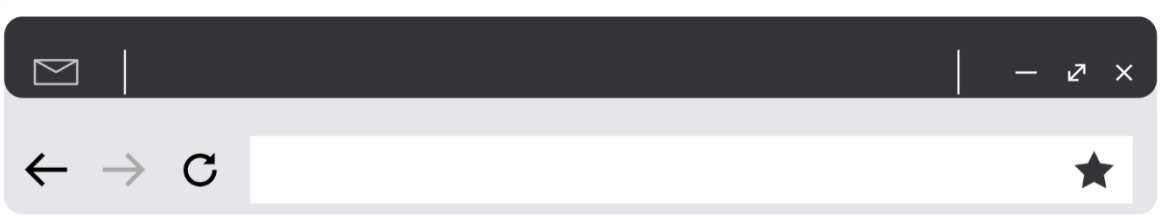
Zapletenost

Vsestranskost

Opombe

Priloga 6 | Delovni list | Analiza lažnih e-poštnih sporočil

Pozorno preberite spodnja e-poštna sporočila. Prepoznajte elemente, ki kažejo, da gre za lažna e-poštna sporočila.



Subject : **Nujno! Vaš račun je bil blokiran!**

Spoštovani uporabnik

zaradi sumljive aktivnosti na vašem računu je bil vaš račun začasno blokiran, da bi zaščitili vaše osebne podatke. Da bi se izognili trajni blokadi, nemudoma preverite svoj račun.

Kliknite tukaj, da preverite svoje podatke in odblokirate svoj račun: [Phishing povezava]

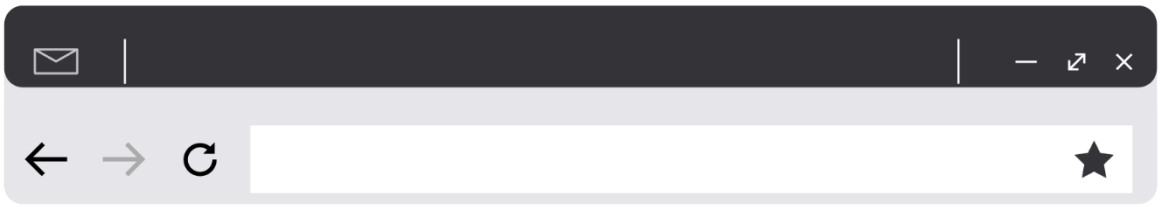
Če tega ne storite v 24 urah, bo vaš račun trajno blokiran. Prosimo, ukrepajte hitro, da se izognete neprijetnostim.

Če imate kakršna koli vprašanja, se obrnite na našo ekipo za tehnično podporo.

S spoštovanjem
Varnostna ekipa
[Lažno podjetje]

Priloga 6 | Delovni list | Analiza lažnih e-poštnih sporočil

Pozorno preberite spodnja e-poštna sporočila. Prepoznajte elemente, ki kažejo, da gre za lažna e-poštna sporočila.



Subject : **Posodobite svoje podatke! Vaš račun je treba preveriti**

Pozdravljeni [ime],

Vaš račun pri [lažno podjetje] zahteva takojšnjo posodobitev vaših osebnih podatkov. Zaradi rednega varnostnega pregleda moramo zagotoviti, da so vaši podatki posodobljeni, da vam lahko omogočimo polni dostop do naših storitev. Za posodobitev podatkov kliknite spodnjo povezavo in se prijavite v svoj račun:

[Povezava za lažno e-pošto – kliknite tukaj, da posodobite svoje podatke]

Po kliku na povezavo boste preusmerjeni na stran, kjer boste morali vnesti svoje prijavne podatke, številko kreditne kartice in druge občutljive podatke.

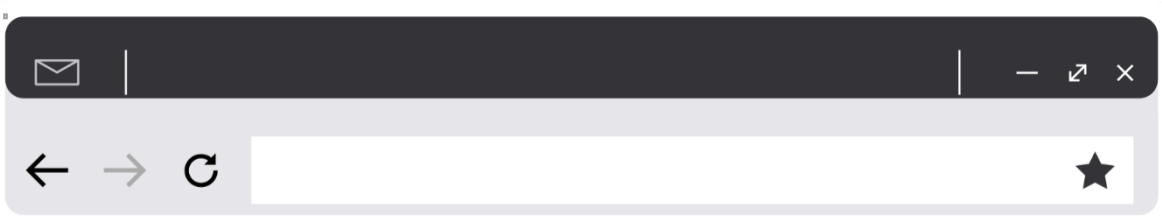
OPOZORILO: Če svojih podatkov ne posodobite v 48 urah, bo vaš račun trajno blokiran.

Hvala za razumevanje in sodelovanje.

S spoštovanjem
[Lažno podjetje]
Ekipa za podporo strankam

Priloga 6 | Delovni list | Analiza lažnih e-poštnih sporočil

Pozorno preberite spodnja e-poštna sporočila. Prepoznajte elemente, ki kažejo, da gre za lažna e-poštna sporočila.



Subject : **Potrditev pošiljke – paket ni bil dostavljen**

Dober dan

Vaš paket ni bil dostavljen zaradi napačnih naslovnih podatkov. Nemudoma preverite svoje podatke, da bomo lahko ponovno poskusili dostaviti paket.

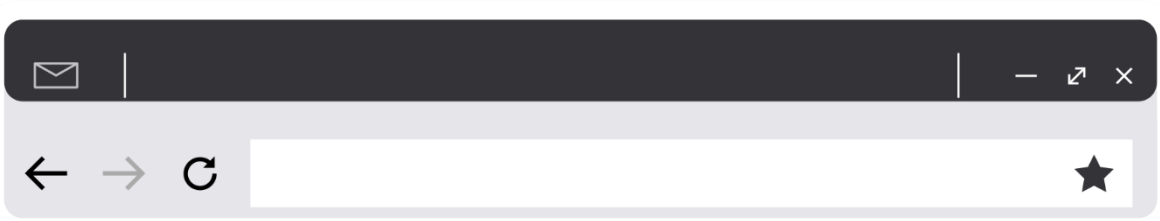
Kliknite tukaj, da posodobite svoje podatke za dostavo: [phishing povezava]

Če naslova ne potrdite v 24 urah, bo paket vrnjen pošiljatelju in vam bodo nastali dodatni stroški.

Hvala za vaš hiter odgovor.
Ekipa za dostavo
[Lažna kurirska družba]

Priloga 6 | Delovni list | Analiza lažnih e-poštnih sporočil

Pozorno preberite spodnja e-poštna sporočila. Prepoznajte elemente, ki kažejo, da gre za lažna e-poštna sporočila.



Subject : **Prejeli ste e-darilno kartico! Zahtevajte jo zdaj!**

Čestitamo!

Izbrani ste bili kot zmagovalec naše naključne promocije. Prejeli boste e-darilno kartico v vrednosti 500 PLN, ki jo lahko uporabite v [Popular Retail Network].

Da bi prevzeli nagrado, kliknite na spodnjo povezavo in potrdite svoje podatke:
[phishing povezava – prevzem e-kartice]

Ponudba velja le 12 ur.
Ne zamudite priložnosti!

Lep dan!
Oddelek za promocijo
[Lažno podjetje ali trgovska mreža]

Priloga 7 | Priporočila za nadaljnje branje in učenje za udeležence

Spletne strani o kibernetski varnosti: Evropske in vladne organizacije, ki se ukvarjajo s kibernetsko varnostjo

1) **ENISA (Agencija Evropske unije za kibernetsko varnost)**
   Spletna stran: https://www.enisa.europa.eu/
   ENISA je agencija EU, ki se ukvarja s kibernetsko varnostjo in objavlja poročila, navodila in opozorila o kibernetskih grožnjah.

2) **CERT-EU (skupina za odzivanje na računalniške izredne dogodke za institucije EU)**
   Spletna stran: https://cert.europa.eu/
   Organizacija spremlja kibernetske grožnje in odgovarja na kibernetske napade na evropske institucije.

3) **EC3 – Europolov center za kibernetski kriminal**
   Spletna stran: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime
   Europol ponuja informacije o kibernetskem kriminalu in varnosti podatkov.

4) **NCSC UK (Nacionalni center za kibernetsko varnost)**
   Spletna stran: https://www.ncsc.gov.uk/
   Portal britanske vlade za kibernetsko varnost, ki ponuja vodnike, opozorila in spletne tečaje za državljane, podjetja in javne institucije.

2.5 Modul I – Predhodni/naknadni test

1. Katera od naslednjih trditev najbolje opisuje „phishing“?

A) Namestitev posodobitev za izboljšanje delovanja računalnika
B) Metoda, s katero se ljudi z lažnimi e-poštnimi sporočili zvabi v razkritje osebnih podatkov
C) Vrsta protivirusnega programa
D) Postopek šifriranja podatkov

2. Zakaj so redne posodobitve programske opreme pomembne?

A) Zaradi njih je računalnik počasnejši
B) Spremenijo zasnovo računalnika
C) Popravijo varnostne ranljivosti in ščitijo pred novimi grožnjami
D) Odstranijo protivirusno programsko opremo

3. Katera je glavna funkcija požarnega zidu?

A) Pospešiti vašo internetno povezavo
B) Zaščita pred nepooblaščenim dostopom do omrežja
C) Varno shranjevanje gesel
D) Samodejno brisanje neželene pošte

4. Katero od naslednjih gesel je najvarnejše?

A) geslo123
B) 12345678
C) MyDogIsCute
D) M@rK_82!x

5. Kaj naj storite, če prejmete e-pošto od neznanega pošiljatelja, ki vas prosi za osebne podatke?

A) Takoj odgovorite z vašimi podatki
B) Kliknite na povezavo, da preverite, za kaj gre
C) Izbrišite e-poštno sporočilo ali ga prijavite kot phishing
D) Posredujte ga svojim prijateljem, da jih opozorite

6. Za kaj se uporablja „dvostopenjska avtentikacija (2FA)“?

A) Omogoča vam, da uporabljate dve gesli hkrati
B) Dodaja dodatno raven varnosti, saj zahteva dve obliki preverjanja
C) Samodejno šifrira vaše e-poštne sporočila
D) Shrani vaše podatke za prijavo

7. Katera od naslednjih trditev o javnih omrežjih Wi-Fi je PRAVILNA?

A) Vedno so varna, če je povezava brezplačna
B) Pri uporabi javnega Wi-Fi-ja se morate izogibati vnašanju občutljivih podatkov
C) Lahko jih varno uporabljate brez gesla
D) Vaše podatke samodejno šifrirajo

8. Kakšen je namen VPN (virtualnega zasebnega omrežja)?

A) Izboljšati hitrost vašega interneta
B) Blokiranje pojavnih oglasov
C) Zagotoviti varno in zasebno povezavo z internetom
D) Za upravljanje vaših gesel

9. Kateri od naslednjih primerov je primer izsiljevalske programske opreme?

A) Programska oprema, ki šifrira vaše datoteke in zahteva plačilo za njihovo odklepanje
B) Protivirusni program, ki pregleduje vaš sistem
C) Orodje za blokiranje neželene e-pošte
D) Aplikacija požarni zid

10. Katera je dobra praksa za zaščito vaše zasebnosti na družbenih omrežjih?

A) Deljenje vašega polnega naslova in telefonske številke
B) Nastavitev vseh objav na „javno“
C) Redno pregledovanje in prilagajanje nastavitev zasebnosti
D) Uporaba istega gesla za vse račune

Povzetek odgovorov

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

MODUL II

Pogoste spletne prevare, ki so usmerjene v starejše

3. Modul II – Pogoste spletne prevare, usmerjene v starejše

Ta štiriurni modul starejšim omogoča, da prepoznajo, razumejo in se zaščitijo pred spletnimi prevari in grožnjami kibernetski varnosti. Obravnava njihove posebne ranljivosti s praktičnimi strategijami in preventivnimi ukrepi, s čimer spodbuja zaupanje v varno uporabo digitalnih tehnologij. Udeleženci se bodo naučili, kako delujejo prevare, prepoznali opozorilne znake v digitalni komunikaciji in razumeli manipulacijske taktike, kot je socialni inženiring. Modul obravnava pogoste prevare (phishing, smishing, vishing) in tehnične grožnje (zlonamerna programska oprema, izsiljevalska programska oprema, vohunska programska oprema) ter ponuja strategije za zaščito. Poleg tega poudarja varnost osebnih podatkov in starejšim omogoča, da zaupajo v shranjevanje, deljenje in varnostno kopiranje občutljivih podatkov.

3.1 Cilji učenja

Cilj tega modula je izboljšati razumevanje starejših o pogostih spletnih prevarah, taktikah, ki jih uporabljajo prevaranti, ter pomenu prepoznavanja in izogibanja digitalnim grožnjam. Udeležencem želimo posredovati praktična znanja in preventivne ukrepe za zaščito pred tveganji kibernetske varnosti, vključno s phishingom, smishingom, vishingom in zlonamerno programsko opremo. Želimo okrepiti zaupanje in digitalno pismenost starejših, tako da jih naučimo, kako varovati osebne podatke, prepoznati manipulacijske taktike in varno uporabljati digitalne tehnologije.

- Razumevanje delovanja prevar in prepoznavanje psiholoških in tehnoloških metod, ki jih uporabljajo prevaranti.
- Prepoznavanje sumljivih vsebin in razlikovanje med legitimno in goljufivo komunikacijo.
- Pridobivanje znanja o pogostih vrstah prevar in učenje strategij za zaščito pred kibernetskimi grožnjami.
- Krepitev zaupanja v varovanje osebnih podatkov, ustvarjanje varnostnih kopij in varno uporabo digitalnih orodij.

3.2 Struktura, vsebina in učni izidi

Po uspešnem zaključku tega modula bodo udeleženci sposobni:

- Prepoznati pogoste tehnike, tehnologije in cilje, ki se uporabljajo v prevarah, ter pojasniti, kako prevaranti zavajajo svoje žrtve.
- Prepoznati opozorilne znake v digitalnih vsebinah, kot so e-pošta, SMS-sporočila, spletne strani in oglasi, ter razlikovati med legitimnimi in sumljivimi sporočili.
- Opredeliti socialni inženiring, prepoznati pogoste taktike, ki jih uporabljajo prevaranti, razumeti, zakaj so pogosto tarča starejši ljudje, in uporabiti preventivne ukrepe za zaščito pred napadi socialnega inženiringa.
- Pojasniti, kako goljufi izkoriščajo čustva in pogoste vedenjske vzorce starejših, ter uporabiti strategije, da ostanejo mirni in previdni, ko so pod čustvenim pritiskom.
- Prepoznajte najpogostejše vrste prevar, vključno s phishingom, smishingom, vishingom in prevarami z lažno identiteto ali finančnimi prevarami, ter opišite manipulacijske tehnike, ki se uporabljajo v vsaki od njih.
- Prepoznajte različne vrste zlonamerne programske opreme, kot so malware, ransomware, spyware, virusi in trojanski konji, opišite metode za zaščito pred njimi, prepoznajte nevarna pojavna okna, jih varno zaprite in uporabite orodja za blokiranje pojavnih oken in preverjanje varnosti spletnih strani.

- Opredeliti osebne podatke, prepoznati, katere vrste so dragocene za goljufe in kako se izkoriščajo, ter uporabiti najboljše prakse za varno shranjevanje in deljenje osebnih podatkov.
- Pojasnite pomen varnostnega kopiranja podatkov, izvedite nasvete za zmanjšanje ranljivosti za izgubo podatkov in zgradite zaupanje v varno uporabo tehnologije.

3.3 Dnevni red I Podroben načrt seje

MODUL II
Pogoste spletne prevare, usmerjene v starejše

1. seja

Dobrodošli
Trajanje *5 min*

Cilji

- Predstavite temo in ustvarite prijetno vzdušje.

Vsebina/metoda

- Kratek uvod v sejo, opis ciljev in postavitev pričakovanj
- Pripravite teren za usposabljanje s predstavitvijo modula in njegovega pomena.

Material

- Tabla ali flipchart za cilje seje.
- Flomasterji.
- Natisnjena agenda ali predstavitvene diapozitive, ki opisujejo sejo.

2. seja

Dejavnost za spoznavanje: „Dve resnici in ena laž“
Trajanje *10 min*

Cilji

- Po zaključku te dejavnosti bodo udeleženci znali razlikovati med pravilnimi varnostnimi praksami na spletu in pogostimi zmotnimi prepričanji, ki se uporabljajo v prevarah.

Vsebina/metoda

- Interaktivna skupinska vaja v obliki igre z naslovom „Dve resnici in ena laž“, katere cilj je predstaviti ključne koncepte, povezane z goljufijami in varnostjo na internetu. Udeleženci analizirajo kratke izjave, jih obravnavajo v parih ali manjših skupinah in ugotovijo, katera je napačna (laž ali mit). Izvajalec vaje zagotovi hitro povratno informacijo in pojasni morebitne dvome.

- Udeleženec prejme kartico s tremi izjavami in mora odločiti, katera je prevara. Nato se udeleženec predstavi in po navedbi svojega imena prebere izjave in pove, katera se mu zdi prevara. Vsi ostali poslušajo in pokažejo, ali se strinjajo ali ne. Če se nekdo ne strinja, vstane in pojasni, katera izjava se mu zdi prava prevara. Na koncu vodja vpraša udeležence, ali je kdor koli kdaj naletel na katero od teh prevar ali slišal zanje.

Material

- Natisnjen ali digitalni seznam izjav (2 resnični + 1 prevara) – Priloga 1, 2
- Pero in papir (neobvezno, za zapisovanje ali skupinsko ugibanje)
- Tabla ali zaslon (neobvezno, za prikazovanje odgovorov in pojasnil)

3. Srečanje

Predavanje 1: Prepoznavanje prevar
Trajanje *30 min*

Cilji učenja

- Udeležencem pomagajte razumeti ključne mehanizme prevar, kakšne so zvijače in cilji prevarantov.

Vsebina/metoda

- Izobraževalec s pomočjo diapozitivov predstavi najpogostejše prevare, ki so usmerjene v starejše odrasle, in pojasni cilje in mehanizme teh prevar. Na koncu izobraževalec udeležence vpraša, kateri mehanizem jih najbolj plaši.

Material

- Slike za predstavitev, ki prikazujejo različne možne spletne prevare, usmerjene v starejše odrasle.
- Projektor in prenosni računalnik za predstavitev.
- Letaki, ki povzemajo različne mehanizme prevar, trike, ki se uporabljajo za doseganje teh ciljev – Priloga 3.

Dejavnost 1: Prepoznavanje sumljive vsebine
Trajanje *15 min*

Cilji učenja

- Seznaniti udeležence z opozorilnimi znaki v e-pošti, SMS-sporočilih, spletnih straneh in oglasih.

Vsebina/metoda

- Udeležencem bodo prikazani resnični posnetki zaslona dejanskih SMS-sporočil, e-poštnih sporočil, spletnih strani in nevarnih pojavnih oken. Prosili jih bodo, naj prepoznajo neskladja in določijo, kateri primeri so legitimni in kateri so prevare. Po vsaki odločitvi sledi pojasnilo, zakaj je nekaj prevara in zakaj nekaj ni.

- Izobraževalec prikaže slike dveh posnetkov zaslona drugega ob drugem in prosi skupino, naj ugotovi razlike med prevaro in legitimnim primerom ter določi, kateri je prevara. Izobraževalec nadaljuje na enak način z vsemi primeri, pri čemer ohranja lahkotni in zanimiv ton, da ohrani pozornost in sodelovanje skupine. Izobraževalec pojasni vsak par primerov, potem ko udeleženci delijo svoje misli. Vprašajte jih, kateri primer je bil najtežje prepoznati kot prevaro. Nato izobraževalec razdeli gradivo.

Material

- Prezentacijske diapozitive z vizualnimi primeri pravih in lažnih posnetkov zaslona SMS-sporočil, e-poštnih sporočil, spletnih strani in pojavnih oken.
- Projektor in prenosni računalnik za predstavitev.
- Delovni listi, na katere udeleženci vpišejo odgovore ali napišejo opombe.
- Delovni listi s smernicami za prepoznavanje lažnih primerov med resničnimi – Priloga 4.

Odmor | Trajanje *5 min*

- **Udeležencem omogočite čas za počitek in razmislek.**
- **Kratek odmor za osvežitev.**

4·seja

Predavanje 2: Razumevanje manipulacije
Trajanje *30 min*

Cilji učenja

- Udeležencem pomagati razumeti socialni inženiring.

Vsebina/metoda

- Udeležence seznanite s socialnim inženiringom – pregled najpogostejših taktik, razlogov, zakaj goljufi ciljajo na starejše, in kako se zaščititi pred tovrstnimi goljufijami. Opredelite situacijo tako, da bo vsak, ki se znajde v socialni inženiring goljufiji, ostal miren in zbran ter se ne bo podlegel pritisku.
- Izobraževalec predstavi primere lažnih e-poštnih in SMS-sporočil, ki vzbujajo strah in tesnobo, nato pa pogosto predlagajo enostavno in hitro rešitev – na primer, da kliknete na povezavo in vnesete svoje bančne podatke ali osebne informacije ali celo sledite vrsti ukazov, da lahko »oni« rešijo problem za vas. Izobraževalec vpraša udeležence, kaj bi storili v primeru napada socialnega inženiringa. Izobraževalec razdeli tiskano gradivo z dodatnimi informacijami o taktikah socialnega inženiringa in kako jih prepoznati.

Gradivo

- Predstavitvene diapozitive, ki pojasnjujejo socialni inženiring.
- Projektor in prenosni računalnik za živo predstavitev nastavitev zasebnosti.
- Tiskano gradivo z opisom socialnega inženiringa in smernicami za opozorilne znake in preventivne ukrepe v primeru, da je nekdo tarča te vrste prevare – Priloga 5.

Dejavnost 2: Socialni inženiring v živo
Trajanje *20 min*

Cilji učenja

- Udeležencem omogočiti, da v varnem okolju izkusijo različne metode socialnega inženiringa.

Vsebina/metoda

- Udeležencem bodo predstavljeni različni scenariji, od katerih so nekateri oblika socialnega inženiringa, drugi pa ne. Scenariji socialnega inženiringa bodo usmerjeni v njihova čustva in vedenje.
- Vodja usposabljanja prosi udeležence, naj oblikujejo pet skupin po tri osebe. Vodja usposabljanja razdeli delovne liste in da navodila skupinam. Njihova naloga je ugotoviti, kateri scenariji so prevare in kateri so resnični, ter zapisati razloge za svoje sklepe. Ko skupine pregledajo vse scenarije in sprejmejo odločitve, vodja usposabljanja prosi, naj svoje ugotovitve delijo z ostalimi. Vodja usposabljanja vodi razpravo o scenarijih in udeležence vpraša, zakaj menijo, da so nekateri pristni, drugi pa prevare, kateri scenarij bi jim vzbudil največ strahu, če bi se znašli v njem, in zakaj.

Material

- Natisnjene delovne liste z različnimi scenariji.
- Delovni list, na katerem udeleženci označijo, kateri scenariji so prevara in kateri ne – Priloga 6.

Odmor | Trajanje *5 min*

- **Omogočite udeležencem, da si odpočijejo in se pripravijo na naslednjo sejo.**
- **Kratek odmor za osvežitev.**

5. del

Predavanje 3: Najpogostejše vrste prevar
Trajanje *30 min*

Cilji

- Osvežitev že omenjenih prevar, hiter pregled najpogostejših prevar, kot so smishing, vishing in phishing.
- Dopolnitev že pridobljenega znanja iz prejšnjih predavanj o zlonamerni programski opremi.

Vsebina/metoda

- Kratek pregled najpogostejših prevar. Phishing, smishing, vishing, lažne identitete in denarne prevare. Dodatno obveščanje udeležencev o zlonamerni programski opremi, kaj je in kako jo odkriti.
- Izobraževalec s pomočjo diapozitivov pojasni najpomembnejše informacije o najpogostejših prevarah in zlonamerni programski opremi. Nato razdelijo gradivo, ki jih opisuje, in o njem razpravljajo z udeleženci izobraževanja, da se prepričajo, da vsi čim bolje razumejo vsebino. Na koncu vprašajo udeležence, ali vedo, na kakšne znake morajo biti pozorni na internetu.

Gradivo

- Slike s predstavitvijo primerov phishinga, vishinga in smishinga.
- Projektor in prenosni računalnik za prikazovanje primerov najpogostejših prevar.
- Tiskane brošure, ki podrobno opisujejo najpogostejše prevare in zlonamerno programsko opremo, kaj je to, kako lahko škodi žrtvi in kako jo prepoznati – Priloga 7.

Dejavnost 3: Prepoznaj zlonamerno programsko opremo
Trajanje *20 min*

Cilji učenja

- Razviti sposobnost prepoznavanja različnih vrst zlonamerne programske opreme.

Vsebina/metoda

- Skupinska dejavnost, v kateri udeleženci prek delovnih listov prepoznajo in razpravljajo o različnih vrstah zlonamerne programske opreme.
- Izobraževalec pojasni, da bodo udeleženci v skupinah po trije preverili svoje znanje o zlonamerni programski opremi. Izobraževalec razdeli scenarije in udeležence prosi, naj jih preberejo. Naloga udeležencev je ugotoviti, kakšna vrsta programske opreme je bila uporabljena (trojanski konj, virus, adware, ransomware ali spyware), in odgovoriti na vprašanja pod vsakim scenarijem. Vsaka skupina svoje odgovore predstavi drugim skupinam. Izobraževalec nato razdeli liste z odgovori in udeležence prosi, naj pregledajo odgovore in analizirajo ključne vidike prepoznavanja uporabljene programske opreme ter načine zaščite pred takšnim napadom. Na koncu izobraževalec vpraša, katero vrsto programske opreme udeleženci štejejo za najbolj in najmanj škodljivo.

Gradivo

- Letaki z opisi zlonamerne programske opreme.
- Delovni listi, na katere udeleženci napišejo, za kakšno programsko opremo gre v danem primeru, kaj ta naredi z napravo in kakšni so preventivni ukrepi za dani primer.
- Delovni list za udeležence – Prepoznaj zlonamerno programsko opremo – Priloga 8

Odmor | Trajanje 5’

- **Čas za počitek in pripravo.**
- **Kratek odmor za osvežitev.**

6. seja

Predavanje 4: Osnovna zaščita podatkov in varnostno kopiranje podatkov
Trajanje *30 min*

Cilji

- Udeleženci bodo znali opredeliti osebne podatke in podatke, ki so dragoceni za prevarante. Zavedali se bodo tudi pomembnosti varnostnega kopiranja podatkov.

Vsebina/metoda

- Predstavitev z razlago osebnih podatkov. Udeleženci bodo seznanjeni s temami, kje je varno deliti podatke in kje ne, obveščeni bodo o pomembnosti prepoznavanja podatkov, ki se lahko uporabijo proti njim. Udeleženci bodo obveščeni tudi o tem, katere podatke je treba varnostno kopirati in zakaj.
- Izobraževalec razdelil natisnjene materiale in udeležence popeljal skozi vsebino s pomočjo diapozitivov, pri čemer je pojasnil: kategorije osebnih podatkov, kateri podatki so lahko škodljivi v napačnih rokah in zakaj, kje lahko delimo osebne podatke na spletu, česa nikoli ne smemo deliti na spletu, kaj je varnostno kopiranje, kako vas varnostne kopije lahko zaščitijo pred napadi zlonamerne programske opreme, najboljše prakse za varno varnostno kopiranje in nasvete za varovanje vaših podatkov.
- Izobraževalec spodbuja razpravo in udeležence vpraša, ali so kdaj bili priča poskusu kibernetskega napada z uporabo programske opreme ali sodelovali v takšnem napadu. Na koncu izobraževalec vpraša, ali bodo odslej izdelovali varnostne kopije pomembnih podatkov.

Gradivo

- Predstavitev o osebnih podatkih, kje in kaj lahko delimo na spletu, skupaj z informacijami o varnostnem kopiranju podatkov.
- Gradivo s smernicami o osebnih podatkih, kje jih deliti, kje ne in zakaj je pomembno, da se pomembne informacije varnostno kopirajo – Priloga 9.

Dejavnost 4: Varnostno kopiranje datotek v oblak in zunanji pomnilnik. Trajanje *20 min*

Cilji

- To znanje bo udeležencem pomagalo varno varnostno kopirati datoteke z uporabo preverjenih storitev v oblaku in zunanjih trdih diskov.

Vsebina/metoda

- Udeleženci bodo varnostno kopirali lažne datoteke v oblak, ki jim je znan (Google Drive, Dropbox, iCloud, OneDrive). Enake lažne datoteke bodo varnostno kopirali tudi na USB-ključ.
- Izobraževalec razdeli gradivo z informacijami o varnostnem kopiranju datotek na zunanji disk in v storitev v oblaku. Izobraževalec prikazuje na zaslonu ali projektorju, udeleženci pa sledijo postopku kopiranja datotek z računalnika na zunanji disk in nalaganja datotek v storitev v oblaku. Izobraževalec pomaga tistim, ki potrebujejo pomoč. Vprašanje za razmislek na koncu: »Misliš, da lahko sam varnostno kopiraš svoje datoteke, ali kdo potrebuje dodatne informacije?«, »Ali bi rad kaj vprašal ali podal svoje mnenje o današnji temi spletnih prevar?«

Material

- Lažne datoteke, da se lahko naredi varnostna kopija.
- Računalniki in USB-ključi.
- Prenosni računalnik in projektor, da lahko učitelj pokaže primer postopka.

- Letaki z navodili za varnostno kopiranje datotek na zunanji pogon in v oblak – navodila, prilagojena vsem večjim ponudnikom storitev v oblaku – Kako varnostno kopirati datoteke – Priloga 10

7·seja

Razprava | Trajanje *10* min

Cilji učenja

- Spodbujati proaktivno miselnost, polno zavesti v zvezi z spletnimi prevari.
- Povzemite usposabljanje in se prepričajte, da udeleženci razumejo, kako se zaščititi pred spletnimi prevari.

Vsebina/metoda

- Pregled ključnih točk najpogostejših spletnih prevar. Ozaveščanje, da je treba biti vedno pozoren na morebitne prevare, če je nekaj sporočeno na izredno nujen način.
- Skupinska razprava o tem, kako ravnati v situaciji, ko se znajdemo v spletni prevari. Kateri so ključni znaki sumljivih dejavnosti, s katerimi se lahko srečamo, in kaj storiti v takšnih primerih.
- Izobraževalec povzame najpomembnejše informacije o tem, kaj storiti, če postanete žrtev spletne prevare, in navede ključne znake sumljivih dejavnosti. Izobraževalec se zahvali udeležencem in jim zagotovi podporno gradivo, nato pa razdeli kontrolni seznam o tem, kako prepoznati spletno prevaro in kaj storiti v takšnem primeru. Izobraževalec udeležencem zastavi odprta vprašanja: „Kaj je najpomembnejše, kar ste se danes naučili o spletni prevari in kako se pred njo zaščititi?“ „Ali se zdaj počutite bolj samozavestni pri prepoznavanju in izogibanju prevaram?“ „Ali je kakšna tema ali vprašanje iz današnje seje, o kateri bi želeli več informacij?“

Material

- Tabla in flomasterji za brainstorming o načinih prepoznavanja prevar.
- Gradivo: kontrolni seznam v zvezi z spletnimi prevarami – Priloga 11.
  Delovni listi Seznam za preverjanje varnosti na spletu.

Zaključek
Trajanje 5

Cilji

- Povzemite vsebino seje in udeležence spodbudite, naj še naprej ravnajo varno.

Vsebina/metoda

- Končni povzetek ključnih točk, zagotovite dodatne vire za nadaljnje učenje.

Material

- Gradivo s ključnimi točkami in viri.

3.4 Dodatne informacije

3.4.1 Samorefleksija izobraževalcev

- Ali sem učinkovito posredoval pomembnost nevarnosti na spletu?
- Ali sem zagotovil, da so udeleženci razumeli preventivne ukrepe?
- Kako sem udeležence vključil v dejavnosti in razprave?
- So bili viri in materiali koristni za udeležence?

3.4.2 Ocena programa s strani izobraževalcev

- Ali je vsebina usposabljanja ustrezna in jasna za starejše?
- So bile dejavnosti in razprave učinkovite pri pomoči udeležencem pri učenju snovi?
- Ali so rezultati v skladu z učnimi cilji modula?

3.4.3 Gradivo, dodatni viri

Priloga 1 | Dve resnici in ena prevara

Skupina 1

Prevaranti se pogosto izdajajo za osebe, ki jim zaupate.

Legitimna podjetja vam nikoli ne bodo poslala e-pošte.

Lažna e-poštna sporočila pogosto ustvarjajo občutek

Skupina 2

Nikoli ne smete nikomur razkriti svoje bančne PIN-kode.

Vse spletne strani, ki se začnejo z „https“, so 100 % varne.

Prevaranti lahko uporabijo uradno izgledajoče logotipe, da

Skupina 3

Izsiljevalska programska oprema lahko blokira dostop do vašega

S klikom na neznana pojavna okna lahko namestite

Vse priloge od prijateljev je varno odpreti brez preverjanja.

Skupina 4

Socialni inženiring pogosto vključuje čustveno manipulacijo.

Vladne agencije vas vedno najprej kontaktirajo po telefonu.

Starejši ljudje so pogosto tarča zaradi domnevne ranljivosti.

Skupina 5

Enako geslo lahko brez težav uporabljate za več računov.

Močno geslo vsebuje črke, številke in simbole.

Uporaba dvofaktorskega preverjanja pristnosti zagotavlja

Skupina 6

Prevaranti lahko ponaredijo identifikacijsko številko klicatelja,

V spletnih nagradnih igrah je varno navesti svoj polni naslov.

Vedno bodite previdni pri nezaželenih ponudbah.

Skupina 7

Smishing je prevara, ki se pošilja prek kratkih sporočil.

Zlonamerna programska oprema vpliva samo na stare računalnike.

Protivirusna programska oprema pomaga zaščititi pred

Nastavite 8

Prevaranti se lahko izdajajo za tehnično podporo.

Kliknite na neznane povezave, da preverite, ali delujejo.

Vedno preverite URL-je, preden vnesete osebne podatke.

Skupina 9

Lažne ponudbe za delo se lahko uporabijo za krajo vaših osebnih

Prevare se dogajajo le ljudem, ki niso tehnološko podkovani.

Spletni oglasi lahko včasih vodijo do spletnih strani, ki so

Skupina 10

Nekatere prevare zahtevajo plačilo z darilnimi karticami.

Aplikacije je varno prenesti iz zaupanja vrednih trgovin z

Svoje podatke za prijavo morate deliti s prijatelji.

Skupina 11

Prevaranti včasih uporabljajo strah, da vas prisilijo.

Vsako pojavno opozorilo je resnično opozorilo o virusu.

Pomembno je, da preverite sporočila, preden ukrepate.

Skupina 12

Legitimna podjetja ne zahtevajo osebnih podatkov prek e-pošte.

Javni Wi-Fi je vedno varen in zanesljiv za uporabo.

Posodobitev naprave pomaga odpraviti varnostne ranljivosti.

Skupina 13

Prevare se lahko pojavijo na platformah družbenih medijev.

Klik na »odjava« v lažnem e-sporočilu je neškodljiv.

Sumljivo dejavnost morate prijaviti platformi.

Skupina 14

Svoje potovalne načrte lahko brez skrbi objavite na spletu.

Prevaranti lahko spremljajo vaše objave na družbenih omrežjih.

Bodite previdni pri sprejemanju prijateljskih zahtev od

Skupina 15

Varnostne kopije zaščitijo vaše podatke v primeru napadov.

Spomine na posodobitve programske opreme morate

Za vsak račun uporabljajte močna, edinstvena gesla.

Dodatek 2 | Pravilni odgovori

Skupina 1

- Resnično – Prevaranti se pogosto izdajajo za osebe, ki jim zaupate.
- Napačno – legitimna podjetja vam nikoli ne bodo poslala e-pošte. (To je mit. Legitimna podjetja lahko uporabnike kontaktirajo prek e-pošte, vendar ne zahtevajo občutljivih osebnih ali finančnih podatkov.
- Resnično – Lažna e-poštna sporočila pogosto ustvarjajo občutek nujnosti.

Skupina 2

- Resnično – Nikoli ne smete nikomur razkriti svoje bančne PIN-kode.
- Napačno – Vse spletne strani, ki se začnejo z »https«, so popolnoma varne. (To je mit. »https« označuje šifriranje, ne legitimnost.)
- Resnično – Prevaranti lahko uporabijo uradno izgledajoče logotipe, da zavedejo uporabnike.

Skupina 3

- Res – Ransomware lahko uporabnikom onemogoči dostop do njihovih računalnikov.
- Res – S klikom na neznana pojavna okna lahko namestite zlonamerno programsko opremo.
- Napačno – Vse priloge od prijateljev je varno odpreti brez preverjanja. (To je mit. Priloge od zaupanja vrednih stikov so lahko prav tako okužene.)

Skupina 4

- Res – Socialni inženiring pogosto temelji na čustveni manipulaciji.
- Neresnično – Vladne agencije vedno najprej pokličejo posameznike po telefonu. (To je mit. Uradna komunikacija pogosto poteka po pošti.)
- Res – Starejši ljudje so pogosto tarča zaradi domnevne ranljivosti.

Skupina 5

- Napačno – Sprejateljivo je ponovno uporabiti isto geslo za več računov. (To je mit. Ponovna uporaba gesla poveča varnostna tveganja.)
- Res – Močna gesla vključujejo kombinacijo črk, številk in simbolov.
- Resnično – Dvostopenjska avtentikacija zagotavlja dodatno raven varnosti.

Skupina 6

- Resnično – Prevaranti lahko ponaredijo podatke o identiteti klicatelja.
- Napačno – V spletnih nagradnih igrah je varno navesti svoj polni naslov. (To je mit. Osebni podatki se lahko zlorabijo za prevare.)
- Res je – Nezaželene ponudbe je treba vedno obravnavati previdno.

Skupina 7

- Res – Smishing se nanaša na prevare, poslane prek kratkih sporočil.
- Napačno – Zlonamerna programska oprema prizadene samo stare računalnike. (To je mit. Prizadeti so lahko vsi naprave.)
- Res – Protivirusna programska oprema pomaga zaščititi pred zlonamernimi grožnjami.

Skupina 8

- Res – Prevaranti se lahko izdajajo za službe tehnične podpore.
- Napačno – Neznane povezave je treba klikniti, da se preveri, ali so legitimne. (To je mit. Klik na neznane povezave je lahko nevaren.)
- Resnično – Pred vnosom osebnih podatkov je treba vedno preveriti URL-je.

Skupina 9

- Res – Lažne ponudbe za delo se lahko uporabijo za krajo osebnih podatkov.
- Napačno – Prevare so usmerjene le v ljudi z nizkimi digitalnimi znanji. (To je mit. Prevara lahko doleti vsakogar.)
- Resnično – Spletne oglase lahko včasih preusmerijo uporabnike na spletne strani z goljufijami.

Skupina 10

- Resnično – Nekatere prevare zahtevajo plačilo v obliki darilnih kartic.
- Res – Prenos aplikacij iz zaupanja vrednih trgovin z aplikacijami je na splošno varnejši.
- Napačno – Podatke za prijavo je treba deliti s prijatelji. (To je mit. Podatkov za prijavo nikoli ne smete deliti.)

Skupina 11

- Res – Prevaranti pogosto uporabljajo strah, da pritiskajo na žrtve.
- Neresnično – Vsako pojavno opozorilo kaže na resnično grožnjo virusa. (To je mit. Mnoga opozorila so lažna.)
- Res – Sporočila je treba vedno preveriti, preden ukrepate.

Skupina 12

- Resnično – legitimna podjetja ne zahtevajo osebnih podatkov prek e-pošte.
- Napačno – Javna omrežja Wi-Fi so vedno varna. (To je mit. Javna omrežja lahko izpostavijo osebne podatke.)
- Resnično – Redne posodobitve programske opreme pomagajo odpraviti varnostne ranljivosti.

Skupina 13

- Resnično – Prevare se lahko pojavijo na platformah družbenih medijev.
- Napačno – Klik na »odjava« v lažnih e-poštnih sporočilih je neškodljiv. (To je mit. Lahko potrdi, da je uporabnik aktiven cilj.)
- Resnično – Sumljive dejavnosti je treba prijaviti ustrezni platformi.

Skupina 14

- Napačno – Na spletu je varno javno deliti potovalne načrte. (To je mit. Takšne informacije lahko izkoristijo goljufi.)
- Res – Prevaranti lahko spremljajo dejavnosti na družbenih omrežjih.
- Resnično – Prošnje za prijateljstvo od neznanih oseb je treba obravnavati previdno.

Skupina 15

- Resnično – Varnostne kopije podatkov ščitijo informacije v primeru kibernetskih napadov.
- Napačno – Opomnike za posodobitev programske opreme je treba ignorirati. (To je mit. Posodobitve so ključnega pomena za varnost.)
- Res – Za vsak račun je treba uporabljati močna in edinstvena gesla.

Priloga 3 | Mehanizmi, ki se uporabljajo v spletnih prevarah, usmerjenih v starejše

1. Phishing (prevare po e-pošti)

Starejši prejmejo e-poštna sporočila, ki izgledajo, kot da prihajajo iz zaupanja vrednih virov (banke, zdravstvene službe itd.).

Trik: lažne povezave ali strani za prijavo

Cilj: Kraja osebnih ali finančnih podatkov

2. Smishing (prevare prek SMS-sporočil)

Prevaranti pošiljajo SMS-sporočila z lažnimi obvestili o dostavi, obvestili o nagradah ali opozorili.

Trik: nujen jezik + povezava do zlonamerne spletne strani

Cilj: namestitev zlonamerne programske opreme ali zbiranje zasebnih podatkov

3. Vishing (prevare s telefonskimi klici)

Telefonski klici od goljufov, ki se izdajajo za predstavnike banke, tehnične podpore ali vlade.

Trik: lažna identiteta klicatelja + čustveni pritisk

Cilj: pridobiti bančne podatke ali oddaljeni dostop

4. Lažne spletne strani (spoofing)

Starejše osebe so preusmerjene na lažne spletne strani, ki izgledajo kot prave (banke, trgovine, medicinski portali).

Trik: rahlo spremenjeni URL-ji (npr. paypa1.com)

Cilj: pridobiti podatke za prijavo ali plačilo

5. Prevare tehnične podpore (prevare po e-pošti)

Pojavna okna ali klici opozarjajo na „virus“ ali težave z računalnikom in starejše osebe pozivajo, naj poiščejo pomoč.

Trik: lažna sporočila o napakah + zahteve za oddaljeni dostop

Cilj: Nadzor nad napravo ali kraja podatkov kreditne kartice

6. Romantične prevare

Na družbenih omrežjih ali spletnih straneh za zmenke goljufi ustvarjajo čustvene vezi, da bi manipulirali žrtve.

Trik: Lažne fotografije, zgodbe in naklonjenost

Cilj: Prepričati starejše, da pošljejo denar

7. Investicijske ali loterijske prevare

Obljube velikih donosov ali sporočila „zmagali ste“, ki zahtevajo predplačilo.

Trik: Lažni dokumenti, nujnost ali uradno zveneča imena

Cilj: Pridobiti elektronske prenose, kriptovalute ali darilne kartice

Priloga 4 | Prepoznajte prevaro: Hitri vodnik

Uporabite ta kontrolni seznam, da se odločite, ali je sporočilo, e-pošta, spletna stran ali oglas resničen ali lažen.

1. Preverite pošiljatelja ali vir

- *E-poštni naslov/telefonska številka: Ali so podatki pošiljatelja sumljivi ali neznani?*

✗ ***Lažno:*** *support@paypal-secure123.com*
✔ ***Resnično:*** *support@paypal.com*

- *Nepravilno napisana imena blagovnih znamk ali čudne URL-je:*

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

2. Bodite pozorni na nujnost ali pritisk

- Ali vas sporočilo poskuša prestrašiti ali prisiliti v hitro odločitev?

  „Ukrepajte zdaj, sicer bo vaš račun blokiran!“
  „Zadnje opozorilo pred pravnimi ukrepi!“

Prave družbe vas ne grozijo ali pritiskajo na tak način.

3. Preverite jezik in ton

- Poiščite pravopisne in slovnične napake
- Je ton preveč neformalno ali preveč agresiven?
- Ali zveni nenaravno ali prevedeno?

  ✗ **Lažno:** »Dragi stranka, vaš račun je bil nujno blokiran, prosimo, ukrepajte takoj.«
  ✔ **Resnično:** „Opazili smo nenavadno aktivnost na vašem računu. Prosimo, da ga pregledate.“

4. Preverite povezavo, preden kliknete

- Premaknite miško nad povezave, da vidite, kam dejansko vodijo
- Ali se URL ujema z resnično spletno stranjo podjetja?

  ✗ **Lažno:** http://paypal.verify-now-support.com
  ✔ **Resnično:** https://www.paypal.com

5. Bodite pozorni na zahteve po osebnih podatkih

Prava podjetja nikoli ne zahtevajo:

- gesla
- PIN-kod
- številk bančnih računov ali kartic
- številk socialnega zavarovanja

✗ „Prosimo, pošljite svoje podatke za prijavo, da potrdimo vaš račun.“

✔ „Nikoli ne bomo po e-pošti zahtevali vašega gesla.“

6. Pogledajte logotipe in obliko

- So logotipi zamegljeni, raztegnjeni ali barvno spremenjeni?
- Je postavitev nenavadna ali neenotna?

Prave družbe uporabljajo čisto, profesionalno in dosledno oblikovanje.

7. Preveč dobro, da bi bilo res? Verjetno je.

„Osvojili ste nov iPhone!“

„Izbrani ste bili za darilno kartico v vrednosti 1000 dolarjev!“

Prave nagrade ne zahtevajo vnaprejšnjega plačila ali občutljivih podatkov.

✔ **Resnično ali ✗ Lažno?**

Vprašajte se:

- **Ali zaupam viru?**
- **Ali me silijo ali prestrašujejo, da ukrepam?**
- **Ali se mi kaj zdi nenavadno ali neobičajno?**

Če ste v dvomih, ne klikajte, ne odgovarjajte in prijavite to!

Priloga 5 | Prevare s socialnim inženiringom – kaj morate vedeti

Kaj je socialni inženiring?

Socialni inženiring je, ko goljufi uporabijo manipulacijo, pritisk in čustva, da vas prevarajo in pridobijo vaše osebne podatke, denar ali dostop do vaših računov.

Nevarnosti socialnega inženiringa

Prevaranti se lahko izdajajo za zaupanja vredne vire, kot so:

- banke (npr. »Vaš račun je bil blokiran!«)
- Kurirske službe (npr. »Zamudili ste paket. Plačajte zdaj!«)
- Vladne agencije (npr. »Imate neplačane davke.«)
- Policija ali Ministrstvo za pravosodje (npr. »Proti vam teče preiskava.«)
- Tehnična podpora (npr. »Na vašem računalniku smo odkrili virus.«)
- Družina ali prijatelji (npr. »Sem v težavah, prosim, pošlji mi denar!«)

Pogosto ustvarjajo občutek nujnosti ali strahu, da bi vas prisilili v hitro ukrepanje brez razmišljanja.

Opozorilni znaki, na katere morate biti pozorni

- Povedo vam, da morate ukrepati **takoj**, sicer boste nosili posledice
- Od vas zahtevajo **osebne podatke**, gesla ali bančne podatke
- Od vas zahtevajo **plačilo z darilnimi karticami**, **kriptovalutami ali bančnimi nakazili**
- Sporočila imajo **čudno slovnico ali črkovanje.**
- Nenadoma vas kontaktira nekdo, ki ga ne poznate

Preventivni ukrepi

Vedno storite naslednje:

1. Ostanite mirni. Vzemite si trenutek za dihanje in se ne prenaglite.
2. Nikoli ne posredujte osebnih podatkov po telefonu, e-pošti ali SMS-sporočilu.
3. Če se vam zdi sumljivo, odložite slušalko ali izbrišite sporočilo.
4. Zahtevo preverite sami:

Če nekdo trdi, da je iz banke, dostavne službe, vladne službe ali tehnične podpore, se vedno obrnite neposredno na organizacijo.
Uporabite njihovo uradno spletno stran ali telefonsko številko, ne tisto, ki je navedena v sporočilu ali e-pošti.

Primer:

- **Pokličite svojo banko na številko, ki je navedena na vaši bančni kartici ali uradni spletni strani.**
- **Obiščite uradno spletno stran vlade, če niste prepričani o sporočilih, povezanih z davki.**
- **Obrnite se na uradno podporo kurirskega podjetja, da preverite, ali je paket resničen.**

Ne pozabite:

- **Prave družbe vas ne grozijo in ne pritiskajo**
- **Prave institucije vas nikoli ne bodo prosile za gesla ali PIN-kode**
- **Prava sporočila so profesionalna in spoštljiva.**
- **Prevare temeljijo na strahu, zmedi in hitrosti.**

Če se vam nekaj zdi „nenavadno“, se ustavite in vprašajte nekoga, ki mu zaupate. Vedno je bolje dvakrat preveriti, kot pa pasti v past.

Priloga 6 | Scenariji: Prepoznajte prevaro

Scenarij 1: Nujno sporočilo banke

Prejmete e-poštno sporočilo, ki izgleda, kot da je poslala vaša banka. Naslov sporočila je: „NUJNO: Težava z dostopom do računa“. V sporočilu je navedeno, da je na vašem računu prišlo do sumljive aktivnosti in da morate nemudoma preveriti svoje osebne in bančne podatke. V sporočilu je navedena povezava in opozorilo, da bo vaš račun trajno blokiran, če ne odgovorite v 24 urah.

Scenarij 2: Opozorilo o polnem pomnilniku telefona

Med brskanjem po internetu ali uporabo aplikacije se prikaže pojavno sporočilo: »Opozorilo! Pomnilnik vašega telefona je poln. Tapnite tukaj, da očistite napravo in preprečite izgubo podatkov.« Sporočilo deluje nujno, posnema slog sistema vašega telefona, ko pa ga tapnete, vas preusmeri na prenos aplikacije tretje osebe, ki obljublja optimizacijo vaše naprave.

Scenarij 3: Klic tehnične podpore

Prejmete klic od osebe, ki trdi, da je tehnik Microsoft. Pove vam, da je vaš računalnik okužen z nevarnim virusom in pošilja sporočila o napakah. Ponudi vam, da ga popravi na daljavo in vas vodi skozi postopek prenosa programske opreme, da bi dobil dostop do vašega računalnika. Ko se poveže, »pregleda« vaš računalnik in nato zahteva plačilo za odstranitev virusa, pogosto pa prosi za vaše podatke o kreditni kartici ali dostop do spletnega bančništva.

Scenarij 4: Prevara s plačilom računa za komunalne storitve

Prejmete e-pošto ali SMS-sporočilo, ki izgleda, kot da je poslano od vašega dobavitelja električne energije. V njem je navedeno, da je vaše zadnje plačilo ni bilo uspešno in da bo vaša električna energija odklopljena, če ne boste poravnali neporavnanega zneska v 12 urah. Sporočilo vsebuje povezavo do strani za plačilo, ki je zelo podobna pravi spletni strani dobavitelja, vendar zahteva vaše kreditne kartice in osebne podatke.

Scenarij 5: Obvestilo o bančni transakciji

Prejmete e-poštno sporočilo od svoje banke z naslovom: »Potrditev transakcije – 74,60 € pri MERKUR«. Sporočilo potrjuje transakcijo, opravljeno danes ob 13:45. Če ne prepoznate zneska, vas sporočilo napoti, da pokličete oddelek banke za preprečevanje goljufij na uradno številko, navedeno na njihovi spletni strani. E-poštno sporočilo ne vsebuje klikljivih povezav in je napisano v mirnem in profesionalnem tonu.

Scenarij 6: Opozorilo o prostem prostoru v Googlu

Prejmete e-poštno sporočilo od Googla z naslednjim besedilom: »Vaš Google račun je zapolnjen 98 %. Trenutno uporabljate 14,8 GB od 15 GB prostora za shranjevanje. Da boste lahko še naprej prejemali e-poštna sporočila in uporabljali Google Drive, upravljajte s svojim prostorom za shranjevanje ali ga nadgradite.« Sporočilo vsebuje dva gumba: enega za upravljanje prostora za shranjevanje in drugega za nadgradnjo, oba pa vodita na uradne spletne strani Googla.

Priloga 7 | Pogoste spletne prevare in kako se pred njimi zaščititi

1. Smishing (SMS phishing)

Prejmete kratko sporočilo, ki izgleda, kot da prihaja od vaše banke, dostavne službe ali vladne institucije. V njem je lahko navedeno, da je prišlo do težave z vašim računom ali paketom, in vključuje povezavo.

Smishing: Phishing prek kratkih sporočil, ki pogosto vsebujejo nujna sporočila, ki vas zavedejo, da kliknete na povezavo ali posredujete osebne podatke.

Rdeče zastave:

- Nujni jezik („vaš račun bo zaprt“)
- Sumljive povezave
- Zahtevanje osebnih ali bančnih podatkov

Kaj storiti:

- Nikoli ne klikajte na povezave iz neznanih številk.
- Neposredno se obrnite na podjetje prek uradne telefonske številke ali spletne strani.
- Blokirajte in prijavite pošiljatelja.

2. Vishing (glasovno phishing)

Prejmete telefonski klic od nekoga, ki se izdaja za predstavnika vaše banke, policije ali tehnične podpore. Zahteva osebne podatke ali trdi, da je prišlo do sumljive dejavnosti.

Vishing: glasovno phishing, pri katerem se prevaranti po telefonu izdajajo za legitimne subjekte, da bi ukradli podatke.

Različica: lažni glas z uporabo umetne inteligence

Prevaranti lahko zdaj z umetno inteligenco posnemajo glas ljubljene osebe. Pokličejo lahko in se izdajo za vašega vnuka ali otroka ter prosijo za nujno pomoč ali denar.

Opozorilni znaki:

- Klicatelj vas pritiska, da ukrepate hitro
- Čustvena manipulacija („Sem v težavah!“)
- Prosi za denar ali informacije

Kaj storiti:

- Odložite slušalko in pokličite osebo nazaj neposredno na znano številko.
- Pokličite drugega družinskega člana, da preveri zgodbo.
- Nikoli ne dajte osebnih ali bančnih podatkov po telefonu.

3. Phishing (goljufija prek e-pošte)

Prejmete e-pošto, ki izgleda uradno (od vaše banke, PayPala, davčnega urada itd.), v kateri vas prosijo, da potrdite podatke, ponastavite geslo ali kliknete povezavo.

Phishing: lažna e-poštna sporočila ali SMS-sporočila, ki vas zavedejo, da razkrijete zaupne podatke (kot so gesla ali bančne podatke).

Opozorilni znaki:

- E-pošta vsebuje slovnične napake
- Uporablja strah („zaznano nepooblaščeno prijavo“)
- Zahteva osebne podatke

Kaj storiti:
- Ne klikajte na sumljive povezave.
- Pazljivo preverite e-poštni naslov pošiljatelja.
- Stopite v stik s podjetjem prek njihove uradne spletne strani.

4. Finančna goljufija
Prevaranti se izdajajo za investicijske svetovalce, lažne dobrodelne organizacije ali celo romantične partnerje. Najprej vzpostavijo zaupanje, nato pa prosijo za denar, donacije ali pomoč.

Finančne prevare: goljufi prosijo za denar pod lažnimi pretvezami, pogosto obljubljajo nagrade ali grozijo s posledicami.

Opozorilni znaki:
- Preveč dobri donosi naložb, da bi bili resnični
- Čustvena manipulacija
- Neoverljive dobrodelne organizacije ali namene

Kaj storiti:
- Nikoli ne pošiljajte denarja osebam, ki jih niste osebno spoznali.
- Vedno preverite podjetje ali osebo.
- Pred sprejetjem finančnih odločitev se posvetujte z zaupanja vrednim družinskim članom ali svetovalcem.

5. Lažne identitete in prevzemanje identitete
Prevaranti se lahko izdajajo za nekoga, ki niso – na primer za vladnega uradnika, bančnega uslužbenca ali celo družinskega člana. Uporabljajo lažne dokumente, e-pošto ali glasove, ustvarjene z umetno inteligenco, da ljudi zvabijo v razkritje občutljivih podatkov ali pošiljanje denarja.

Lažne identitete: Prevaranti ustvarijo lažne spletne profile, da vzpostavijo zaupanje in manipulirajo žrtve, da jim izročijo denar ali osebne podatke.

Opozorilni znaki:
- Nenadna zahteva po osebnih podatkih ali denarju
- Občutek nujnosti ali čustvenega pritiska
- Stik prek neuradnih ali sumljivih kanalov

Kaj storiti:
- Vedno preverite identiteto tako, da pokličete pravo osebo ali institucijo prek uradnih kontaktnih podatkov.
- Ne bojte se prekiniti pogovor in najprej preveriti.
- Če ste v dvomih, prosite nekoga, ki mu zaupate, da vam pomaga oceniti situacijo.

6. Zlonamerna programska oprema ali malware
Je vsaka programska oprema, ki je zasnovana za poškodovanje računalnika ali krajo osebnih podatkov. Prevaranti pogosto zvabijo uporabnike, da jo prenesejo prek lažnih e-poštnih sporočil, povezav ali pojavnih oglasov. Ko je zlonamerna programska oprema enkrat nameščena, lahko krade gesla, zaklene datoteke in celo prevzame nadzor nad vašo napravo. Vedno bodite previdni pri neznanih povezavah ali prilogah in poskrbite, da ima vaš računalnik posodobljeno protivirusno programsko opremo, ki vas ščiti.

Priloga 8 | Gradivo za udeležence – Prepoznajte zlonamerno programsko opremo

Cilj

Seznanite se z najpogostejšimi vrstami zlonamerne programske opreme (virusi, trojanski konji, vohunska programska oprema, izsiljevalska programska oprema, oglaševalska programska oprema) s prebiranjem in analiziranjem teh realističnih scenarijev.
Za vsako prevaro zapišite, za kakšno prevaro gre (trojanski konj, virus, adware, izsiljevalska programska oprema, vohunska programska oprema) in odgovorite na vprašanje.

Scenarij 1

„Prejmete e-pošto od zaupanja vrednega prijatelja s prilogo z naslovom »Pomemben dokument«. Ko jo odprete, se vaš računalnik začne upočasnjevati in pojavijo se čudna pojavna okna.“

Vprašanje: Kakšna vrsta zlonamerne programske opreme je to po vašem mnenju? Kako bi se zaščitili?

Scenarij 2

„Med brskanjem se prikaže pojavno okno z napisom: »Vaša naprava je zastarela! Kliknite tukaj, da prenesete posodobitev.« Kliknete povezavo in nevede prenesete zlonamerno programsko opremo, ki je prikrita kot posodobitev.“

Vprašanje: V čem je nevarnost? Kaj bi morali storiti namesto tega?

Scenarij 3

»S neznane spletne strani prenesete brezplačno aplikacijo za urejanje fotografij. Sčasoma opazite, da se v vašem brskalniku pojavljajo oglasi in začnete prejemati neželena tržna e-poštna sporočila.«

Vprašanje: Kaj menite, da se je zgodilo? Kaj naj storite?

Scenarij 4

»Po kliku na povezavo v e-poštnem sporočilu z besedilom »Vaša naročnina na Netflix bo kmalu potekla, kliknite tukaj za potrditev plačila« se prikaže sporočilo, v katerem vas pozivajo, da plačate odkupnino za odklepanje datotek.«

Vprašanje: Kako lahko ugotovite, da gre za prevaro? Kaj naj storite, če se kaj takega zgodi?

Scenarij 5

„Po kliku na povezavo v e-poštnem sporočilu z besedilom »Vaša naročnina na Netflix se bo kmalu iztekla, kliknite tukaj za potrditev plačila« se prikaže sporočilo, v katerem vas pozivajo, da plačate odkupnino za odklepanje datotek.“

Vprašanje: Ali je to nevarna vrsta programske opreme? Kako se je lahko znebite?

Priloga 9 | Varstvo osebnih podatkov

1. Kaj so osebni podatki?

Osebni podatki so vse informacije, ki se lahko uporabijo za vašo neposredno ali posredno identifikacijo. To vključuje:

- **Osnovne podatke:** ime, priimek, datum rojstva, naslov
- **Kontaktne informacije:** e-poštni naslov, telefonska številka
- **Identifikacijske številke:** osebna številka, davčna številka, številka potnega lista
- **Finančne podatke:** številke bančnih računov, številke kreditnih kartic
- **Prijavni podatki:** uporabniška imena, gesla
- **Zdravstveni podatki:** zdravstvene kartoteke, recepti
- **Biometrični podatki:** prstni odtisi, prepoznavanje obraza, glas
- **Podatki o lokaciji:** sledenje GPS, IP-naslov
- **Osebne preference:** zgodovina iskanja, aktivnost na družbenih omrežjih

2. Kateri podatki so lahko škodljivi v napačnih rokah (in zakaj)?

Prevaranti in kiberkriminalci ciljajo na določene podatke, ki jih lahko uporabijo za:

- **Krajo vaše identitete**
- **Dostop do vaših bančnih računov**
- **izvršitev goljufije v vašem imenu**
- **manipuliranje z vami na čustveni ali finančni ravni**

Najbolj dragoceni podatki za goljufe:

- **Osebna identifikacijska številka (potni list itd.) –** uporablja se za krajo identitete ali odpiranje goljufivih računov.
- **Prijavni podatki –** omogočajo dostop do e-pošte, družbenih omrežij, spletnega bančništva.
- **Podatki o bančnih in kreditnih karticah –** uporabljajo se za nepooblaščene nakupe ali prenose sredstev.
- **Telefonske številke in e-poštni naslovi –** uporabljajo se za phishing, smishing, spam in prevare z lažno identiteto.
- **Vsebina družbenih omrežij –** uporabljena za ustvarjanje lažnih profilov ali manipulacijo z vami.

3. Kje lahko delimo svoje osebne podatke na spletu?

Pomembno je vedeti, kje in kdaj je varno deliti osebne podatke. Nekatere platforme so zanesljive, druge pa predstavljajo večje tveganje.

Mesta, kjer je na splošno varno deliti osebne podatke (z previdnostjo):

- Preverjene spletne trgovine (npr. Amazon, Zalando, Mimovrste): za nakupe, samo če ima spletna stran HTTPS šifriranje in varne načine plačila.
- Uradne vladne spletne strani (npr. IRS, portali socialne varnosti, portali e-uprave): za oddajo dokumentov, davkov, vlog.
- Ugledni ponudniki storitev (npr. vaša banka, ponudnik zdravstvenih storitev): samo prek njihovih uradnih spletnih strani ali aplikacij.
- Zaupanja vredni ponudniki e-pošte in storitev v oblaku (npr. Gmail, Outlook, Dropbox): Pri ustvarjanju računov, varnostnem kopiranju podatkov.

Pred predložitvijo kakršnih koli podatkov se vedno prepričajte, da je spletno mesto uradno, da ima HTTPS in da je dobro znano.

Krajev, kjer morate biti izredno previdni ali se izogibati deljenju osebnih podatkov:

- Nepreverjene spletne trgovine ali oglasi (pogosto najdete jih v pojavnih oknih ali na družbenih omrežjih)
- Neznane ankete, spletni kvizi ali nagradne igre
- Nezaščitena javna omrežja Wi-Fi
- Povezave v neželenih e-poštnih sporočilih ali SMS-sporočilih
- Platforme družbenih medijev, zlasti v komentarjih ali neposrednih sporočilih

Nasvet: Tudi če se vam platforma zdi znana, vedno preverite spletni naslov in se izogibajte deljenju občutljivih podatkov, kot so identifikacijske številke ali finančne informacije, razen če to ni nujno potrebno in varno.

4. Katere podatke lahko delimo – in katerih nikoli ne smemo deliti na spletu?

- **Lahko delimo (z previdnostjo):** ime, mesto in nespecifična lokacija, splošni interesi ali hobiji, poklicne informacije (npr. delovno mesto), javni e-poštni naslov (za delo), profilne fotografije
- **Nikoli ne smete deliti na spletu:** gesla in PIN-kode, polni naslov (razen v preverjenih vladnih spletnih trgovinah), identifikacijske številke, davčne številke, podatki o bančnih računih ali kreditnih karticah, zdravstveni podatki ali informacije o zdravju, občutljivi podatki o družini ali potovalni načrti

Pravilo: če bi se informacije lahko uporabile za dostop do vašega denarja, identitete ali zasebnega življenja, jih ne delite na spletu, ne glede na to, kdo vas za to prosi.

5. Varnostno kopiranje podatkov pomeni izdelavo kopije pomembnih datotek, dokumentov, fotografij in nastavitev na varnem in ločenem mestu. To je lahko zunanji trdi disk, ključ USB ali varna storitev za shranjevanje v oblaku.

Zakaj je varnostno kopiranje pomembno:

Vaši podatki se lahko nenadoma izgubijo ali ogrozijo zaradi:

- Okvare naprave (npr. okvara računalnika, poškodba telefona)
- Krajo ali izgubo telefona ali računalnika
- napadov z izsiljevalsko programsko opremo ali zlonamerno programsko opremo, ki zaklenejo ali uničijo vaše datoteke
- Naključnega izbrisa ali formatiranja
- naravnih nesreč (požar, poplava itd.)

Kako vas varnostna kopija ščiti pred napadi zlonamerne programske opreme:

Zlonamerna programska oprema, kot je izsiljevalska programska oprema, lahko šifrira vaše datoteke in zahteva plačilo za njihovo odklepanje. Če imate varno varnostno kopijo, vam ni treba plačati odkupnine – lahko ponastavite napravo in varno obnovite datoteke iz varnostne kopije.

Podobno lahko virusi in trojanski konji poškodujejo vaše datoteke ali operacijski sistem. Če imate varnostno kopijo datotek, lahko ponovno namestite sistem in obnovite pomembne podatke, ne da bi kaj izgubili.

Najboljše prakse za varno varnostno kopiranje:

- Uporabljajte lokalno varnostno kopijo in varnostno kopijo v oblaku: shranite kopijo na zunanji trdi disk in eno v zanesljivi storitvi v oblaku (kot so Google Drive, Dropbox, iCloud, OneDrive).
- Šifrirajte občutljive varnostne kopije: za občutljive podatke uporabite zaščito z geslom ali šifriranje.
- Redno varnostno kopirajte: nastavite tedenski ali mesečni urnik, odvisno od tega, kako pogosto posodabljate datoteke.
- Odklopite zunanje diske, ko jih ne uporabljate: če pride do napada izsiljevalske programske opreme, lahko ta napade tudi priključene diske.
- Preizkusite varnostne kopije: Preverite, ali vaš sistem varnostnega kopiranja deluje, tako da občasno poskusite obnoviti datoteke.

6. Nasveti za varnost vaših podatkov

- Uporabljajte močna, edinstvena gesla (in jih redno spreminjajte)
- Omogočite dvofaktorsko avtentikacijo (2FA)
- Poskrbite, da je programska oprema in protivirusni program posodobljen
- Ne klikajte na sumljive povezave ali priloge
- Ne delite osebnih podatkov po telefonu ali e-pošti, razen če so preverjeni
- Redno varnostno kopirajte svoje podatke (v oblak ali na zunanji trdi disk)
- Bodite previdni pri uporabi javnega Wi-Fi-ja – ne prijavljajte se v občutljive račune
- Preverite nastavitve zasebnosti na družbenih omrežjih
- Premislite, preden objavite – ko je nekaj enkrat na spletu, ga je mogoče kopirati ali zlorabiti

Priloga 10 | Kako varnostno kopirati datoteke

1. Varnostno kopiranje datotek na zunanji disk

Korak 1: Priključite zunanji disk

- Z ustreznim kablom ali vtičnico priključite zunanji trdi disk ali USB-ključ na računalnik.
- Preverite, ali računalnik prepozna napravo (preverite mapo »Ta računalnik« ali »Moj računalnik« v sistemu Windows ali Finder v sistemu Mac).

Korak 2: Izberite datoteke, ki jih želite varnostno kopirati

- Odprite mapo, ki vsebuje datoteke, ki jih želite varnostno kopirati.
- Izberete lahko posamezne datoteke ali celotne mape. Če želite izbrati več datotek ali map, med klikom na elemente pridržite tipko Ctrl (Windows) ali Cmd (Mac).

Korak 3: Kopirajte datoteke

- Desno kliknite na izbrane datoteke in izberite Kopiraj (ali uporabite bližnjico na tipkovnici **Ctrl+C** za Windows, **Cmd+C** za Mac).
- Pojdite na zunanji disk v »Ta računalnik« (Windows) ali Finder (Mac).
- Desno kliknite na zunanji disk in izberite Prilepi (ali uporabite **Ctrl+V** za Windows, **Cmd+V** za Mac), da kopirate datoteke.

Korak 4: Varno izključite zunanji disk

- Ko so datoteke kopirane, se prepričajte, da zunanji disk varno izključite, da ne poškodujete datotek.
- V sistemu Windows desno kliknite zunanji disk v »Ta računalnik« in izberite Izvleci.
- V sistemu Mac povlecite ikono zunanjega diska v koš ali kliknite gumb za izmet ob disku v Finderju.
- Na napravi Apple (Mac ali iPhone) odprite **Nastavitve** in se prijavite s svojim Apple ID.
- Na računalniku Mac lahko dostopate do iClouda v **System Preferences** (Sistemski nastavitve) > **Apple ID** > **iCloud**.
- Na telefonu iPhone odprite **Nastavitve** > [Vaše ime] > **iCloud**.

2. Varnostno kopiranje datotek v oblak

Uporaba Google Drive

Korak 1: Prijavite se v svoj Google račun

- Odprite spletni brskalnik in odprite Google Drive.
- Prijavite se s svojimi podatki za Google račun (ali ustvarite nov račun, če ga še nimate).

Korak 2: Prenos datotek v Google Drive

- Kliknite gumb Novo na levi stranski vrstici.
- Izberite Naloži datoteko ali Naloži mapo, odvisno od tega, kaj želite varnostno kopirati.
- Poiščite datoteke ali mape, ki jih želite naložiti, in kliknite Odpri.

Korak 3: Uredite datoteke (neobvezno)

- V Google Drive lahko ustvarite mape, da bodo vaše varnostne kopije organizirane. Kliknite Novo > Mapa, poimenujte mapo in vanjo premaknite datoteke s povlečenjem in spuščanjem.

Korak 4: Preverite nalaganje

- Preverite, ali je nalaganje datotek končano. Google Drive med nalaganjem prikaže vrstico stanja.

Uporaba Dropboxa

Korak 1: Prijavite se v svoj račun Dropbox

- Odprite brskalnik in obiščite Dropbox.
- Prijavite se ali ustvarite nov račun Dropbox, če ga še nimate.

Korak 2: Naložite datoteke v Dropbox

- Ko se prijavite, kliknite gumb Naloži datoteke.
- Izberite datoteke ali mape, ki jih želite varnostno kopirati iz računalnika, in kliknite Odpri.
- Datoteke lahko tudi povlečete in spustite neposredno na spletno mesto Dropbox.
- Na iPhonu preverite porabo prostora v iCloudu tako, da odprete Nastavitve > [Vaše ime] > iCloud

Pomembni nasveti za varnostno kopiranje:

- Redno varnostno kopirajte: Vzpostavite navado, da vsaj enkrat na teden varnostno kopirate svoje podatke, da ne izgubite pomembnih datotek.
- Uporabljajte lokalne in oblačne varnostne kopije: za dodatno varnost shranite kopijo podatkov na zunanji trdi disk in v oblak.
- Šifrirajte občutljive datoteke: Pri shranjevanju občutljivih podatkov (npr. finančnih evidenc, osebnih dokumentov) razmislite o njihovem šifriranju, preden jih naložite v oblak ali shranite na zunanji disk.
- Preizkusite varnostno kopijo: občasno preizkusite varnostno kopijo z obnovitvijo nekaterih datotek, da se prepričate, da vse deluje pravilno.

Varnostno kopiranje datotek je ključnega pomena za zagotovitev varnosti in obnovljivosti podatkov v primeru okvare naprave, kibernetskega napada ali naključnega izbrisa. Zunanji diski in storitve v oblaku ponujajo zanesljive načine za varno shranjevanje podatkov. Če imate kakršna koli vprašanja, prosimo, da zaprosite za pomoč pri nastavitvi sistema za varnostno kopiranje!

Priloga 11| Seznam za preverjanje varnosti na spletu

1. Zaščita osebnih podatkov

- **Preglejte osebne podatke, ki jih delite na spletu** – Vedno bodite previdni pri objavljanju na družbenih omrežjih in drugih platformah. Delite samo potrebne informacije.

- **Zaupne podatke ohranite zasebne** – Nikoli ne delite gesel, PIN-kod, številk bančnih računov ali identifikacijskih številk na spletu.

- **Uporabljajte močna, edinstvena gesla** za svoje račune in jih redno spreminjajte.

  Če je mogoče, **omogočite dvofaktorsko avtentikacijo** za račune, zlasti za bančne račune, e-pošto in družbena omrežja.

2. Prepoznavanje prevar

- **Bodite pozorni na pogoste spletne prevare** – Naučite se prepoznati prevare, kot so phishing, smishing, vishing in finančne prevare.

- **Opozorilni znaki za prevare**:

  - Nujni jezik (npr. »Takojšnje ukrepanje je potrebno!«)
  - Zahteve po osebnih, bančnih ali prijavnih podatkih
  - Sumljive povezave ali telefonske številke
  - Čustvena manipulacija ali grožnje (npr. »Vaš račun bo zaprt«)

- **Poznajte razliko med legitimnimi in goljufivimi zahtevami** – preverite pristnost vsakega telefonskega klica, e-poštnega sporočila ali sporočila, ki ga prejmete, preden odgovorite.

- **V primeru dvoma se vedno obrnite neposredno na organizacijo** prek njenih uradnih kontaktnih podatkov**,** da preverite trditev.

3. Obravnavanje prevar in zlonamernih vsebin

- **Ne klikajte na sumljive povezave in ne odpirajte prilog** od neznanih pošiljateljev. To so lahko poskusi phishinga ali lahko vsebujejo zlonamerno programsko opremo.

- **Vse sumljive e-pošte, sporočila ali telefonske klice prijavite** pristojnim organom (npr. SI-CERT v Sloveniji).

- **Vedno preverite vse finančne zahteve** (denarna nakazila, podatki o kreditnih karticah) tako, da pokličete neposredno osebo ali organizacijo.

- **Bodite previdni pri nezaželenih telefonskih klicih**, še posebej če vas klicatelj pritiska, da mu posredujete denar ali osebne podatke. Odložite slušalko in pokličite nazaj na znano številko.

4. Zaščita vaših naprav pred zlonamerno programsko opremo

- **Namestite in posodobite protivirusno programsko opremo,** da zaščitite svojo napravo pred virusi, zlonamerno programsko opremo in vohunsko programsko opremo.
- **Izogibajte se prenašanju aplikacij ali programske opreme** iz nepreverjenih virov. Uporabljajte samo uradne trgovine z aplikacijami (Google Play Store, Apple App Store).
- **Redno varnostno kopirajte svoje podatke** na zunanji disk ali v oblak, da preprečite izgubo podatkov zaradi morebitnega napada.
- **Poskrbite, da je vaša programska oprema in naprave posodobljene** z najnovejšimi varnostnimi popravki.
- **Bodite previdni pri uporabi javnega Wi-Fi-ja** – izogibajte se dostopu do občutljivih računov, ko ste povezani z javnimi omrežji.

5. Varno spletno nakupovanje

- **Nakupujte samo na preverjenih, zaupanja vrednih spletnih straneh** – v brskalniku poiščite simbol ključavnice in »https« v naslovu URL.
- Pri spletnem nakupovanju **uporabljajte varne načine plačila**, kot so kreditne kartice, saj ponujajo zaščito pred goljufijami.
- **Preverite ocene in mnenja,** preden nakupujete v novi spletni trgovini.

6. Varnostno kopirajte svoje podatke

- **Pomembne datoteke** (dokumente, fotografije, stike) redno **varnostno kopirajte** na zunanji disk ali v oblak. Tako boste svoje podatke zaščitili pred okvarami naprav ali napadi izsiljevalske programske opreme.
- Za dodatno varnost **uporabljajte zanesljivo storitev varnostnega kopiranja v oblaku** (Google Drive, Dropbox, OneDrive).
- **Ustvarite urnik varnostnega kopiranja**, da boste lahko zagotovili, da so vaši podatki vedno posodobljeni in varni.

7. Varnost na družbenih omrežjih

- **Bodite previdni pri tem, kar delite** na platformah družbenih omrežij (Facebook, Instagram itd.). Izogibajte se deljenju občutljivih podatkov, kot so vaš polni naslov, telefonska številka in finančni podatki. .
- **Prilagodite nastavitve zasebnosti,** da boste lahko nadzorovali, kdo lahko vidi vaše objave in osebne podatke.
- **Ne sprejemajte zahtev za prijateljstvo** ali sporočil od neznancev. Če osebe ne poznate, je varneje, da zahtevo ignorirate.

8. Kako ravnati v primeru napada socialnega inženiringa

- **Ostanite mirni in ne ukrepajte prenaglo,** če prejmete sumljivo sporočilo ali telefonski klic.
- **Nikoli ne posredujte osebnih podatkov po telefonu, e-pošti** ali **SMS-sporočilu, razen če ste prepričani o identiteti** osebe, s katero govorite.
- **Preverite identiteto klicatelja** tako, da ga pokličete nazaj na uradno telefonsko številko (npr. uradno številko vaše banke ali številko, navedeno na spletni strani podjetja).
- **Ne pustite se pritiskati** – goljufi pogosto ustvarjajo občutek nujnosti, da bi vas prisilili k hitremu ukrepanju. Vzemite si čas in preverite zahtevo.

9. Ukrepanje v nujnih primerih

- **Če sumite, da gre za prevaro, ali če so vaši osebni podatki ogroženi**, nemudoma obvestite svojo banko ali izdajatelja kreditne kartice, da zamrznejo vaše račune.
- **Prevare prijavite organom,** kot je SI-CERT v Sloveniji, ali lokalni policiji, če je to potrebno.
- Če niste prepričani o situaciji, **poiščite nasvet zaupanja vrednega prijatelja ali družinskega** člana.

10. Bodite obveščeni

- Bodite na tekočem z najnovejšimi prevarami – naročite se na novice ali opozorila iz zanesljivih virov, kot so SI-CERT ali druge varnostne platforme.
- Redno se izobražujte o spletnih grožnjah in o tem, kako se pred njimi zaščititi.

Ne pozabite:
Internet je lahko odlično orodje, vendar je pomembno, da ostajate pozorni in obveščeni o potencialnih tveganjih. Sledite temu seznamu in tako znatno zmanjšajte svojo ranljivost ter zaščitite svoje osebne podatke in naprave. Če kdaj koli dvomite, vedno prosite za pomoč ali nasvet nekoga, ki mu zaupate. Vaša varnost in mirna vest sta najpomembnejša!

Priloga 12 | Priporočila za nadaljnje branje in učenje za udeležence
Spletne strani o kibernetski varnosti: Evropske in vladne organizacije, ki se ukvarjajo s kibernetsko varnostjo

1) **OLAF – EVROPSKI URAD ZA BORBO PROTI GOLJUFIJAM**
   Spletna stran: https://anti-fraud.ec.europa.eu/olaf-and-you/report-fraud_en
   OLAF je organ EU, ki preiskuje goljufije, korupcijo in huda kršitve v institucijah in skladih EU .

2) **Podpora žrtvam Evropa**
   Spletna stran: https://victim-support.eu/help-for-victims/info-on-specific-types-of-victims/fraud-victims/
   Victim Support Europe je evropska krovna organizacija, ki zagovarja pravice vseh žrtev kaznivih dejanj in nudi podporne storitve prek svoje mreže nacionalnih organizacij, članic .

3) **EC3 – Europolov center za kibernetski kriminal**
   Spletna stran: https://www.europol.europa.eu/crime-areas/cybercrime
   Europol ponuja informacije o kibernetskem kriminalu in varnosti podatkov.

4) **CERT-EU (Ekipa za odzivanje na računalniške izredne dogodke za institucije EU)**
   Spletna stran: https://cert.europa.eu/
   Organizacija spremlja kibernetske grožnje in odgovarja na kibernetske napade na institucije Evropske unije ( ).

3.5 Modul II – Predhodni/naknadni test

1. Kateri od naslednjih primerov je primer varne rabe interneta?
A) Deljenje osebnega naslova na družbenih omrežjih
B) Uporaba močnih in edinstvenih gesel za vsak račun
C) Sprejemanje zahtev za prijateljstvo od neznanih oseb
D) Klik na vsako povezavo, ki izgleda zanimiva

2. Kakšno je pogosto tveganje pri uporabi družbenih omrežij?

A) Spoznavanje novih prijateljev
B) Preobremenjenost z informacijami
C) Prekomerno deljenje osebnih podatkov, ki se lahko zlorabijo
D) Redno posodabljanje nastavitev zasebnosti

3. Zakaj je treba preveriti vir, preden informacije delite na spletu?

A) Da se izognete širjenju napačnih informacij ali prevaram
B) Da povečate število všečkov in sledilcev
C) Da izboljšate delovanje računalnika
D) Da spremenite raven varnosti svojega profila

4. Katero od teh gesel je najmočnejše?

A) 123456
B) qwerty
C) Sunflower2025!#
D) geslo

5. Kaj naj storite, če prejmete sumljivo sporočilo iz hekerskega računa prijatelja?

A) Kliknite na povezavo, da vidite, kaj je

B) Prijavite ali blokirajte račun in obvestite prijatelja
C) Odgovorite in prosite za več informacij
D) Popolnoma ga ignorirajte

6. Kaj pomeni »digitalni odtis«?

A) Skupna količina podatkov, shranjenih na vašem računalniku
B) Zapis vaših spletnih dejavnosti in deljenih informacij
C) Geslo, ki ga uporabljate za svoje račune
D) Programska oprema, ki ščiti vaš računalnik

7. Zakaj je tvegano uporabljati isto geslo za vse račune?

A) Zaradi tega je lahko prijavanje prepočasno
B) Če je eden od računov hekan, so lahko tudi drugi računi ogroženi
C) Prihrani preveč časa
D) Zahteva uporabo upraviteljev gesel

8. Kakšen je najboljši način za zaščito vaše zasebnosti na družbenih omrežjih?

A) Nastavite svoj profil na „javno“
B) Delite vse osebne podatke
C) Redno pregledujte in prilagajajte nastavitve zasebnosti
D) V vsakem prispevku uporabite svoj pravi rojstni datum in naslov

9. Kaj je znak lažne ali prevare spletne strani?

A) Začne se z „https://“
B) Vsebuje pravopisne napake in nerealne ponudbe
C) V brskalniku je prikazan simbol ključavnice
D) Vsebuje kontaktne podatke

10. Zakaj se morate odjaviti iz svojih računov na skupnih ali javnih računalnikih?

A) Da naredite prostor za naslednjega uporabnika
B) Da preprečite nepooblaščen dostop do vaših podatkov
C) Da prihranite baterijo
D) Da se vaše geslo samodejno posodobi

Povzetek odgovorov

1-B, 2-C, 3-A, 4-C, 5-B, 6-B, 7-B, 8-C, 9-B, 10-B

MODULE III

Online Banking and Shopping Safety

4. Modul III – Varnost spletnega bančništva in spletnega nakupovanja

Cilj tega modula je opolnomočiti starejše, da bodo samozavestno uporabljali spletno bančništvo in nakupovalne platforme, tako da jim zagotovi osnovno znanje in praktične veščine za upravljanje digitalnih finančnih dejavnosti. Modul krepi razumevanje udeležencev o delovanju spletnega bančništva in storitev e-trgovine, hkrati pa poudarja varne in odgovorne prakse za zaščito pred goljufijami, prevari in kibernetskimi grožnjami.

S praktičnimi nasveti in primeri iz resničnega življenja modul podpira razvoj digitalne pismenosti in spodbuja starejše, da sprejmejo varne navade pri spletnih plačilih, upravljanju računov in deljenju osebnih podatkov. Ob koncu modula so udeleženci bolje opremljeni za ohranjanje finančne neodvisnosti, izkoriščanje digitalnih storitev in samozavestno, varno in samostojno spletno bančništvo in nakupovanje.

Poleg tega modul obravnava pogoste strahove in negotovosti, ki jih lahko doživljajo starejši pri uporabi digitalnih finančnih storitev, s ciljem zmanjšati tesnobo v zvezi z spletnimi transakcijami. Udeleženci se naučijo prepoznati zaupanja vredne platforme, izvajati osnovne varnostne preglede in ustrezno odgovarjati na sumljive dejavnosti. Z okrepitvijo zaupanja skozi prakso in jasna pojasnila modul pomaga starejšim, da se počutijo bolj v nadzoru nad svojimi digitalnimi finančnimi odločitvami, in podpira njihovo dolgoročno sodelovanje pri spletnem bančništvu in nakupovanju na varen in ozaveščen način.

4.1 Cilji učenja

Glavni cilj tega modula je opremiti starejše z praktičnim znanjem in spretnostmi, potrebnimi za varno uporabo spletnega bančništva in platform za e-trgovanje. Modul se osredotoča na gradnjo digitalnega zaupanja ob zmanjševanju strahu in tesnobe, povezanih s tehnologijo, kar udeležencem omogoča varno in neodvisno upravljanje finančnih transakcij. Udeleženci se bodo naučili, kako zaščititi svoje osebne in finančne podatke, prepoznati spletna tveganja in uporabljati učinkovite varnostne prakse v vsakdanjih digitalnih finančnih dejavnostih.

- Razumevanje osnov spletnega bančništva in e-trgovine, ki podpirajo varno navigacijo, upravljanje računa in digitalne transakcije.
- Razviti veščine za ustvarjanje močnih gesel in aktivirati dvofaktorsko avtentikacijo (2FA) z namenom povečati varnost spletnih računov.
- Prepoznati zanesljive spletne nakupovalne platforme in prodajalce s prepoznavanjem varnostnih indikatorjev, kot so HTTPS, ikone ključavnice, ocene strank in zanesljive plačilne metode.
- Prepoznajte in se izogibajte spletnim prevaram in finančnim goljufijam, vključno z lažnimi spletnimi stranmi, poskusi phishinga in zavajajočimi ponudbami.
- Zaščitite osebne in finančne podatke z uporabo protivirusne programske opreme, spremljanjem transakcij in nastavitvijo opozoril za sumljive dejavnosti.
- Uporabljajte varne internetne prakse pri uporabi javnih omrežij, vključno z razumevanjem tveganj javnega Wi-Fi-ja in uporabo VPN-jev za varne povezave.
- Razvijte digitalno samozavest in finančno neodvisnost z uporabo pridobljenih znanj v realnih situacijah spletnega bančništva in nakupovanja, z manj strahu in večjim zaupanjem v digitalna orodja.

4.2 Struktura, vsebina in učni izidi

Po uspešnem zaključku tega modula bodo udeleženci sposobni:

- Razumeti, kako deluje spletno bančništvo, spoznati prednosti upravljanja računov prek spleta in pridobiti pregled nad priljubljenimi bančnimi platformami.
- Navigirati po spletnih trgovinah, spoznati prednosti spletnega nakupovanja in priljubljenih platform.
- Nastaviti močna gesla in dvofaktorsko avtentikacijo (2FA): nasveti za ustvarjanje močnih gesel in uporabo 2FA za povečanje varnosti.
- Varno uporabljati bančne aplikacije in spletne strani: uporabljati samo uradne aplikacije/spletne strani, preveriti varne povezave (https).
- Nakupovanje na zaupanja vrednih spletnih straneh: preverjanje pristnosti spletne strani in razumevanje ocen in mnenj.
- Prepoznajte varne možnosti plačila: prepoznajte varne načine plačila (kreditne kartice) in se izogibajte nezavarovanim plačilom (bančnim prenosom).
- Zaščitite naprave: kako uporabljati protivirusno programsko opremo in posodabljati programsko opremo.
- Varno uporabljajte javna omrežja Wi-Fi za finančne transakcije: tveganja, povezana z javnimi omrežji, in uporaba VPN-jev za zagotavljanje varnosti.

4.3 Agenda I Podroben načrt seje

MODUL III
Pogoste spletne prevare, usmerjene v starejše

1. seja

Dobrodošli
Trajanje 5

Cilji

- Predstavite temo in ustvarite prijetno vzdušje.

Vsebina/metoda

- Kratek uvod v sejo, opis ciljev in postavitev pričakovanj. Pripravite teren za usposabljanje s predstavitvijo modula in njegovega pomena.

Material

- Tabla ali flipchart za cilje seje.
- Flomasterji.
- Natisnjena agenda ali predstavitvene diapozitive, ki opisujejo sejo.

2. seja

Dejavnost za spoznavanje: »Moj prvi trenutek z internetnim bančništvom«

Trajanje 10

Cilji učenja

- Vzpostavite povezavo prek skupnih izkušenj in predstavite temo.

Vsebina/metoda

- Izobraževalec prosi udeležence, naj na kratko predstavijo svoje prve izkušnje z internetnim bančništvom, vključno s tem, kaj so storili in kako so se počutili. Medtem ko udeleženci delijo svoje izkušnje, izobraževalec aktivno posluša in na flipchart ali tablo zapiše ključna čustva in misli (npr. nervoza, navdušenje, zmeda), s čimer vizualno zajame skupinske izkušnje in čustva. Na koncu izobraževalec na kratko povzame čustva in izkušnje, ki so jih udeleženci delili.

Material

- Flipchart ali tabla za zapisovanje ključnih besed (npr. nervozen, navdušen), flomasterji.

3. Srečanje

Predavanje 1: Razumevanje osnov spletnega bančništva in spletnega nakupovanja

Trajanje 30

Cilji

- Udeležencem pomagati razumeti, kako delujejo spletno bančništvo in spletno nakupovanje, ter razlikovati med varnimi in nevarnimi platformami.

Vsebina/metoda

- Izobraževalec obravnava uporabniku prijazne primere, kot so Monzo ali Revolut (bančništvo) in Zalando ali Coolblue (nakupovanje), ter poudari ključne značilnosti, kot so varnost, navigacija in uporabnost. Da bi utrdili svoje znanje, udeleženci primerjajo pravo spletno stran z lažno in uporabijo svoje znanje, da odkrijejo znake verodostojnosti in goljufije.
- Izobraževalec predstavi osnove spletnega bančništva in nakupovanja s pomočjo posnetkov zaslona in živih predstavitev. Izobraževalec udeležence popelje skozi preprosto bančno platformo, jim pojasni, kako deluje spletno bančništvo, in jim pokaže, kako preveriti stanje na računu, prenesti denar in uporabljati druge osnovne funkcije. Izobraževalec nato stori enako za spletno trgovino, udeležencem pokaže, kako se sprehajati po platformi, izbirati izdelke in nadaljevati z nakupnim postopkom. Izobraževalec prikaže dve spletni strani – eno varno in eno lažno – in udeležence prosi, naj ugotovijo, katera je varna, in pojasnijo, zakaj, ter jih spodbuja, naj uporabijo svoje znanje o varnosti spletnih strani. Na koncu izobraževalec obravnava ključne zaključke iz seje: pomembnost preverjanja varnih povezav (HTTPS), prepoznavanja legitimnih platform in načinov izogibanja prevaram.

Material

- PowerPoint predstavitev, vizualni gradivi,
- prenosni računalnik, projektor.

Dejavnost 1: Raziskovanje platforme
Trajanje 20

Cilji učenja

- Vaja uporabe spletnih platform in prepoznavanja ključnih funkcij.

Vsebina/metoda

- Izobraževalec udeležence razdeli v pare in vsaki pari da eno kartico z nalogo, pri čemer jih obvesti, da vsaka kartica vsebuje navodila o tem, kaj naj iščejo med vajo, npr. prepoznavanje varnostnih značilnosti na bančni ali nakupovalni spletni strani. Ko se vaja začne, izobraževalec hodi po prostoru, opazuje udeležence, daje nasvete in odgovarja na vprašanja. Vodja usposabljanja udeležencem pomaga, da se osredotočijo na ključne varnostne elemente, kot so ikone ključavnic, nastavitve 2FA, naslovi „https“ ali simboli za varno plačevanje, da se prepriča, da razumejo, kako prepoznati varnostne funkcije. Po vaji vodja usposabljanja vsak par prosi, da na kratko predstavi, kaj je odkril med preiskavo. Vodja spodbuja kratko razpravo z vprašanji, kot so: „Kaj je bilo pri nalogi enostavno in kaj težko?“ in „Kaj vas je pripeljalo do sklepa, da je spletna stran ali aplikacija varna ali nevarna?“ To bo udeležencem pomagalo razmisliti o svojih izkušnjah in poglobiti razumevanje tega, kaj spletno platformo naredi varno.
- Na koncu izvajalec usposabljanja zagotovi dodatne vire, tako da deli povezave do kratkih člankov ali videoposnetkov o varnosti spletnih platform. Razdeljeni bodo tudi tiskani materiali s primeri varnih in nevarnih elementov spletnih strani/aplikacij, ki bodo služili kot referenčni materiali in utrdili znanje, pridobljeno med vajo.

Material

- Tiskani priročniki z nalogami za udeležence.
- Tablični računalniki, prenosni računalniki ali veliki natisnjeni zasloni z demo različicami bančnih ali nakupovalnih platform.

Odmor | Trajanje *5'*

- **Udeležencem omogočite čas za počitek in razmislek.**
- **Kratek odmor za osvežitev.**

4· Srečanje

Predavanje 2: Varnostne prakse pri spletnem bančništvu
Trajanje 30

Cilji učenja

- Udeležencem pomagati pri ustvarjanju močnih gesel in spremljanju računov.

Vsebina/metoda

- Izobraževalec začne s predstavitvijo ključnih varnostnih praks pri spletnem bančništvu. Teme, ki se obravnavajo, vključujejo ustvarjanje močnih gesel, omogočanje dvofaktorskega preverjanja pristnosti (2FA) in nastavitev opozoril za račune. Izobraževalec bo v predavanje vključil primere iz resničnega življenja ali kratke zgodbe o spletnih bančnih prevarah. Na podlagi primerov prevar iz resničnega življenja izobraževalec poudari pogoste grožnje in deli praktične varnostne nasvete. Eden takih primerov je prevara »Safe Account«, o kateri so poročali na Irskem in ki pomaga ponazoriti, kako goljufije delujejo v praksi. Udeleženci so spodbujeni, da te korake uporabijo na svojih napravah, kar naredi delavnico praktično, koristno in takoj uporabno .
- Izobraževalec udeležencem pojasni, zakaj je varno spletno bančništvo bistvenega pomena in kako pogosto prihaja do kršitev varnosti. Izpostavi potencialna tveganja in pokaže, kako lahko preprosti varnostni ukrepi udeležence zaščitijo pred goljufijami. Z uporabo preverjanja moči gesla izobraževalec v realnem času prikaže razliko med šibkimi in močnimi gesli. Izobraževalec udeležence prosi, naj predlagajo vzorčna gesla, in jih v živo preizkusi, da poudari pomembnost ustvarjanja močnih, edinstvenih gesel. Nato s pomočjo posnetkov zaslona ali simulacij v živo prikaže, kako omogočiti 2FA. Izobraževalec pojasni vlogo 2FA pri preprečevanju nepooblaščenega dostopa in udeležence vodi skozi proces njene omogočitve. Nato izobraževalec pojasni, kako spremljati bančne aktivnosti in nastaviti opozorila za sumljive transakcije. Z uporabo posnetkov zaslona ali vzorčne bančne aplikacije izobraževalec udeležence vodi skozi korake za nastavitev teh opozoril in poudari pomen budnosti pri spremljanju aktivnosti na računu. Med sejo vprašanj in odgovorov izobraževalec udeležence prosi, naj delijo svoje izkušnje ali pomisleke glede varnosti spletnega bančništva. Na koncu bo izobraževalec razdelil tiskane sezname, ki povzemajo navade za varno spletno bančništvo in bodo udeležencem v pomoč.

Material

- Predstavitev, orodje za prikaz moči gesla.
- Natisnjen kontrolni seznam.

Dejavnost 2: Zaščitite svoje spletno bančništvo
Trajanje 20

Cilji

- Udeleženci se v simuliranem bančnem okolju naučijo nastaviti 2FA in spremljati transakcije.

Vsebina/metoda

- Izobraževalec udeležence razdeli v pare ali majhne skupine. Vsaka skupina bo delala na prenosnih računalnikih ali pametnih telefonih, na katerih so nameščene demo aplikacije ali bančne platforme, kot sta Revolut ali Monzo. Izobraževalec udeležence vodi skozi proces omogočanja 2FA: s pomočjo podrobnih navodil jim pomaga zaključiti postopek nastavitve 2FA na demo platformi. Hodijo po prostoru, nudijo pomoč in poskrbijo, da vsi pravilno sledijo navodilom. Nato udeležence prosi, naj preverijo, ali so bile opravljene kakšne nepooblaščene

transakcije, in jim pomaga nastaviti opozorila za sumljive dejavnosti. Prepriča se, da udeleženci razumejo postopek in izvedejo te korake na svoji demo platformi.

- Po vaji prosite vsako skupino, da deli svoje izkušnje: »Na kakšne izzive ste naleteli pri nastavitvi 2FA?« »Ste uspeli najti in nastaviti opozorila o transakcijah? Kateri koraki so bili koristni in kateri so bili težki?« Zagotovi povratne informacije: poudari pomen omogočanja 2FA in spremljanja transakcij za varnost spletnega bančništva.

Material

- Prenosni računalniki ali pametni telefoni.
- Demo bančna aplikacija.
- Podrobna navodila za nastavitev 2FA in pregled transakcij.

Odmor | Trajanje *5'*

- **Čas za počitek in pripravo**
- **Kratek odmor za osvežitev.**

5. Srečanje

Predavanje 3: Varno spletno nakupovanje
Trajanje 30

Cilji

- Pomagati starejšim razumeti, kako oceniti spletne strani, prepoznati varne možnosti plačila in prepoznati goljufive prodajalce.

Vsebina/metoda

- Med predavanjem izobraževalec pojasni, kako prepoznati varne spletne strani za spletno nakupovanje in preveriti pristnost prodajalcev. Izobraževalec pojasni, kako prepoznati varne spletne strani, s poudarkom na protokolu HTTPS, ikonah ključavnice in drugih varnostnih simbolih. Predstavi primere dobrih in slabih spletnih strani, da pokaže, kako oceniti njihovo verodostojnost. Izobraževalec tudi pokaže, kako brati ocene in preveriti, ali so prodajalci pristni. Na koncu predavanja izvajalec udeležencem zastavi vprašanja, kot so „Kaj protokol HTTPS pove o varnosti spletnih strani?“ in „Kako lahko preverite, ali je spletni prodajalec zaupanja vreden?“, da utrdi ključne koncepte in vključi udeležence.
- Na koncu izobraževalec udeležence spodbudi, da delijo svoje izkušnje z nakupovanjem na spletu ali svoje pomisleke glede varnega nakupovanja na spletu. Obravnavajo se morebitne težave, s katerimi so se udeleženci srečali pri nakupovanju na spletu, izobraževalec pa odgovori na vsa njihova vprašanja.

Material

- Natisnjeni primeri nakupov, posnetki zaslona spletnih strani.

Dejavnost 3: Nakupovanje na zaupanja vrednih spletnih straneh
Trajanje 20

Cilji

- Udeleženci se naučijo, kako oceniti varnost spletnih trgovin in preveriti načine plačila.

Vsebina/metoda

- Udeleženci se v skupinah najprej seznanijo z legitimno spletno stranjo trgovine, da prepoznajo ključne varnostne značilnosti (npr. HTTPS, pečati zaupanja, varne možnosti plačila). Nato jim s pomočjo predstavitve ali vnaprej posnetega videa pokažejo primere lažnih spletnih strani ali sumljivih spletnih dejavnosti. Vaja se osredotoča na to, da jim pomaga prepoznati pogoste opozorilne znake in primerjati varne in nevarne spletne strani.
- Izobraževalec udeležence razdeli v manjše skupine in jim da seznam spletnih strani, ki jih morajo pregledati. Vsaka skupina oceni varnost spletnih strani, pri čemer se osredotoči na kazalnike, kot so protokol HTTPS, varne plačilne metode in verodostojne ocene. Izobraževalec hodi med skupinami, po potrebi jim pomaga in jim svetuje, če potrebujejo pomoč pri prepoznavanju opozorilnih znakov, kot so sumljive ocene ali nevarnostni elementi spletne strani. Na koncu skupine izmenjajo informacije o spletnih straneh, ki so bile ocenjene kot varne, in utemeljijo svojo oceno.

Material

- Računalniki z dostopom do interneta.
- Seznam spletnih strani za nakupovanje.

Odmor | Trajanje 5 minut

- **Čas za počitek in pripravo.**
- **Kratek odmor za osvežitev.**

6. Srečanje

Predavanje 4: Zaščita osebnih in finančnih podatkov
Trajanje 30

Cilji

- Seniorjem posredovati znanje o varnosti naprav, uporabi protivirusne programske opreme in zaščiti Wi-Fi povezav.

Vsebina/metoda

- Izobraževalec predava o konceptih protivirusne programske opreme, VPN-jev in varnega brskanja po spletu. Predstavitev vključuje diapozitive s ključnimi informacijami in primeri za vsako temo, pri čemer poudarja najboljše prakse za varnost naprav. Izobraževalec pokaže, kako posodobiti naprave, namestiti protivirusno programsko opremo in upravljati nastavitve zasebnosti za izboljšanje varnosti. Pokaže kratek poučni video, ki prikazuje pravilno uporabo VPN za varno brskanje po spletu. Med predavanjem bo izobraževalec spodbujal udeležence k aktivni udeležbi in poskrbel za interaktivnost s postavljanjem vprašanj in navajanjem primerov

iz prakse o tem, kako ostati varen na spletu. Po predavanju bodo udeleženci imeli priložnost postaviti vprašanja in pojasniti morebitne dvome o varnosti naprav in zaščiti na spletu.

- Na koncu bo izobraževalec predstavil preproste, vsakodnevne prakse za zaščito osebnih podatkov, kot so izogibanje sumljivim povezavam, neposredovanje preveč informacij na spletnih straneh in prepoznavanje pogostih spletnih pasti. Ti koraki udeležencem pomagajo razviti varnejše digitalne navade.

Material

- Predstavitvene diapozitive, video vodič o VPN-jih.

Dejavnost 4: Zaščita vaših naprav
Trajanje 20

Cilji

- Udeleženci se naučijo namestiti protivirusno programsko opremo, uporabljati VPN-je in upravljati nastavitve zasebnosti.

Vsebina/metoda

- Udeleženci v skupinah namestijo protivirusno programsko opremo, omogočijo VPN za varno brskanje po spletu in preverijo nastavitve zasebnosti v aplikacijah in družbenih medijih. Ta praktična vaja jim pomaga uporabiti praktične ukrepe za zaščito svojih naprav in osebnih podatkov na spletu.
- Izobraževalec udeležence razdeli v majhne skupine ali pare in jim za vajo zagotovi prenosne računalnike, protivirusno programsko opremo in aplikacije VPN. Vsaka skupina sledi navodilom izobraževalca, da namesti protivirusno programsko opremo, omogoči VPN za varno brskanje po spletu in preveri nastavitve zasebnosti v aplikacijah in računih družbenih medijev. Izobraževalec kroži med skupinami, po potrebi nudi pomoč in zagotavlja, da vsi udeleženci uspešno opravijo naloge. Izobraževalec skupine tudi vodi skozi proces prepoznavanja ključnih nastavitev zasebnosti na njihovih napravah in profilih v družbenih medijih, ki izboljšujejo varnost. Po vaji izobraževalec udeležence prosi, naj delijo svoje izkušnje z zaščito svojih naprav in nastavitvami zasebnosti.

Material

- Prenosni računalniki, protivirusna programska oprema, aplikacija VPN

7. seja

Razprava | Trajanje 10 min

Cilji učenja

- Razmislite o ključnih spoznanjih iz seje in pojasnite morebitna vprašanja.

Vsebina/metoda

- Skupinska razprava, med katero udeleženci delijo svoje izkušnje in zaključke. Izobraževalec odgovori na vsa preostala vprašanja. Udeležence spodbuja, naj nadaljujejo z vadbo veščin, pridobljenih med sejo.

Zaključek | Trajanje 5

Cilji učenja

- Povzemite sejo in spodbujajte udeležence, naj nadaljujejo z varnim izvajanjem.

Vsebina/metoda

- Izobraževalec povzame sejo in poudari najpomembnejše obravnavane teme. Udeležence spodbudi, naj nadaljujejo z vajo pridobljenih veščin v okviru svojih osebnih spletnih dejavnosti. Izobraževalec se udeležencem zahvali za sodelovanje in jih spodbudi, naj pridobljeno znanje uporabijo za zagotavljanje svoje varnosti na internetu.

Material

- Gradivo z glavnimi točkami in viri.

4.4 Dodatne informacije

4.4.1 Samorefleksija izvajalcev

- Kateri vidiki usposabljanja so potekali posebej dobro?
- Kateri deli seje so bili zame najbolj zahtevni?
- Kako so bili udeleženci vključeni in odzivni med aktivnostmi?
- So udeleženci dosegli učne cilje? Če ne, zakaj?
- Kakšne prilagoditve bi lahko izboljšale sejo v prihodnjih ponovitvah?

4.4.2 Ocena programa s strani izvajalcev usposabljanja

- Je bila vsebina usposabljanja ustrezna potrebam starejših in prilagojena njihovi ravni znanja in digitalnih izkušenj?
- So udeleženci razumeli osnovna načela spletnega bančništva, e-trgovine, kibernetske varnosti in zasebnosti na spletu?
- Ali so bile praktične vaje, kvizi in predstavitve učinkovite pri utrjevanju znanja in krepitvi digitalne samozavesti?
- So razprave in razmisleki udeležencem omogočili poglobiti razumevanje varnih spletnih praks?
- Ali so bili doseženi želeni učni cilji, kot so sposobnost ustvarjanja močnih gesel, prepoznavanja lažnih spletnih strani, spremljanja transakcij in konfiguriranja varnostnih nastavitev?
- So udeleženci pokazali večjo samozavest in neodvisnost pri opravljanju spletnega bančništva in nakupovanju?
- Kateri vidiki usposabljanja so bili najuspešnejši in katera področja bi bilo mogoče izboljšati za prihodnje seje?

4.4.3 Gradivo, dodatni viri

Priloga 1 | Značilnosti močnih gesel

Da bi zagotovili varnost vaših spletnih računov, mora vaše geslo imeti naslednje značilnosti:

- Vsaj 8 znakov – daljše, kot je geslo, bolje je
- Mešanica velikih in malih črk
- Kombinacija črk in številk
- Vključitev vsaj enega posebnega znaka, npr. !, @, #, ?,]
- Opomba: V geslu ne uporabljajte znakov < ali >, saj lahko povzročijo težave v spletnih brskalnikih
- Podrobna navodila so na voljo spodaj!

Varnost pri spletnem bančništvu in nakupovanju
Značilnosti močnih gesel
Zakaj so močna gesla pomembna

Ustvarjanje močnih gesel je ključni korak pri zaščiti vaših osebnih in poklicnih podatkov. Šibka gesla hekerjem olajšajo dostop do vaših računov.

Uporabite naslednja navodila za ustvarjanje varnih gesel:

<u>Značilnosti močnih gesel</u>

- Najmanj 8 znakov – daljša so, bolje je.
- Kombinacija velikih in malih črk.
- Mešanica črk in številk.
- Vsaj en poseben znak, na primer: !, @, #, ?,].
- V geslu ne uporabljajte znakov < ali >, saj lahko v nekaterih spletnih brskalnikih povzročijo težave.
- Dodatni nasveti
- Ne uporabljajte osebnih podatkov (kot so vaše ime ali datum rojstva).
- Za vsak račun uporabite edinstveno geslo.
- Razmislite o uporabi zaupanja vrednega upravitelja gesel.
- Redno spreminjajte gesla in se izogibajte ponovni uporabi starih gesel.

Vaja (neobvezno)
Ustvarite močno vzorčno geslo z uporabo zgornjih nasvetov:

Ocenite moč gesla:

SLABO	ZADOVOLJIVO	MOČNO

Dodatek 2 | Navodila za 2FA in opozorila

Del I: *Nastavitev dvofaktorskega preverjanja pristnosti (2FA)*

Namen: *2FA zagotavlja dodatno varnost, saj zahteva tako geslo kot tudi drugo metodo preverjanja (npr. kodo, poslaną na vaš telefon).*

Koraki

1. Odprite demo bančno aplikacijo ali platformo na svojem napravi.

2. Pojdite v Nastavitve → Varnostne nastavitve.

3. Tapnite Omogoči dvofaktorsko avtentikacijo (2FA).

4. Izberite metodo preverjanja:

- SMS-koda

- Aplikacija za avtentifikacijo (npr. Google Authenticator)

5. Sledite navodilom (vnesite preveritveno kodo, ki ste jo prejeli).

6. Preverite, ali je 2FA aktivna in deluje.

2. del*: Pregled transakcij in nastavitev opozoril*

Namen: *S spremljanjem transakcij in nastavitvijo opozoril lahko pravočasno odkrijete sumljive dejavnosti.*

Koraki:

7. V aplikaciji prejdite na Zgodovina transakcij.

8. Preglejte nedavne transakcije.

9. Prepoznajte in označite vse, kar vam ni znano.

10. Pojdite v Nastavitve obvestil ali opozoril.

11. Vključite opozorila za:

- Velike ali nenavadne transakcije

- Prijave z novih naprav

- spremembe nastavitev vašega računa

Ključni opomniki

- *Omogočite 2FA na vseh finančnih aplikacijah.*
- *Redno preverjajte zgodovino transakcij.*
- *Uporabite opozorila, da boste obveščeni o nenavadnih dejavnostih.*

Priloga 3| Prepoznavanje varnostnih elementov na bančnih in spletnih nakupovalnih platformah

Naloga 1. Poiščite stanje na računu

Poskusite najti mesto, kjer lahko preverite stanje na računu.

- Kje se nahaja? .....
- Kako je označeno (npr. „Saldo“, „Pregled računa“, „Razpoložljiva sredstva“)? .....

Naloga 2. Poiščite možnost plačila

Poskusite najti, kje lahko opravite plačilo ali zaključite nakup.

- Kako se ta možnost imenuje?
  ☐ Prenos
  ☐ Plačilo
  ☐ Košarica / Blagajna
  ☐ Drugo: .....
- Je bilo enostavno najti?
  ☐ Da
  ☐ Ne
  Zakaj? .....

Naloga 3. Prepoznajte varnostne funkcije spletnega mesta

Pazljivo si oglejte spletno stran in označite elemente, ki kažejo, da je varna.

☐ ikona ključavnice v naslovni vrstici brskalnika
☐ naslov se začne s **https**
☐ prepoznavni logotipi plačilnih sistemov (npr. Visa, Mastercard, PayPal, BLIK)
☐ dodatna potrditev plačila (SMS koda, bančna aplikacija)
☐ informacije o politiki zasebnosti

Ste opazili še kaj drugega? .....

Naloga 4. Poiščite morebitne opozorilne znake

Ali ste opazili kaj, kar bi lahko nakazovalo, da je spletna stran lahko nevarna?

☐ ni ikone ključavnice
☐ sumljiv naslov spletnega mesta
☐ preveč pojavnih oken
☐ zahteve po preveč osebnih podatkih
☐ drugo: .....

Naloga 5. Preverite dodatne varnostne nastavitve

Poiščite informacije o dodatni zaščiti računa ali plačil.

Ali ste našli:
☐ dvofaktorsko preverjanje pristnosti (2FA)
☐ preverjanje prek SMS
☐ potrditev prek bančne aplikacije

Kje se nahaja ta možnost? .....

Povzetek vaje:
Kateri del naloge je bil najlažji? .....
Kateri del je bil najtežji? .....
Kaj vam pomaga prepoznati, da je spletna stran ali aplikacija varna? .....

Zaključek: Za varno uporabo spletnega bančništva in spletnih trgovin je treba paziti na varnostne kazalnike spletne strani, spletni naslov in način potrjevanja plačil.

Ne pozabite: Če vas kaj na spletni strani spravi v negotovost ali vzbuja sum, **ne vnašajte svojih osebnih podatkov in prekinite postopek.**

Priloga 4 | Priporočila za nadaljnje branje in učenje za udeležence

Spletne strani o kibernetski varnosti: evropske in vladne organizacije, ki se ukvarjajo s kibernetsko varnostjo

---

1) **Kako nastaviti dvofaktorsko avtentikacijo na vseh vaših spletnih računih**
   Spletna stran: https://www.loginradius.com/blog/identity/how-to-setup-2fa-in-online-accounts/
   Ta izčrpen vodnik pojasnjuje pomen dvofaktorskega preverjanja pristnosti (2FA) in vsebuje podrobna navodila za njegovo nastavitev na različnih spletnih računih, vključno z e-pošto, družbenimi omrežji in bančnimi platformami. Obravnava metode, kot so SMS-kode, aplikacije za preverjanje pristnosti in varnostni ključi, ki izboljšujejo varnost računa.
2) **Nastavitev dvofaktorskega preverjanja pristnosti | Storitve tehnološke podpore**
   Spletna stran: https://it.nmu.edu/docs/setting-2-factor-authentication
   Ta vir iz oddelka za informacijsko tehnologijo Univerze Severne Michigane opisuje postopek za omogočanje dvofaktorskega preverjanja pristnosti (2FA) v storitvah NMU, kot sta MyNMU in MyUser. Ponuja več možnosti preverjanja, vključno z aplikacijami za preverjanje pristnosti, varnostnimi ključi USB in rezervnimi kodami, da se zagotovi varen dostop do univerzitetnih sistemov.
3) **Bank of Ireland opozarja na porast prevar z »varno računom«**
   Članek: https://www.rte.ie/news/business/2025/0606/1517043-spike-in-safe-account-scam-warning-boi/
   Ta novica poroča o znatnem povečanju števila prijav goljufij z »varnimi računi« na Irskem, ki so se v zadnjem tednu povečale za desetkrat. Banka Irske opozarja potrošnike na tovrstne goljufije, pri katerih goljufi pod lažnimi pretvezami prepričajo posameznike, da prenesejo denar na »varne« račune, in poudarja pomen pazljivosti in varnih bančnih praks.

4) **Nacionalni center za kibernetsko varnost – Varno spletno nakupovanje**
   Spletna stran: https://www.ncsc.gov.uk/guidance/shopping-online-securely
   Ta uradna navodila britanske vlade potrošnikom ponujajo praktične nasvete za varno spletno nakupovanje. Obravnavajo področja, kot so preverjanje legitimnosti spletnih trgovin, uporaba varnih načinov plačila, zaščita osebnih podatkov in prijavljanje sumljivih dejavnosti. Ključna priporočila vključujejo uporabo kreditnih kartic za spletne nakupe, omogočanje dvofaznega preverjanja in previdnost pri nezaželenih ponudbah in povezavah.
5) **Kako ustvariti močno geslo**
   Video: https://www.youtube.com/watch?v=_wQTRMBAvzg
   Ta video ponuja praktične nasvete za ustvarjanje močnih in zapomnljivih gesel. Poudarja pomembnost uporabe kombinacije črk, številk in simbolov, izogibanja pogostim napakam in upoštevanja gesel kot varne alternative.
6) **TechRadar – Virtualne zasebne mreže (VPN)**
   Spletna stran: https://www.techradar.com/vpn/virtual-private-networks
   Ta izčrpen vodnik TechRadar raziskuje koncept virtualnih zasebnih omrežij (VPN). Pojasnjuje, kako delujejo VPN, njihove prednosti za zasebnost in varnost na spletu, ter ponuja priporočila za najboljše storitve VPN na podlagi strokovnih testiranj.

4.5 Modul III – Predhodni/naknadni test

1. Kaj pomeni „HTTPS“ v naslovu spletnega mesta?

A) Spletno mesto je gostovano v drugi državi
B) Spletna stran je varna in podatki so šifrirani
C) Spletna stran ponuja popuste
D) Spletna stran zahteva prijavo

2. Zakaj je pomembno uporabljati dvofaktorsko avtentikacijo (2FA) za spletno bančništvo?

A) Pospeši spletne transakcije
B) Omogoča prijavo z več naprav hkrati
C) Zagotavlja dodatno raven varnosti, saj zahteva dva koraka preverjanja
D) Nadomesti potrebo po geslu

3. Kakšna je glavna prednost uporabe protivirusne programske opreme?

A) Pospeši delovanje računalnika
B) Ščiti pred zlonamerno programsko opremo in napadi phishinga
C) Pomaga pri upravljanju spletnih gesel
D) Blokira dostop do vseh spletnih trgovin

4. Katero od naslednjih gesel je najvarnejše?

A) Nakupovanje2024
B) 12345678
C) Mybankpassword
D) H@ppy$hopper92!

5. Kaj naj storite, če vidite spletno ponudbo, ki izgleda „preveč dobra, da bi bila resnična“?

A) Takoj jo delite s prijatelji
B) Kliknite na povezavo, da preverite podrobnosti
C) Se ji izognite in preverite spletno stran, preden ukrepate
D) Hitro posredujte svoje podatke, da izkoristite ponudbo

6. Kateri način plačila je varen za spletno nakupovanje?

A) Plačilo s kreditno kartico na varni spletni strani
B) Pošiljanje denarja z neposrednim bančnim nakazilom
C) Posredovanje številke kartice po e-pošti
D) Uporaba katere koli metode, če spletna stran izgleda profesionalno

7. Zakaj se je treba izogibati uporabi javnega Wi-Fi-ja za finančne transakcije?

A) Prepočasen je za spletno bančništvo
B) Lahko je nešifriran in omogoča hekerjem, da ukradejo vaše podatke
C) Ne podpira varnih spletnih strani
D) Blokira dostop do bančnih aplikacij

8. Kaj pomeni ikona ključavnice v naslovni vrstici brskalnika?

A) Spletna stran je v vzdrževanju
B) Povezava med vašo napravo in spletnim mestom je varna
C) Spletna stran zahteva piškotke
D) Spletna stran ni zanesljiva

9. Kako lahko prepoznate zanesljivo spletno trgovino?

A) Po e-pošti zahteva vaše geslo
B) Vsebuje pravopisne napake in nejasne kontaktne podatke
C) Ima HTTPS, ikono ključavnice in preverjene ocene strank
D) Ponuja brezplačne izdelke brez plačila

10. Kaj morate storiti, da zaščitite svojo napravo in finančne podatke?

A) Onemogočite protivirusno programsko opremo, da bo vaš računalnik deloval hitreje
B) Poskrbite, da je vaša programska oprema posodobljena, in uporabljajte VPN v javnih omrežjih
C) Izogibajte se preverjanju zgodovine transakcij
D) Uporabljajte isto geslo za vse svoje račune

Povzetek odgovorov

1-B, 2-C, 3-B, 4-D, 6-A, 7-B, 8-B, 9-C

MODUL IV

Varna in odgovorna raba družbenih omrežij za starejše

5. Modul IV Varno in odgovorno uporabljanje družbenih medijev za starejše

Modul „Varno uporabljanje družbenih medijev“ starejšim predstavlja odgovorno in varno uporabo platform družbenih medijev, pri čemer združuje osnovno znanje s praktičnimi nasveti. Udeleženci se naučijo, kako nastaviti in upravljati račune, prilagoditi nastavitve zasebnosti, prepoznati pogoste spletne prevare in varno komunicirati, kar jim omogoča, da z večjo samozavestjo in nadzorom sodelujejo v digitalnih družbenih prostorih.

Modul vključuje praktične dejavnosti, ki udeležencem pomagajo prepoznati sumljiva sporočila, lažne profile in zavajajoče povezave, ki so pogoste v družbenih medijih. Osredotoča se tudi na zaščito osebnih podatkov in digitalne identitete z učinkovitim upravljanjem zasebnosti, omejenim deljenjem podatkov in varnimi praksami za račune, kot so močna gesla in dvofaktorska avtentikacija. Na voljo so tudi navodila o varnosti naprav, posodobitvah programske opreme in varnih internetnih povezavah.

Z integracijo teh elementov modul zagotavlja, da starejši ne le razumejo tveganja, povezana z družbenimi omrežji, ampak tudi razvijejo praktične spretnosti za njihovo učinkovito obvladovanje. Udeleženci modul zaključijo z večjo digitalno ozaveščenostjo, samozavestjo in sposobnostjo uporabe varnih praks na družbenih omrežjih v vsakdanjih spletnih interakcijah.

5.1 Cilji učenja

Cilj tega modula je izboljšati razumevanje in veščine starejših za varno, odgovorno in smiselno uporabo družbenih medijev. S tem usposabljanjem bodo starejši, stari 65 let in več:

- Pridobili samozavest pri uporabi priljubljenih platform družbenih medijev.
- razumeli pomen nastavitev zasebnosti in se naučili, kako jih učinkovito prilagoditi
- prepoznali in se izognili pogostim spletnim prevaram in grožnjam na družbenih omrežjih
- razvili navade za varno in odgovorno deljenje osebnih podatkov na spletu
- odgovorno sodelovali z vsebinami družbenih medijev, hkrati pa zagotovili svojo varnost in dobro počutje.

5.2 Struktura, vsebina in učni izidi

Po uspešnem zaključku tega modula bodo udeleženci sposobni:

- Prepoznati ključne značilnosti in uporabo priljubljenih platform, kot so Facebook, Instagram in LinkedIn.
- Prikazati sposobnost ustvarjanja računov v družbenih medijih z uporabo varnih metod, kot so izbira močnih gesel in omogočanje dvofaktorskega preverjanja pristnosti.
- Prilagoditi nastavitve zasebnosti za nadzor vidnosti osebnih podatkov in objav.
- Upravljati nastavitve stikov, da omejijo neželena sporočila in zahteve za povezavo.
- Prepoznati opozorilne znake prevar, kot so phishing, lažni profili in lažne povezave.
- Izvajajte strategije za zaščito občutljivih osebnih podatkov pred zlonamernimi akterji.
- Preglejte in spremenite prej deljene vsebine, da bodo v skladu z najboljšimi praksami za varnost na spletu.
- Razvijte navade za varno deljenje informacij, vključno z izogibanjem pretiranemu deljenju ali deljenju občutljivih vsebin.

5.3 Dnevni red I Podroben načrt seje

MODUL IV
Varno in odgovorno uporabljanje družbenih medijev za starejše

1. seja

Dobrodošli
Trajanje 5

Cilji

- Predstavite temo in ustvarite prijetno vzdušje.

Vsebina/metoda

- Kratek uvod v sejo, opis ciljev in postavitev pričakovanj
- Pripravite teren za usposabljanje s predstavitvijo modula in njegovega pomena.

Material

- Tabla ali flipchart za cilje seje.
- Flomasterji.
- Natisnjena agenda ali predstavitvene diapozitive, ki opisujejo sejo.

2. seja

Dejavnost za spoznavanje: Bingo na družbenih omrežjih
Trajanje 5

Cilji učenja

- Spodbuditi udeležence k interakciji in razmišljanju o svojih digitalnih navadah.

Vsebina/metoda

- Udeleženci se predstavijo in označijo izraze, ki jih poznajo. Prvi udeleženec, ki izpolni vrstico na svoji bingo kartici, prejme majhno nagrado. To udeležence spodbudi, da delijo svoje izkušnje z družbenimi mediji in sproži pogovor o njihovih digitalnih navadah.

Material

- Natisnite kartice z običajnimi izrazi iz družbenih medijev, kot so »Facebook«, »Instagram«, »Všeč mi je«, »Hashtag«, »Komentar«, »Sledi«, »Profil« itd.
- Pisala in svinčniki, označevalci in/ali nalepke

3·seja

Predavanje 1: Pregled družbenih omrežij
Trajanje *30*

Cilji

- Udeležencem pomagati razumeti ključne funkcije in vrste platform družbenih medijev.

Vsebina/metoda

- Predstavite pregled priljubljenih platform (Facebook, Instagram, Twitter itd.) in pojasnite njihove osnovne značilnosti in funkcije. Pojasnite njihove značilnosti, prednosti in potencialna tveganja ter kako varno ustvariti račun.

Material

- Prezentacijske diapozitive, ki zajemajo priljubljene platforme družbenih medijev, njihove značilnosti in varnostna tveganja.
- Projektor in prenosni računalnik za predstavitev.
- Letaki s povzetkom značilnosti in varnostnih nasvetov za Facebook, Instagram in Twitter.
- Internetna povezava za predstavitev funkcij platform v živo.

Dejavnost 1: Seznanjanje s platformo
Trajanje 20 minut

Cilji učenja

- Udeležence seznaniti z navigacijo po platformah družbenih medijev.

Vsebina/metoda

- Praktično spoznavanje platform (npr. Facebook, Instagram, Twitter). Udeleženci se bodo naučili ustvariti račun na družbenih omrežjih s poudarkom na varnosti (npr. izbira močnih gesel, omogočanje dvofaktorske avtentikacije).

Material

- Računalniki, tablični računalniki ali pametni telefoni, s katerimi bodo udeleženci raziskovali platforme.
- Tiskani vodniki za varno ustvarjanje računov, vključno z: *navodili za ustvarjanje močnih gesel. Koraki za omogočanje dvofaktorskega preverjanja pristnosti.*

Odmor | Trajanje *5'*

- **Udeležencem omogočite čas za počitek in razmislek.**
- **Kratek odmor za osvežitev.**

4. Srečanje

Predavanje 2: Nastavitve zasebnosti
Trajanje *30*

Cilji

- Udeležencem posredovati znanje za prilagajanje nastavitev zasebnosti in zaščito osebnih podatkov.

Vsebina/metoda

- Naučiti, kako prilagoditi nastavitve zasebnosti na platformah družbenih medijev za zaščito osebnih podatkov.

Material

- Predstavitvene diapozitive, ki pojasnjujejo nastavitve zasebnosti za pogoste platforme.
- Tiskani priročniki s podrobnimi navodili za prilagajanje nastavitev zasebnosti za Facebook, Instagram in Twitter.
- Projektor in prenosni računalnik za prikaz nastavitev zasebnosti v živo.

Dejavnost 2: Prilagajanje nastavitev zasebnosti
Trajanje *20*

Cilji učenja

- Udeležence naučite, kako nastaviti nastavitve zasebnosti na platformah družbenih medijev.

Vsebina/metoda

- Interaktivna vaja, v kateri udeleženci prilagodijo nastavitve zasebnosti na svojih računih v družbenih medijih.

Material

- Računalniki, tablični računalniki ali pametni telefoni za praktično vajo.
- Vnaprej ustvarjeni lažni računi (neobvezno) za udeležence, ki nimajo osebnih računov.
- Natisnjene delovne liste z prostorom za zapisovanje spremenjenih nastavitev zasebnosti.

Odmor | Trajanje *5 minut*

- **Čas za počitek in pripravo na naslednjo sejo.**
- **Kratek odmor za osvežitev.**

Predavanje 3: Prepoznavanje prevar in spletnih groženj na družbenih omrežjih
Trajanje *30 minut*

Cilji

- Udeležencem pomagati prepoznati prevare in grožnje, značilne za družbena omrežja.

Vsebina/metoda

- Razprava o pogostih prevarah v družbenih medijih, vključno z lažnim ribarjenjem, lažnimi oglasi, lažnimi profili in krajo identitete.

Material

- Predstavitvene diapozitive s primeri prevar, kot so lažna elektronska sporočila in lažne zahteve za prijateljstvo.
- Tiskane brošure s podrobnimi informacijami o pogostih prevarah in opozorilnih znakih, na katere je treba biti pozoren.
- Projektor in prenosni računalnik za prikazovanje primerov ali videoposnetkov prevar v družbenih medijih.

Dejavnost 3: Vaja za prepoznavanje prevar
Trajanje 20

Cilji učenja

- Razviti sposobnost prepoznavanja prevar v družbenih medijih in naučiti se, kako se izogniti padcu v prevarantske sheme.

Vsebina/metoda

- Skupinska dejavnost, v kateri udeleženci prepoznajo in razpravljajo o primerih prevar v družbenih medijih, kot so lažne prijateljske zahteve ali lažna sporočila.

Material

- Kartice s scenariji z zgledi prevar za skupinsko razpravo.
- Flipchart ali tabla za zapisovanje ugotovitev skupine.
- Flomasterji za zapisovanje odgovorov udeležencev.

Odmor | Trajanje 5 minut

- **Omogočite čas za počitek in pripravo.**
- **Kratek odmor za osvežitev.**

6. seja

Predavanje 4: Varno in odgovorno sodelovanje v družbenih medijih
Trajanje *30*

Cilji

- Pojasniti pomen varne in odgovorne uporabe družbenih medijev
- Učence naučiti, kako razviti varne navade pri deljenju vsebin.

Vsebina/metoda

- Predstavitev *»Zakaj je varnost na spletu pomembna za posameznike in strokovnjake?«*. Primeri potencialnih tveganj zaradi nevarnih navad pri deljenju (npr. kraja identitete, škoda ugledu). Učencem predstavite hipotetične scenarije (npr. deljenje načrtov za počitnice ali poklicnih dosežkov). Vprašajte: *»Kaj bi delili? Kako bi to delili na varen način?«*. Skupinska razprava o odgovorih.

Material

- Diapozitivi s statističnimi podatki o tveganjih na spletu.
- Infografika, ki povzema ključna tveganja in posledice nevarnih praks.

Dejavnost 4: Pregled preteklih objav in informacij
Trajanje *20*

Cilji

- Omogočiti udeležencem, da ocenijo in spremenijo svoje profile in objave v družbenih medijih zaradi varnosti.

Vsebina/metoda

- Vodena revizija vzorčnega profila na družbenih omrežjih (izmišljen ali anonimiziran primer). Prepoznavanje nevarnih ali preveč osebnih vsebin (npr. telefonske številke, lokacije, občutljive fotografije). Prikaz, kako izbrisati ali spremeniti objave in prilagoditi nastavitve zasebnosti.

Material

- Primer profila v družbenih medijih (natisnjen ali na zaslonu).
- Podrobna navodila za prilagajanje nastavitev zasebnosti (PDF ali gradivo).

7. Srečanje

Razprava | Trajanje 10’

Cilji učenja

- Spodbujati proaktivno miselnost pri prepoznavanju in prijavljanju sumljivih dejavnosti na družbenih omrežjih.

Vsebina/metoda

- Skupinska razprava o tem, kako ravnati v primeru sumljivih dejavnosti na družbenih omrežjih, na primer kako prijaviti prevare in prepoznati lažne račune.

Material

- Tabla in flomasterji za brainstorming o načinih prijavljanja prevar in ravnanja s sumljivimi računi.
- Tiskani viri s kontaktnimi podatki za prijavljanje prevar (npr. povezave do centrov za pomoč platform).

Zaključek | Trajanje 5 minut

Cilji učenja

- Povzemite usposabljanje in se prepričajte, da udeleženci razumejo, kako se zaščititi pred grožnjami v družbenih medijih.

Vsebina/metoda

- Preglejte ključne točke o prevarah in grožnjah v družbenih medijih, odgovorite na morebitna vprašanja in zagotovite vire za nadaljnje učenje.

Gradivo

- Gradivo, ki povzema ključne točke, obravnavane v okviru seje: ***Seznam za preverjanje varnosti v družbenih medijih***

5.4 Dodatne informacije

5.4.1 Samorefleksija izobraževalcev

- Ali sem učinkovito posredoval pomen varnosti na spletu in sodelovanja v družbenih medijih?
- Ali sem zagotovil, da so udeleženci razumeli tehnične vidike nastavitev zasebnosti in prepoznavanja prevar?
- Kako sem udeležence vključil v dejavnosti in razprave?
- So bili viri in materiali koristni za udeležence?

5.4.2 Ocena programa s strani izobraževalcev

- Ali je vsebina usposabljanja ustrezna in jasna za starejše?
- Ali so dejavnosti in razprave učinkovito pomagale udeležencem pri učenju snovi?
- Ali so rezultati v skladu z učnimi cilji modula?

5.4.3 Gradivo, dodatni viri

Priloga 1 | Dejavnost za spoznavanje: Bingo na družbenih omrežjih

Kartica za bingo na družbenih omrežjih – A

Všeč	Komentar	Facebook	Zgodba	Oznaka
Selfie	Sporočilo	Instagram	Oznaka	Profil
Emoji	Sledilci	BREZPLAČNO	Tweet	Del
Video	Zasebnost	LinkedIn	Status	Objava
Časovnica	Obvestilo	Twitter	Skupina	Reels

Kartica za bingo v družbenih medijih – B

Oznaka	Objava	Instagram	Zgodba	Zasebnost
Sporočilo	Facebook	Časovnica	Všeč	Skupina
Reels	Oznaka	BREZPLAČNO	Status	Komentar
Tweet	Del	LinkedIn	Video	Selfie
Sledilci	Obvestilo	Profil	Emoji	Blokiraj

Kartica za bingo v družbenih medijih – C

Status	Všeč	LinkedIn	Selfie	Del
Facebook	Emoji	Instagram	Tweet	Reels
Sporočilo	Zasebnost	BREZPLAČNO	Skupina	Zgodba
Časovnica	Oznaka	Obvestilo	Objava	Oznaka
Blokiraj	Sledilec	Video	Komentar	Profil

Dodatek 2 I Predavanje 1: Pregled družbenih medijev

Slike za predstavitev:

- **Facebook:** „To je najbolj razširjena platforma za ohranjanje stikov s prijatelji in družino. Na njej lahko delite fotografije, komentirate novice, se pridružite interesnim skupinam in še več.“
- **Instagram:** „Ta platforma se osredotoča na fotografije in videoposnetke. Odlična je za vizualno deljenje trenutkov, saj ponuja funkcije, kot je „Stories“, ki izginejo po 24 urah.“
- **LinkedIn:** „To si predstavljajte kot svoj profesionalni življenjepis na spletu. Je koristen za iskanje zaposlitve in mreženje, čeprav ga starejši ljudje ne uporabljajo pogosto, razen če so še aktivni na trgu dela.“
- **Twitter:** „Tukaj uporabniki objavljajo kratka besedilna sporočila, imenovana tweets. Uporablja se predvsem za spremljanje novic in javnih osebnosti.“

Primerjava platform družbenih medijev

Kategorija	Facebook	Instagram	LinkedIn	Twitter	Twitter (podvojen stolpec)
Namen	Povezovanje s prijatelji in družino	Deljenje fotografij in kratkih videoposnetkov	Strokovno mreženje	Deljenje kratkih novic	Deljenje kratkih novic
Vrste objav	Besedilo, fotografije, videoposnetki, povezave, zgodbe	Fotografije, videi, posnetki, zgodbe	Novice o delovnih mestih, članki, življenjepisi	Tviti (besedilo), fotografije, videi	Javno, sledilci
Komentarji in reakcije	Prijatelji, skupine, javnost	Sledilci, javnost	Poklicni stiki	Všečki, komentarji	Všečki, komentarji
Sporočila	Aplikacija Messenger	Všečki, komentarji	Všečki, komentarji	Všečki, komentarji, retweeti	Všečki, retweeti
Nastavitve zasebnosti	Prilagodljive: javne, prijatelji, skupine	Omejeno, večinoma javno, razen če je zasebno	Privzeto bolj javno	Večinoma javno, omejen nadzor	Javno ime in objave privzeto
Vidnost profila	Nastavljivo: ime, fotografije, biografija	Omejen nadzor, razen pri zasebnem računu	Javno, razen če ni privzeto prilagojeno	Javno ime in prilagojeno	Javno ime in objave privzeto
Pogosta tveganja	Lažni računi, pretirano deljenje, prevare	Prevare v zasebnih sporočilih, prevzemanje identitete	Phishing sporočila, prevzemanje identitete	Nadlegovanje, lažne povezave, prevzemanje identitete	Nadlegovanje, lažne povezave, prevzemanje identitete
Primerno za	✓	✓	✓	✓	✓

Dodatek 3 | Aktivnost 1: Seznanjanje s platformo

Vodja skupine vodi skupino korak za korakom:

„Odprite internetni brskalnik in obiščite www.facebook.com ali www.instagram.com.“

„Kliknite na ‚Ustvari nov račun‘ in vnesite svoje podatke – ime, datum rojstva itd.“

„Ko vas prosi, da izberete geslo, poskrbite, da je geslo močno. Dobro geslo ima vsaj 8 znakov, vsebuje kombinacijo črk in številk ter simbol.“

Vodja dodaja:

„Namesto ‚maria123‘ lahko na primer uporabite ‚Maria!74books‘.“

„Sedaj omogočimo dvofaktorsko avtentikacijo – dvofaktorska avtentikacija (2FA) dodaja dodatno raven varnosti. Po vnosu gesla boste morali vnesti kodo, ki bo poslana na vaš mobilni telefon ali e-pošto.“

Priloga 4 | Seznam za preverjanje nastavitev računa, Seznam za preverjanje nastavitev računa

1. Izberite platformo (Facebook, Instagram itd.)
2. Obiščite uradno spletno stran ali prenesite uradno aplikacijo.
3. Kliknite na »Ustvari nov račun«.
4. Vnesite svoje pravo ime in datum rojstva.
5. Uporabite močno in edinstveno geslo (glejte gradivo 2).
6. Vnesite svojo mobilno telefonsko številko ali e-poštni naslov.
7. Omogočite dvofaktorsko avtentikacijo.
8. Preskočite nepotrebne osebne podatke (kot je vaš naslov).
9. Takoj po ustvarjanju računa preglejte nastavitve zasebnosti.
10. Odjavite se, ko uporabljate javno ali skupno napravo.

Seznam za preverjanje nastavitev računa

Močno geslo mora:

- biti dolgo vsaj 8 znakov
- Vsebovati mešanico velikih in malih črk.
- Vsebovati vsaj eno številko in en posebni znak (npr. !, @, #, $).
- Izogibati se uporabi pogostih besed ali informacij, ki jih je mogoče zlahka uganiti (kot so vaše ime ali rojstni dan).
- Biti edinstveno za vsak račun, ki ga ustvarite.

Primer šibkega gesla: maria123
Primer močnega gesla: M@r!a74Books

Priloga 5 | Predavanje 2: Nastavitve zasebnosti

Seznam za preverjanje zasebnosti v družbenih medijih

[ ] Ste pregledali nastavitve vidnosti svojega profila?

[ ] Ali so vaši prispevki omejeni samo na »prijatelje« ali »sledilce«?

[ ] Ali ste na vseh platformah omogočili dvofaktorsko avtentikacijo?

[ ] Se izogibate deljenju svoje telefonske številke, domačega naslova ali celotnega datuma rojstva?

[ ] Ali ste preverili, kdo vam lahko pošilja sporočila ali zahteve za prijateljstvo?

[ ] Preverite označene fotografije in objave, preden se pojavijo na vašem profilu?

[ ] Ste previdni pri sprejemanju novih zahtev za prijateljstvo ali sledilce?

[ ] Ali ste izbrisali stare objave, ki vsebujejo občutljive podatke?

[ ] Redno preverjate nastavitve zasebnosti?

[ ] Ali veste, kam lahko prijavite prevare in zlorabe na posamezni platformi?

Vodnik po nastavitvah zasebnosti

Povezave in navodila za prilagajanje nastavitev zasebnosti na priljubljenih platformah:

1. Facebook:

- Pojdite na orodje za preverjanje zasebnosti: https://www.facebook.com/privacy/checkup
- Center za zasebnost: https://www.facebook.com/privacy/center
- Prilagodite, kdo lahko vidi vaše objave, kdo vam lahko pošilja zahteve za prijateljstvo in kdo vas lahko poišče.

2. Instagram:

- Pojdite na Center za varnost: https://help.instagram.com/196883487377501
- Kako nastaviti svoj Instagram račun na zaseben: https://help.instagram.com/448523408565555
- Nastavite svoj račun na zasebno, upravljajte komentarje in nadzorujte oznake.

3. LinkedIn:

- Pojdite na Pregled nastavitev zasebnosti: https://www.linkedin.com/help/linkedin/answer/66
- Upravljajte nastavitve javnega profila LinkedIn: https://www.linkedin.com/help/linkedin/answer/83
- Izberite, kdo lahko vidi vaše povezave, podrobnosti profila in dejavnosti.

4. Twitter (X):

- Pojdite na Varnostne nastavitve: https://help.twitter.com/en/safety-and-security/twitter-privacy-settings
- Varnost in dostop do računa: https://help.twitter.com/en/managing-your-account/accessing-your-twitter-data
- Zaščitite svoje tvite, omejite, kdo vam lahko pošilja sporočila ali vas omenja, in nadzorujte odkritost.

Priloga 6 | Aktivnost 2: Prilagajanje nastavitev zasebnosti

Delovni list za prilagajanje zasebnosti

Uporabite ta delovni list za spremljanje sprememb, ki jih naredite v nastavitvah zasebnosti na družbenih omrežjih. Po pregledu svojega računa navedite podrobnosti o spremembah, ki ste jih naredili, in razloge zanje.

1.

Prilagojena nastavitev _____

Nova vrednost/možnost _____

Razlog za spremembo _____

2.

Prilagojena nastavitev _____

Nova vrednost/možnost _____

Razlog za spremembo _____

3.

Prilagojena nastavitev _____

Nova vrednost/možnost _____

Razlog za spremembo _____

4.

Prilagojena nastavitev _____

Nova vrednost/možnost _____

Razlog za spremembo _____

5.

Prilagojena nastavitev _____

Nova vrednost/možnost _____

Razlog za spremembo _____

Priloga 7| Predavanje 3: Prepoznavanje prevar in spletnih groženj na družbenih omrežjih

Ključne ugotovitve o najpogostejših prevarah:

- **Phishing:** *„To so lažna sporočila, ki vas skušajo prevarati, da bi jim posredovali svoje osebne podatke. Na primer, sporočilo z besedilom: ‚Osvojili ste nagrado! Kliknite tukaj, da jo prevzamete.'"*
- **Lažne zahteve za prijateljstvo:** *„Lahko prejmete zahtevo od nekoga, ki se izdaja za vašega bratranca ali soseda – vedno preverite."*
- **Sumljive povezave:** *»Te lahko okužijo vašo napravo ali ukradejo vaše gesla. Če se povezava zdi sumljiva ali je niste pričakovali, ne klikajte nanjo.«*
- **Prevare z lažno identiteto in romantične prevare:** *»Nekateri ljudje lahko začnejo prijateljstvo ali romantičen pogovor samo zato, da vas kasneje prosijo za denar.«*
- **Lažne identitete***: „Prevaranti ustvarijo lažne profile na spletu, da vzpostavijo zaupanje in manipulirajo žrtve, da jim dajo denar ali osebne podatke."*

Priloga 8| Priročnik za prepoznavanje prevar

Naučite se prepoznati pogoste prevare na družbenih omrežjih:

1. Phishing sporočila:

- Pazite na nujne zahteve, kot je „Vaš račun bo blokiran!"
- Preverite e-poštni naslov ali uporabniško ime pošiljatelja – ali se vam zdi sumljivo?

2. Lažne zahteve za prijateljstvo:

- Bodite previdni pri ljudeh, ki jih ne poznate.
- Bodite pozorni na podvojene profile, ki se izdajajo za nekoga, ki ga poznate.

3. Prevare z nagradami ali loterijami:

- Sporočila »Zmagali ste!« so skoraj vedno prevare.
- Nikoli ne posredujte svojih bančnih podatkov ali plačujte za prevzem nagrade.

4. Prevare v zvezi z ljubeznijo ali prijateljstvom:

- Prevaranti lahko najprej vzpostavijo zaupanje, nato pa prosijo za denar.
- Bodite previdni, če nekdo postane prehitro preveč oseben.

5. Sumljive povezave:

- Ne klikajte na neznane povezave, zlasti tiste, ki so poslane v zasebnih sporočilih.
- Vedno dvakrat preverite in prijavite sumljive dejavnosti.

Priloga 9| Nasveti za varnost na družbenih omrežjih

Upoštevajte naslednje pomembne nasvete za varno uporabo družbenih omrežij:

- Nastavite svoj profil na zaseben in nadzorujte, kdo lahko vidi vaše objave.
- Uporabljajte močna, edinstvena gesla za vsak račun.
- Za dodatno varnost vklopite dvofaktorsko avtentikacijo.
- Ne sprejemajte zahtev za prijateljstvo od neznancev.
- Bodite pozorni na to, kar objavljate – ne delite potovalnih načrtov ali osebnih podatkov.
- Odjavite se, ko uporabljate javne ali skupne naprave.
- Prijavite vse sumljivo, vključno z goljufijami in lažnimi računi.
- Posodabljajte svoje aplikacije, da boste zaščiteni pred novimi grožnjami.
- Premislite, preden kliknete na povezave ali prenesete datoteke.
- Če ste v dvomih, se posvetujte z osebo, ki ji zaupate, ali prijavite problem.

Bodite obveščeni. Bodite varni.

Priloga 10 | Aktivnost 3: Vaja za prepoznavanje prevar

Scenarij 1: Zmaga!

Prejeli ste sporočilo z neznanega računa, ki pravi:
„Čestitamo! Osvojili ste nov pametni telefon! Kliknite na spodnjo povezavo, da prevzamete nagrado.“
Sporočilo vsebuje povezavo in vas prosi, da vnesete svoje osebne podatke.

Scenarij 2: Prijatelj v težavah

Na Facebook Messengerju prejmete sporočilo od prijatelja, s katerim se že nekaj časa niste pogovarjali. Piše, da je obtičal v tujini in da mu morate takoj poslati 500 EUR.

Prosi vas za vašo telefonsko številko in bančne podatke.

Scenarij 3: Opozorilo banke

Račun, ki trdi, da je vaša banka, vam pošlje neposredno sporočilo na Instagramu:
„Zaznali smo sumljivo aktivnost na vašem računu. Nemudoma potrdite svoje podatke za prijavo, tako da odgovorite tukaj.“
Profil računa ima kot sliko logotip banke.

Scenarij 4: Zaposlitvena priložnost

Na LinkedIn prejmete zahtevo za povezavo od nekoga, ki trdi, da je kadrovik. Ponujajo vam delo na daljavo z visoko plačo in fleksibilnim delovnim časom.
Ko sprejmete, vas prosi za vaš življenjepis, fotografijo osebne izkaznice in številko socialnega zavarovanja.

Scenarij 5: Lokalna skupnost

Povabljeni ste, da se pridružite Facebook skupini za lokalne upokojence. Skupina deli nasvete za zdravje, novice o dogodkih in novice iz skupnosti. Člani so prijazni in nihče ne prosi za osebne podatke.

Priloga 11 | Predavanje 4: Varno in odgovorno sodelovanje v družbenih medijih

Smernice za varno deljenje

Uporabite naslednja navodila za odgovorno deljenje na družbenih omrežjih:

- Premislite, preden objavite: bi vam bilo všeč, če bi to videl neznanec?
- Izogibajte se deljenju svoje natančne lokacije, še posebej v realnem času.
- Ne objavljajte dolgih potovanj ali kdaj bo vaš dom prazen.
- Nikoli ne objavljajte osebnih dokumentov, kot so osebne izkaznice, vozovnice ali bančne podatke.
- Bodite previdni pri deljenju fotografij otrok – po potrebi pridobite dovoljenje.
- Uporabite nastavitve zasebnosti, da nadzirate, kdo vidi vaše objave.
- Izogibajte se deljenju občutljivih tem v javnih objavah.
- Ne delite vsebin, ko ste čustveno razburjeni – najprej se ustavite in razmislite.
- Za osebne pogovore uporabljajte zasebna sporočila namesto javnih komentarjev.
- Redno pregledujte svoje pretekle objave in izbrišite vse, kar se vam zdi nevarno.

Ne pozabite: ko je nekaj enkrat na spletu, je težko to umakniti.

Priloga 12 | Aktivnost 4: Pregled preteklih objav in informacij

Vodja usposabljanja reče:
„Sedaj bomo odprli vaše račune na družbenih omrežjih in pregledali pretekle objave ali fotografije. To je vaja, imenovana ‚digitalno čiščenje'."

Vodja usposabljanja navaja korake:

- *„Pojdite na svoj profil ali časovnico."*
- *„Preglejte 3–5 starejših objav. Vprašajte se: Ali bi to danes delili? Ali razkriva zasebne informacije?"*
- *„Če je odgovor da, ga izbrišite ali uredite. Pokazal vam bom, kako."*

Trener pokaže na zaslonu ali projektorju:

- *Kako izbrisati objavo na Facebooku*
- *Kako se odstraniti iz označb na fotografijah*
- *Kako spremeniti vidnost iz „Javno" v „Prijatelji"*

Priloga 13 | Seznam za preverjanje varnosti profila

Uporabite ta kontrolni seznam, da preverite varnost svojega profila v družbenih medijih:

[ ] Ali je vaša profilna slika primerna in ne omogoča identifikacije (brez osebnih podatkov, kot je naslov doma v ozadju)?

[ ] Ali ste iz svojega profila odstranili ali skriti datum rojstva, telefonsko številko ali domači naslov?

[ ] Ali so tvoje objave nastavljene na „Samo prijatelji“ ali „Zasebno“ namesto na „Javno“?

[ ] Ste preverili, kdo lahko komentira ali deli vaše objave?

[ ] Ste preverili, kdo vam lahko pošilja zahteve za prijateljstvo/sledenje?

[ ] Ali za svoj račun uporabljate močno, edinstveno geslo?

[ ] Ali je omogočena dvofaktorska avtentikacija?

[ ] Redno pregledujete objave in izbrišete vse, kar je zastarelo ali nevarno?

[ ] Ali ste v svojih objavah izklopili deljenje lokacije?

[ ] Preverjate objave, v katerih ste označeni, preden se pojavijo na vaši časovnici?

Ta seznam preverite vsakih nekaj mesecev, da bo vaš profil varen.

Priloga 14 | Seznam za varnost na družbenih omrežjih

[ ] Uporabljajte močna, edinstvena gesla za vsak račun

[ ] Omogočite dvofaktorsko avtentikacijo

[ ] Redno pregledujte in prilagajajte nastavitve zasebnosti

[ ] Bodite pozorni na osebne podatke, ki jih delite javno

[ ] Premislite, preden sprejmete zahteve za prijateljstvo ali sledenje

[ ] Bodite pozorni na prevare, phishing in sumljiva sporočila

[ ] Bodite previdni pri klikanju na povezave ali prenašanju vsebin

[ ] Prijavite in blokirajte sumljive ali žaljive uporabnike

[ ] Omejite deljenje lokacije in geografsko označevanje

[ ] Poskrbite, da so vaše aplikacije in naprave posodobljene

Priloga 15| Priporočila za nadaljnje branje in učenje za udeležence

Spletne strani o kibernetski varnosti: Evropske in vladne organizacije, ki se ukvarjajo s kibernetsko varnostjo

1) **ENISA (Agencija Evropske unije za kibernetsko varnost)**

   Spletna stran: https://www.enisa.europa.eu/

   ENISA je agencija EU, odgovorna za kibernetsko varnost. Objavlja poročila, vodnike in opozorila o kibernetskih grožnjah ter daje praktične nasvete državljanom in organizacijam.

2) **CERT-EU (skupina za odzivanje na računalniške izredne dogodke za institucije EU)**

   Spletna stran: https://cert.europa.eu/

   CERT-EU spremlja kibernetske grožnje in se odziva na kibernetske napade, usmerjene v evropske institucije. Ponuja tudi opozorila in najboljše prakse, ki jih lahko uporabljajo izobraževalci in končni uporabniki.

3) **EC3 – Europolov center za kiberkriminaliteto**

   Spletna stran: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

   EC3 Europola zagotavlja informacije o spletnih prevarah, goljufijah in drugih oblikah kibernetske kriminalitete. Objavlja gradivo za ozaveščanje in študije primerov, ki so pomembni za prepoznavanje tveganj na družbenih medijih.

4) **Stay Safe Online – Nacionalna zveza za kibernetsko varnost (ZDA)**

   Spletna stran: https://staysafeonline.org/

   Center virov s preprostimi kontrolnimi seznami in kampanjami o zasebnosti, varnosti gesel, lažnem predstavljanju in ozaveščanju o družbenih medijih.

5) **Mreža AARP Fraud Watch**

   Spletna stran: https://www.aarp.org/money/scams-fraud/

   Dostopna pobuda s sedežem v ZDA, ki ponuja najnovejše informacije o prevarah, ki so posebej usmerjene v starejše odrasle osebe, ter nasvete za preprečevanje in prijavo.

6) **NCSC UK – Smernice za družbene medije**

   Spletna stran: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/social-media

7) **NCSC UK – Navodila za gesla**

   Spletna stran: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/passwords

8) **Pomoč LinkedIn – Nastavitve zasebnosti**

   Spletna stran: https://www.linkedin.com/help/linkedin/answer/66

5.5 Modul IV – Predhodni/naknadni test

1. Kaj vključujejo „osebni podatki“?

A) Samo vaše objave na družbenih omrežjih
B) Vse informacije, ki vas lahko identificirajo, na primer vaše ime ali identifikacijska številka
C) Samo podatke o vašem bančnem računu
D) Samo vaša spletna gesla

2. Zakaj je pomembno prebrati politike zasebnosti?

A) Vsebujejo šale o varnosti podatkov
B) Pojasnjujejo, kako se bodo vaši podatki zbirali in uporabljali
C) Pomagajo, da vaša naprava deluje hitreje
D) So zakonsko obvezne, vendar nepomembne

3. Kateri od naslednjih primerov je primer občutljivih osebnih podatkov?

A) Najljubša barva
B) Naslov
C) Zdravstvena zgodovina ali biometrični podatki
D) Nakupovalne navade

4. Katera je najboljša praksa pri deljenju fotografij ali informacij na spletu?

A) Deliti vse osebne podatke, da bi bili odprti in družabni
B) Preverite, kdo lahko vidi informacije, preden jih objavite
C) Pogosto objavljajte, da ostajate vidni
D) Vedno navajajte svojo lokacijo

5. Kaj pomeni „šifriranje podatkov”?

A) Skrivanje datotek v skrivni mapi
B) Pretvorba informacij v kodo, da se zaščitijo pred nepooblaščenim dostopom
C) Shranjevanje datotek na pomnilniški ključ
D) Izbris vseh starih podatkov

6. Zakaj bi morali omejiti količino informacij, ki jih delite na družbenih omrežjih?

A) Prihrani internetne podatke
B) Zmanjša tveganje za krajo identitete in goljufije
C) Poveča število sledilcev
D) Preprečuje drugim, da bi komentirali

7. Kaj morate storiti, preden aplikaciji dodelite dostop do svojih osebnih podatkov?

A) Takoj sprejeti, da lahko aplikacijo uporabljate hitreje
B) Pazljivo preberite dovoljenja in dovolite samo potrebna
C) Dovoli vsa dovoljenja, da se izogneš napakam aplikacije
D) Takoj odstranite aplikacijo

8. Kakšen je namen Splošne uredbe o varstvu podatkov (GDPR)?

A) Pomagati podjetjem zbrati več podatkov
B) Zaščititi osebne podatke in pravice do zasebnosti posameznikov
C) Preprečiti ljudem uporabo družbenih medijev
D) Nadzorovati spletno nakupovanje

9. Katera od naslednjih dejanj pomaga zaščititi vaše podatke na skupnem računalniku?

A) Ostati prijavljen zaradi udobja
B) Odjava in izbris zgodovine brskanja po uporabi
C) Omogočanje brskalnikom, da shranijo vaša gesla
D) Deljenje vaših podatkov za prijavo z družinskimi člani

10. Kaj naj storite, če sumite, da so bili vaši osebni podatki ukradeni?

A) To ignorirati in upati, da se bo problem rešil sam
B) Objavite to na družbenih omrežjih
C) Prijavite to pristojnim organom in takoj spremenite gesla
D) Ne storite ničesar, razen če je bil ukraden denar

Povzetek odgovorov

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

MODUL V

Varna digitalizacija starejših

6. Modul V – Varna digitalizacija starejših

Modul 5 se osredotoča na opremljanje izobraževalcev z znanjem, orodji in delovnimi metodami, potrebnimi za učinkovito podporo starejšim pri varni uporabi digitalnih tehnologij. Modul udeležence seznani s posebnimi značilnostmi in učnimi potrebami starejših odraslih, zlasti v zvezi z uporabo internetnih aplikacij, e-poštnih storitev, platform družbenih medijev in orodij za spletno bančništvo.

Poseben poudarek je na kibernetski varnosti, zlasti na zmanjševanju tveganj za goljufije, prevare in dezinformacije. Udeleženci spoznavajo pogoste spletne grožnje, s katerimi se srečujejo starejši, in se naučijo, kako se spopasti s temi tveganji s preventivnimi strategijami, jasno komunikacijo in praktičnimi nasveti, prilagojenimi tej starostni skupini.

Poleg tega modul 5 zagotavlja celovito izobraževalno podporo za digitalizacijo starejših z združevanjem učnih orodij in praktičnih vaj. Udeleženci razvijejo spretnosti za učinkovito in empatsko prenašanje znanja, odzivanje na izzive, povezane s kibernetsko varnostjo, in oblikovanje dostopnih in podpornih učnih okolij za individualne coaching seje in skupinske izobraževalne dejavnosti.

6.1 Cilji učenja

Cilj tega modula je udeležencem omogočiti pridobitev izobraževalnih in praktičnih veščin, potrebnih za učinkovito poučevanje starejših o varni uporabi digitalnih tehnologij in podporo pri spopadanju z izzivi kibernetske varnosti.

- Razumevanje posebnih potreb starejših v zvezi z digitalizacijo.
- Učenje metod poučevanja, prilagojenih starejšim.
- Pridobivanje veščin za prepoznavanje in odzivanje na tipične kibernetske grožnje, usmerjene v starejše.

6.2 Struktura, vsebina in učni izidi

Po uspešnem zaključku tega modula bodo udeleženci sposobni:

- Razumevanje ovir za učenje tehnologije s strani starejših (psiholoških, kognitivnih in tehničnih), uporaba praktičnih in dostopnih metod poučevanja, kot so ponavljanje, vaje v majhnih korakih in preprosta pojasnila.
- Naučite se metod za sporočanje pravil varnega prijave, prepoznavanja varnih spletnih strani in zaščite osebnih podatkov, s čimer boste starejšim pomagali pri samostojni in varni uporabi spletnih storitev.
- Seznanite se z najpogostejšimi grožnjami, za katere so starejši še posebej ranljivi, in se naučite, kako to znanje na preprost način posredovati starejšim, da bodo bolj pazljivi.
- Naučite se, kako podpirati starejše pri prepoznavanju spletnih groženj in razvijanju varnih navad s pomočjo vaj in situacijskih scenarijev.
- Spoznajte, kakšne ukrepe je treba sprejeti v primeru grožnje, na primer takojšnjo spremembo gesla ali odklop naprave iz omrežja, in razumite, katere podatke je treba zaščititi v primeru grožnje.
- Poznavanje postopkov za prijavo incidentov kibernetske grožnje, kot so obvestitev banke, policije ali specializiranih organizacij, ter poznavanje virov podpore za žrtve kibernetske kriminalitete.
- Razložite metode varnostnih pravil v aplikacijah za takojšnje sporočanje, e-pošti in videoklicih ter kako izvajati vaje za prepoznavanje spletnih groženj.
- Zagotavljanje znanja o zaščiti naprav pred virusi in postopno učenje posodabljanja sistemov na dostopen in razumljiv način.

6.3 Dnevni red I Podroben načrt seje

MODUL V
Varno digitaliziranje starejših

1. seja

Dobrodošli
Trajanje 5

Cilji

- Ustvarjanje odprtega in privlačnega vzdušja, ki spodbuja aktivno sodelovanje.

Vsebina/metoda

- Pozdrav udeležencev, kratka predstavitev izvajalca usposabljanja. Izvajalec usposabljanja predstavi načrt usposabljanja in pravila dela.

Material
Ni dodatnega materiala.

Komentar
Lahko je koristno, da cilj delavnice pojasnite v preprostem jeziku.

2. Srečanje

Dejavnost za spoznavanje
Trajanje 15

Cilji

- Vzpostavitev prijateljskih odnosov med udeleženci, spoznavanje drug drugega in aktiviranje skupine pred začetkom vsebinskega dela.

Vsebina/metoda

- Kratka aktivna vaja, ki sproži razpravo: »S kakšnimi izzivi se srečujejo pri poučevanju starejših o novih tehnologijah? Kako se z njimi spopadajo?« Izobraževalec lahko doda dodatna vprašanja, ki bodo vplivala na potek razprave: Kaj vas je presenetilo? Katere metode so se izkazale za najučinkovitejše? Kako je mogoče prilagoditi tempo ali obliko pouka individualnim potrebam udeležencev? Vsak udeleženec lahko predstavi en izziv.

Material
Ni dodatnega materiala.

Komentar
Koristno je, da odgovore udeležencev zapišete na tablo ali flipchart, da lahko ugotovite najpogostejše težave.

3. Srečanje

Predavanje 1: Praktični nasveti za poučevanje starejših o kibernetski varnosti in novih tehnologijah
Trajanje *25*

Cilji

- ❖ Ozaveščanje izobraževalcev o ovirah, s katerimi se srečujejo starejši pri učenju uporabe novih tehnologij, in opremljanje izobraževalcev z učinkovitimi učnimi orodji za podporo učnega procesa.
- ❖ Zagotoviti izobraževalcem znanje in metode za poučevanje starejših o načelih varne uporabe internetnih aplikacij, okrepiti njihov občutek varnosti in digitalne kompetence.

Vsebina/metoda

- ❖ Predavanje je razdeljeno na dve tematski področji:

Tema 1: Metode učinkovitega poučevanja starejših na področju kibernetske varnosti in novih tehnologij

Vsebina/metode:

- Prepoznavanje psiholoških ovir (npr. strah pred tehnologijo, nizka samozavest), kognitivnih ovir (npr. počasnejše obdelovanje informacij, težave s koncentracijo) in tehničnih ovir (pomanjkanje izkušenj z napravami).
- Razprava o načelih prijazne komunikacije s starejšimi.

Gradivo:

Pomoč pri poučevanju za izobraževalce: Praktične metode poučevanja starejših – gradivo za vaje za izobraževalce (Priloga 1)

Tema 2: Priprava izobraževalcev za poučevanje starejših o načelih varne uporabe internetnih aplikacij (bančništvo, nakupovanje, spletna družbena omrežja)

Vsebina / Metode:

- Pregled priljubljenih internetnih aplikacij, ki jih uporabljajo starejši.
- Učenje prepoznavanja varnih spletnih strani in aplikacij (potrdila, URL-ji, videz prijavnih obrazcev).
- Razprava o načelih ustvarjanja varnih gesel in shranjevanja podatkov za prijavo.
- Praktične vaje na fiktivnih računih: prijava, preverjanje varnosti spletnega mesta, simulirano spletno nakupovanje.

Gradivo:

Pomoč pri poučevanju za izobraževalce: Praktične vaje – poučevanje izobraževalcev o načelih kibernetske varnosti za starejše (Priloga 2)

Komentar

Da bi ugotovili najpogostejše težave, je koristno zapisati odgovore udeležencev na tablo ali flipchart.

Dejavnost 1: Ugotavljanje ovir za učenje med starejšimi
Trajanje 15

Cilji učenja

- Povečanje ozaveščenosti o procesu učenja starejših ljudi.
- Prepoznavanje ovir za učenje med starejšimi.

Vsebina/metoda

- Vaja se izvaja individualno ali v parih – odvisno od želja udeležencev.
- Udeleženci prejmejo delovne liste (Priloga 3), ki vsebujejo nalogo, v kateri razmišljajo o možnih ovirah v procesu učenja starejših.
- Udeleženci morajo opredeliti primere psiholoških, kognitivnih in tehničnih ovir, ki se lahko pojavijo pri starejših med učenjem.
- Nato predlagajo načine za premagovanje vsake od teh ovir in opisujejo, kako lahko vplivajo na proces učenja starejših.
- Vaja se konča z razpravo, ki jo vodi vodja, med katero udeleženci delijo svoje zaključke in izkušnje.

Gradivo

- Delovni list – Prepoznavanje ovir pri učenju starejših (Priloga 3)

Komentar

Udeležence je vredno spodbuditi k aktivni udeležbi v razpravi.

Odmor | Trajanje *5'*

- **Udeležencem omogočite čas za počitek in razmislek.**
- **Kratek odmor za osvežitev.**

4. Srečanje

Predavanje 2: Uvod v kibernetsko varnost za starejše
Trajanje *35*

Cilji

- Seznanitev z najpogostejšimi grožnjami, za katere so starejši še posebej ranljivi, in učenje, kako to znanje posredovati na dostopen in učinkovit način, da se poveča njihova pazljivost in varnost na internetu.
- Pridobivanje znanja o tem, kako starejšim pomagati pri prepoznavanju spletnih groženj in kako pri njih oblikovati navade varne rabe interneta, s čimer se poveča njihova digitalna ozaveščenost.

Vsebina/metoda

- ❖ Predavanje je razdeljeno na dve tematski področji:

Tema 1: Pogoste digitalne grožnje in potrebe starejših
Vsebina/metode:

- Razprava o pogostih spletnih grožnjah, kot so phishing, spletne prevare, kraja podatkov, lažne novice.
- Prepoznavanje posebnih tveganj, za katera so starejši ljudje bolj dovzetni.
- Nasveti, kako starejše učinkovito ozaveščati o teh grožnjah, ne da bi pri tem povzročali nepotrebno strah.
- Primeri spletnih prevar, s katerimi se lahko srečujejo starejši, in kako jih prepoznati.

Gradivo:
Pomoč pri poučevanju za izobraževalce: Varno uporabljanje interneta s strani starejših (Priloga 4)

Tema 2: Razvijanje digitalne ozaveščenosti med starejšimi
Vsebina/metode:

- Razprava o metodah za podporo starejšim pri učenju prepoznavanja sumljivih situacij na internetu.
- Primeri vaj, ki starejšim pomagajo zapomniti si načela kibernetske varnosti.
- Simulacije spletnih situacij, v katerih lahko starejši ljudje naredijo napake, in kako jim učinkovito pomagati, da se naučijo izogibati tem napakam.

Gradivo:
Pomoč pri poučevanju za izobraževalce: Prepoznavanje groženj na internetu (Priloga 5)

Komentar
Udeležence spodbudite, da delijo izkušnje iz dela s starejšimi in primere učinkovitih metod za razlago zahtevnih tem.

Dejavnost 2: Simulacijska vaja: pogovor s starejšim o kibernetski varnosti
Trajanje *15*

Cilji

- ❖ Omogočiti izobraževalcu, da se pogovori s starejšim in mu pomaga razumeti, kako se izogniti spletnim grožnjam.

Vsebina/metoda

- Naloga se izvaja v parih, v katerih udeleženci izmenično prevzemajo vlogo izobraževalca in starejše osebe. Cilj vaje je izvesti simulirani izobraževalni pogovor o nevarnostih na internetu, ob upoštevanju resničnih situacij, s katerimi se lahko srečujejo starejše osebe. Vsak par prejme opis, ki predstavlja določeno nevarnost (Priloga 6).
- Vloga izobraževalca je v mirnem in razumljivem pojasnjevanju, kaj je določena nevarnost, kako jo prepoznati in kako se nanjo odzvati. Vloga starejše osebe vam omogoča, da prevzamete vlogo osebe, ki ima morda omejeno digitalno znanje in potrebuje jasna, prijazna navodila. Vaja

se konča s skupno razpravo, ki jo vodi vodja, med katero udeleženci delijo svoje občutke, zaključke in razmišljanja o učinkoviti izobraževalni komunikaciji s starejšimi.

Gradivo

- Simulacijska vaja: Pogovor s starejšim o kibernetski varnosti (Priloga 6)

Komentar
Pomembno je paziti na jasnost jezika in se izogibati tehničnemu žargonu.

Odmor | Trajanje *5'*

- **Omogočite udeležencem čas za počitek in pripravo na naslednjo sejo.**
- **Kratek odmor za osvežitev.**

5. seja

Predavanje 3: Odzivanje na kibernetske grožnje
Trajanje *30*

Cilji

- Priprava izobraževalcev za učinkovito posredovanje znanja starejšim o digitalnih grožnjah in načinih njihovega preprečevanja.
- Razvijanje veščin izobraževalcev pri vodenju pouka za starejše o odzivanju na kibernetske grožnje.
- Krepitev kompetenc izobraževalcev pri uporabi aktivacijskih metod in metod, prilagojenih potrebam starejših.

Vsebina/metoda

- Predavanje je razdeljeno na dve tematski področji:

Tema 1: Ukrepi, ki jih je treba sprejeti v primeru suma kibernetske grožnje
Vsebina/metode:
Izobraževalec obravnava:

- najpogostejše simptome morebitnega kibernetskega napada (npr. nenavadno delovanje naprave, sumljiva e-poštna sporočila, sporočila o napakah, nenadno odjavljanje);
- osnovna varnostna pravila – kako se odzvati v primeru suma napada: takojšnja odklopitev od omrežja, sprememba gesel, ne odpiranje sumljivih prilog ali povezav;
- pomembnost ohranjanja mirnosti in neukrepanja (npr. ne kličite nazaj na neznane številke, ne klikajte na opozorila o phishingu);
- načine za ustvarjanje varnih gesel in njihovo posodabljanje – vključno z izogibanjem rojstnim datumom in preprostimi kombinacijami.

Tema 2: Kako prijaviti digitalne grožnje in kje poiskati pomoč

Vsebina/metode:

Izobraževalec obravnava:

- ustanove in mesta, kjer lahko prijavite kibernetske grožnje (npr. CERT Polska, telefonske številke bank, lokalna policija, organizacije, ki podpirajo starejše);
- kdaj in kako stopiti v stik z banko – npr. ko sumite, da je prišlo do prevzema računa ali nepooblaščene transakcije;
- kako se pripraviti na prijavo – zapisati datum, čas, vsebino sporočila, narediti posnetek zaslona, shraniti sumljiva sporočila;
- vlogo čustvene in informacijske podpore – kako in kje jo poiskati (telefonske linije, svetovalne točke, bližnji);
- pomembnost prijave poskusa goljufije, tudi če ni prišlo do izgube – v korist drugih uporabnikov.

Gradivo

- ❖ Pomoč pri poučevanju za izobraževalce: simulacije scenarijev (priloga 7)

Komentar

Udeležence je vredno spodbuditi k razpravi.

Dejavnost 3: Vaja prepoznavanja goljufij
Trajanje 20

Cilji

- ❖ Pridobivanje znanja o tem, kako pomagati starejšim, da ostanejo mirni in zbrani v primeru spletnih groženj (npr. poskusi goljufij, sumljiva e-poštna sporočila, neznani telefonski klici).
- ❖ Razviti sposobnost sprejemanja racionalnih odločitev, izogibanja prenaglim dejanjem in navezovanja stikov z ustreznimi osebami in institucijami.

Vsebina/metoda

- ❖ Vaja obsega simulacijo pogovora med starejšim in izobraževalcem.
- ❖ Udeleženci delajo v parih in igrajo dodeljene vloge: izobraževalec in starejša oseba. Udeleženci imajo dostop do nasvetov in tem za simulacijo (Priloga 8), ki jim pomagajo izvesti realističen pogovor o kibernetskih grožnjah. Po koncu simulacije vodja moderira razpravo. Vsak par deli svoje razmišljanja z skupino in razpravlja o težavah, s katerimi se je srečal, čustvih in učinkovitih strategijah komuniciranja. Razprava pomaga bolje razumeti metode podpore starejšim pri prepoznavanju groženj in učenju, kako se nanje ustrezno odzvati.

Gradivo

- ❖ Simulacijska vaja: vzorci poročil o kibernetskih grožnjah (priloga 8)

Komentar

Pomembno je, da so izobraževalci dobro pripravljeni na vključevanje starejših in njihovo motiviranje za aktivno sodelovanje v učenju, pri čemer uporabljajo primere iz njihovega vsakdanjega življenja.

Odmor | Trajanje 5'

- **Omogočite čas za počitek in pripravo.**
- **Kratek odmor za osvežitev.**
- **Kratek odmor za osvežitev in sprostitev.**

6. seja

Predavanje 4: Izobraževanje starejših o uporabi elektronskih naprav in internetnih aplikacij – vodnik za izobraževalce
Trajanje *20*

Cilji

- Opremiti izobraževalce z orodji in metodami, ki omogočajo učinkovito poučevanje starejših o načelih varne uporabe komunikacijskih aplikacij, kot so e-pošta, takojšnje sporočanje (npr. Messenger, WhatsApp) in aplikacije za videoklice (npr. Zoom).
- Priprava izobraževalcev za vodenje pouka o zaščiti digitalnih naprav starejših – od osnovne uporabe protivirusnih programov do učenja, kako posodobiti operacijski sistem in aplikacije.

Vsebina/metoda

- Predavanje je razdeljeno na dve tematski področji:

Tema 1: Kako starejše naučiti varne uporabe komunikacijskih aplikacij
Vsebina/metode:

- Načini razlage osnovnih funkcij komunikacijskih aplikacij v preprostem, vsakdanjem jeziku.
- Primeri vaj, ki pomagajo prepoznati nevarna sporočila (spam, phishing), npr. analiza resničnih in lažnih e-poštnih sporočil.
- Praktične demonstracije nastavitev zasebnosti in varnosti v aplikacijah – blokiranje neznanih stikov, spreminjanje gesel, nastavitve zasebnosti.
- Metode aktiviranja: delo s kontrolnim seznamom, simulacije nevarnih situacij, skupno reševanje scenarijev.

Material:
Pomoč pri poučevanju za izobraževalce: Kako naučiti starejše varno uporabljati komunikacijske aplikacije (Priloga 9)

Tema 2: Kako starejše naučiti uporabljati protivirusne programe in posodobitve sistema
Vsebina/metode:

- Kako starejšim na razumljiv način razložiti pojme: računalniški virus, posodobitev, skeniranje sistema.
- Skupinske vaje o namestitvi in uporabi brezplačnih protivirusnih programov (npr. Avast, AVG).
- Korak za korakom: kako starejšim pokazati, kako izvesti posodobitve sistema in aplikacij.

Material:
Pomoč pri poučevanju za izobraževalce: Kako starejše naučiti uporabljati protivirusne programe in posodobitve sistema (Priloga 10)

Komentar
Med razpravo je pomembno zagotoviti izmenjavo idej med udeleženci.

Dejavnost 4: Praktični nasveti in tehnike za starejše
Trajanje *30*

Cilji

- Razviti sposobnost, da starejšim osebam ponudimo preproste in učinkovite nasvete o varni uporabi interneta.
- Razviti sposobnost prepoznavanja in uporabe učnih tehnik, ki so razumljive in dostopne starejšim.
- Izmenjava dobrih praks in resničnih izkušenj iz dela s starejšimi, ki lahko navdihujejo druge izobraževalce.

Vsebina/metoda

- Vaja je sestavljena iz dveh delov: individualnega in skupinskega. V prvem delu udeleženci samostojno izpolnijo delovni list (Priloga 11) in zapišejo svoje razmišljanja, opažanja in ideje o učinkovitih metodah poučevanja starejših o kibernetski varnosti. V drugem delu udeleženci svoje misli delijo na forumu celotne skupine, kar olajša izmenjavo izkušenj in iskanje navdihujočih rešitev in preverjenih praks. Skupna razprava omogoča dopolnjevanje znanja, bogatitev perspektiv in opazovanje različnih stilov izobraževalnega dela s starejšimi. Na koncu vaje vodja začne razpravo, katere cilj je poglobiti temo.

Material

- Delovni list: Varno uporabljanje interneta: praktični nasveti in tehnike za starejše (priloga 11)

Komentar
Udeležence je vredno spodbujati, da med izvajanjem vaje postavljajo vprašanja.

7. seja

Razprava | Trajanje 10’

Cilji učenja

- Udeležencem omogočiti, da po seji delijo izkušnje in opažanja.
- Prepoznavanje izzivov, povezanih z učenjem starejših.
- Začetek skupinske seje za izmenjavo idej za izboljšanje dela s skupinami starejših.

Vsebina/metoda

- Izobraževalec začne odprto razpravo z vprašanji, kot so: „Kaj je bilo najtežje?“, „Katera področja je treba še izboljšati?“, „Kako je mogoče poenostaviti poučevanje starejših?“ Udeleženci delijo svoje razmišljanja, prakse in zaključke iz seje. Zaključki se zapišejo na flipchart ali tablo, kar olajša povzemanje in morebitno uporabo v prihodnosti.

Material

- Flipchart ali tabla
- Flomaster

Zaključek | Trajanje 5 minut

Cilji učenja

- Povzetek ključnih informacij, odgovori na zadnja vprašanja udeležencev in navedba virov za nadaljnje učenje.

Vsebina/metoda

- Kratek povzetek najpomembnejših tem, obravnavanih med usposabljanjem.
- Navedba dodatnih virov znanja (npr. izobraževalne spletne strani, video gradivo).
- Zahvala udeležencem za sodelovanje in zaključek seje.

Material

- Pomoč pri poučevanju za izobraževalce: Spletne strani o varni uporabi tehnologije (Priloga 12).

Komentar

Na koncu je dobro izvesti kratko evalvacijsko anketo.

6.4 Dodatne informacije

6.4.1 Samorefleksija izobraževalcev

- Kaj je bilo za udeležence najtežje razumeti v zvezi s kibernetsko varnostjo?
- Kateri metodi sta bili najučinkovitejši med usposabljanjem?
- Kakšne spremembe bi lahko izboljšale izkušnjo udeležencev med vajo?
- Ali so se udeleženci počutili udobno pri delitvi svojih izkušenj in skrbi v zvezi z učenjem starejših?

6.4.2 Ocena programa s strani izobraževalcev

- So bili cilji usposabljanja doseženi?
- Katera področja je treba v prihodnosti razširiti ali spremeniti?
- Kakšne didaktične tehnike so bile najučinkovitejše pri tej skupini udeležencev?

6.4.3 Gradivo, dodatni viri

Priloga 1 | Praktične metode poučevanja starejših – gradivo za vaje za izobraževalce
Izpolnite vaje za izobraževalce za vsako metodo (npr. ustvarite vodnike, predlagajte analogije, oblikujte vizualne pripomočke ali opišite odgovore).

Ponavljanje in vaje po korakih

- **Opis metode:** kratka, ponavljajoča se navodila, vsaka dejavnost razdeljena na preproste korake.
- **Vaja za izobraževalce:** Razvijte navodila po korakih za prijavo v platformo družbenih medijev ali sistem spletnega bančništva (z uporabo preprostega in jasnega jezika).
- **Cilj:** Razviti sposobnost oblikovanja nalog v logični in enostavni strukturi.

Uporaba vizualizacij in primerov iz resničnega življenja

- **Opis metode:** Povezovanje abstraktnih tehnoloških pojmov z vsakdanjimi izkušnjami starejših (npr. primerjava gesla s ključem od hiše).
- **Vaja za izobraževalce:** Predlagajte 3 analogije, ki bodo starejšim pomagale razložiti naslednje pojme: geslo, varna spletna stran in phishing.
- **Cilj:** Pomagati starejšim razumeti zapletene koncepte s sklicevanjem na znane situacije.

Uporaba materialov z velikim tiskom

- **Opis metode:** Uporaba povečanega tiska, barv z visokim kontrastom, piktogramov in diagramov.
- **Vaja za izobraževalce:** Pripravite primer vizualne pomoči za starejše, ki vključuje načela ustvarjanja varnega gesla.
- **Cilj:** Razviti spretnosti pri ustvarjanju gradiva, prilagojenega vizualnim in kognitivnim potrebam starejših.

Poučevanje v tempu, prilagojenem skupini

- **Opis metode:** Opazovanje reakcij udeležencev, zastavljanje kontrolnih vprašanj in ohranjanje prožnosti pri hitrosti poučevanja.
- **Vaja za izobraževalca:** Opišite, kako bi se odzvali, če polovica skupine ne bi razumela funkcije aplikacije, o kateri se pogovarjate – kakšne ukrepe bi sprejeli?
- **Cilj:** Razviti refleksiven pristop k poučevanju in prilagodljivost pri delu s skupino z različnimi hitrostmi učenja.

  Kako uporabljati prilogo:
  Dodatek se lahko uporabi med delavnicami za izobraževalce kot niz individualnih in skupinskih vaj, gradivo za simulirane izobraževalne seje za starejše in izhodišče za ustvarjanje prilagojenih načrtov pouka.

Priloga 2 | Praktične vaje – Poučevanje izobraževalcev o načelih kibernetske varnosti za starejše osebe iz programa.

Opravite praktične naloge za vsako temo (npr. pregled aplikacij, preverjanje varnosti spletnih strani, ustvarjanje varnih gesel in vaje s testnimi računi).

Vsebina in metode za delo z izobraževalci:

1. Pregled priljubljenih spletnih aplikacij, ki jih uporabljajo starejši
   - **Naloga izobraževalca:** Seznanite se z vmesniki aplikacij, kot so spletne trgovine, npr. Allegro, platforme družbenih medijev, npr. Facebook, in mobilno bančništvo.
   - **Metoda:** analiza posnetkov zaslona, pregled vmesnikov na mobilnih napravah in računalnikih.
   - **Cilj:** Prepoznati skupne elemente in potencialne težave, s katerimi se srečujejo starejši.

2. Naučiti se prepoznati varne spletne strani in aplikacije
   - **Praktična naloga:** Preglejte 5 primerov spletnih strani – prepoznajte, katere so varne. Označite SSL certifikat, oceno URL-ja, sumljive obrazce za prijavo.
   - **Metoda:** Primerjalna analiza (varne in nevarne spletne strani), interaktivni kviz.
   - **Cilj:** Naučiti kritično analizo varnosti spletnih strani.

3. Načela za ustvarjanje varnih gesel in shranjevanje podatkov za prijavo
   - **Vaja:** Ustvarite 3 varna gesla po pravilu 3C (kompleksnost, spremenljivost, zapomljivost). Predlagajte varen način shranjevanja podatkov za prijavo (npr. upravitelji gesel, zvezek za zapisovanje).
   - **Metoda:** Brainstorming, razprava + mini delavnica o ustvarjanju gesel.
   - **Cilj:** Razumeti in posredovati načela varnosti na preprost in prepričljiv način.

4. Praktične vaje z uporabo izmišljenih računov
   - **Naloga:** Prijavite se v testni bančni račun ali račun spletne trgovine (simulacija), opravite varen »nakup« in preverite varnostne elemente na spletnem mestu.
   - **Metoda:** Delo v parih z računalniki/tablicami, situacijski scenariji.
   - **Cilj:** Pretvoriti teoretično znanje v praktična znanja, ki jih lahko izobraževalci posredujejo starejšim.

Priloga 3 | Delovni list: Prepoznavanje ovir pri učenju starejših

Izpolnite delovni list z opredelitvijo ovir (psiholoških, kognitivnih, tehničnih).

Psihološke ovire	Primer	Kako rešiti	Vpliv na učenje
Strah pred neuspehom			
Pomanjkanje samozavesti			
Omejena motivacija			
Kognitivne ovire	Primer	Kako rešiti	Vpliv na učenje
Počasnejše pomnjenje			
Težave s koncentracijo			
Težave s kratkoročnim spominom			
Tehnične ovire	Primer	Kako rešiti	Vpliv na učenje
Težave pri uporabi tehnologije			
Pomanjkanje izkušenj z uporabo interneta			
Težave pri uporabi novih izobraževalnih platform			

Priloga 4 | Varno uporabljanje interneta s strani starejših

Predstavite primere, razpravljajte o resničnih grožnjah in izvedite interaktivne vaje, da starejše naučite varnosti na spletu.

1. Predstavitve s primeri spletnih prevar

- **Opis:** Predstavitve morajo vključevati realistične primere spletnih prevar, ki so pogosto usmerjene v starejše, kot so phishing, lažne dražbe ali lažna e-poštna sporočila. Izobraževalci lahko pripravijo diapozitive ali vizualno gradivo, ki prikazuje konkretne primere in kaže, kako prepoznati nevarne elemente.
- **Cilj:** Ozaveščanje starejših o najpogostejših spletnih grožnjah. Naučiti prepoznavanje prevar in drugih oblik spletnega zlorabljanja, za katere so starejši še posebej ranljivi.
- **Primeri prevar, o katerih je treba razpravljati:**
  Phishing: lažna e-poštna sporočila ali spletne strani, ki poskušajo ukrasti prijavne podatke.
  Spletne dražbene prevare: lažne ponudbe za prodajo izdelkov.
  Lažna SMS-sporočila in e-poštna sporočila: sporočila, ki se izdajajo za sporočila institucij, na primer bank.

2. Razprava o resničnih grožnjah v vsakdanjem življenju starejših

- **Opis:** Po predstavitvi primerov prevar je pomembno, da izobraževalec vodi razpravo, v kateri lahko udeleženci delijo svoje izkušnje in znanje o spletnih grožnjah, s katerimi se srečujejo starejši. Izobraževalci morajo starejše spodbujati, da govorijo o svojih izkušnjah in težavah, s katerimi se srečujejo pri uporabi tehnologije.
- **Cilj**: Razumeti resnične nevarnosti, s katerimi se starejši srečujejo v vsakdanjem življenju. Opredeliti ovire za uporabo interneta med starejšimi, kot so pomanjkanje digitalnih veščin ali strahovi v zvezi z varnostjo.
- **Primeri vprašanj za razpravo**
  - S kakšnimi vrstami spletnih prevar ste se srečali ali o njih slišali?
  - Kakšne so glavne skrbi starejših glede varnosti na spletu?
  - Kaj je največji izziv za starejše pri učenju uporabe interneta?

3. Interaktivne vaje in simulacije za prepoznavanje spletnih groženj

- **Opis:** Vaje in simulacije pomagajo pri praktični uporabi znanja o varnosti na spletu. Starejši lahko sodelujejo v dejavnostih, v katerih morajo prepoznati, katere spletne strani ali sporočila so varne in katere so lahko nevarne. Izobraževalci lahko uporabijo primere, kot so fiktivni bančni račun, spletna trgovina ali profil v družbenih medijih, da v realnem času pokažejo, kako prepoznati sumljive elemente.
- **Cilj:** Izboljšati sposobnost prepoznavanja spletnih groženj s praktičnim delom. Razviti sposobnost starejših, da sprejemajo premišljene odločitve o svoji varnosti na spletu.
- **Primeri vaj**
  - *Vaja prepoznavanja lažnega ribarjenja:* Udeleženci prejmejo vzorčne e-poštne sporočila in morajo označiti, katera so lahko poskusi lažnega ribarjenja.
  - *Simulacija spletnega nakupovanja:* Skupinska analiza spletne trgovine, preverjanje, kako prepoznati lažne ponudbe in kateri elementi kažejo, da je spletna stran varna.
  - *Ocena varnosti spletnih strani:* pregled spletnih strani in prepoznavanje sumljivih elementov, kot so manjkajoči SSL certifikati ali sumljivi obrazci za prijavo.

Priloga 5 | Prepoznavanje groženj na internetu

Naučite starejše prepoznavati spletne grožnje in vadite z e-poštnimi sporočili, povezavami in gesli.

1. Pregled metod za podporo starejšim pri prepoznavanju sumljivih spletnih situacij

- **Opis**

  Izobraževalci naj uporabljajo različne metode, ki starejšim omogočajo prepoznavanje sumljivih situacij na internetu. Glavni cilj je ozaveščanje, da ni vse, kar se zdi zaupanja vredno, tudi dejansko takšno. Jasna in preprosta navodila lahko starejšim pomagajo samostojno oceniti, ali je dana situacija varna.

- **Metode**

  - Osnovna načela za prepoznavanje sumljivih situacij: Naučite starejše, kako prepoznati sumljive e-poštne sporočila, SMS-sporočila ali lažne spletne strani. Primeri: odsotnost SSL-potrdila, pravopisne napake v sporočilih, neskladne URL-naslove.
  - Pravilo „ne zaupaj neznanim“: skupna razprava o situacijah, v katerih lahko starejši prejmejo sumljive ponudbe (npr. lažne naložbene priložnosti, nagrade v nagradnih igrah ali neznane zahteve za osebne podatke).
  - Izobraževanje s pomočjo analogij: primerjava spletnih situacij z realnimi scenariji, npr. prepoznavanje sumljivega prodajalca na tržnici.

2. Primeri vaj, ki starejšim pomagajo zapomniti pravila kibernetske varnosti

- **Opis**

  Praktične vaje, v katere so vključeni starejši, pomagajo utrditi načela kibernetske varnosti in previdno ravnanje na spletu. Starejši si ta pravila lažje zapomnijo, če jih lahko uporabijo v varnem in nadzorovanem okolju.

- **Vaje**

  - Prepoznavanje lažnih e-poštnih sporočil: Udeleženci prejmejo različne primere e-poštnih sporočil (pristnih in lažnih). Njihova naloga je prepoznati, katera e-poštna sporočila so lahko prevare in katera so varna.
  - Prepoznavanje nevarnih povezav: Starejši se učijo prepoznavati sumljive povezave v e-poštnih sporočilih ali SMS-sporočilih in se učijo, kako preveriti, ali je URL-naslov zaupanja vreden.
  - Vaja o varnosti gesel: Udeleženci ustvarijo primere močnih in šibkih gesel. Naučijo se načel ustvarjanja varnih gesel in kako jih varno shraniti.

3. Simulacije spletnih situacij, v katerih lahko starejši naredijo napake – in kako jim pomagati, da se naučijo izogibati tem napakam

- **Opis**

  Spletne simulacije so praktične vaje, ki starejšim omogočajo, da se skozi izkušnje naučijo prepoznavati in izogibati napakam. Simulacije udeležencem pomagajo, da se pri uporabi interneta počutijo bolj samozavestni in ozaveščeni.

- **Metode**

  - **Simulacija phishinga:** Izobraževalec predstavi scenarij, v katerem starejša oseba prejme e-poštno sporočilo, ki izgleda kot pristno sporočilo banke, v katerem se zahtevajo podatki za prijavo. Starejše osebe se naučijo, kako se ne pustiti zavesti in kateri elementi v e-poštnem sporočilu bi morali zbujati sum.

- **Simulacija spletnega nakupovanja:** Starejši obiščejo spletne strani, ki posnemajo spletne trgovine. Njihova naloga je prepoznati sumljive elemente, kot so prenizke cene, odsotnost SSL-potrdila ali nenavadne plačilne metode.
- **Simulacija lažnega obvestila o nagradi:** Izobraževalci predstavijo situacijo, v kateri starejša oseba prejme sporočilo o zmagi v nagradni igri, ki je v resnici prevara. Starejše osebe se naučijo prepoznati takšne prevare in kako se nanje odzvati.

Priloga 6 | Simulacijska vaja: Pogovor s starejšim o kibernetski varnosti

Izvedite vajo vlog z igranjem vlog o phishingu, prevarah, varnosti računov in družbenih medijih, pri čemer učitelj vodi, starejši pa vadijo.

Scenarij naloge

Izoboseba se pogovarjata o spletnih grožnjah in se učita, kako prepoznati in se izogniti raževalec in starejša tveganim situacijam. Vsak scenarij predstavlja različne pogoste grožnje, s katerimi se lahko starejše osebe srečujejo na internetu.

Primeri tem, o katerih se lahko pogovarjate med vajo

- Phishing (ponarejena e-pošta, sporočila)
  Kako prepoznati phishing v e-pošti, SMS-sporočilih in na spletnih straneh?
  Kateri so tipični znaki lažnih sporočil in povezav?
- Lažne nagrade in prevare v zvezi s tekmovanji
  Kakšne so pogoste prevare v zvezi z nagradami in dobitki na nagradnih igrah?
  Kako se je treba odzvati na ponudbe, ki zahtevajo predplačilo?
- Varnost spletnih računov
  Kakšne so dobre prakse za zaščito računov v bankah, spletnih trgovinah in družbenih medijih?
  Kaj naredi geslo varno in zakaj je dvofaktorska avtentikacija pomembna?
- Varno uporabljanje družbenih medijev
  Kako prepoznati lažne profile in prevarante na družbenih omrežjih?
  Katere informacije je treba zaščititi in katerih ne smemo deliti na spletu?

Delitev vlog v vaji (v parih)

- **Vloga izobraževalca (simulacijski trener):**
  Naloga izobraževalca je voditi pogovor, pomagati starejšim razumeti spletne grožnje in jih naučiti, kako jih prepoznati.
  Izobraževalec mora uporabljati preprost in jasen jezik, potrpežljivo razložiti nevarnosti in postavljati vprašanja, da spodbudi starejše k aktivni udeležbi v pogovoru.
  Izobraževalec je odgovoren tudi za opozarjanje starejših o pravilih varnosti na internetu in zagotavljanje, da so razumeli snov.
- **Vloga starejšega**
  Starejši aktivno sodeluje v pogovoru in deli svoje izkušnje v zvezi z uporabo interneta. Izrazi lahko vse svoje dvome ali pomisleke glede varnosti na spletu.
  Starejši odgovarja na vprašanja izobraževalca, deli svoje mnenje in poskuša rešiti predstavljene probleme v zvezi z nevarnostmi na spletu.

- **Phishing (ponarejena e-pošta, sporočila)**

Kako prepoznati phishing v e-pošti, SMS-sporočilih in na spletnih straneh?

Kateri so tipični znaki lažnih sporočil in povezav?

- **Lažne nagrade in prevare v zvezi s tekmovanji**

Kakšne so pogoste prevare v zvezi z nagradami in dobitki na tekmovanjih?

Kako se je treba odzvati na ponudbe, ki zahtevajo predplačilo?

- **Varnost spletnih računov**

Kakšne so dobre prakse za zaščito računov v bankah, spletnih trgovinah in družbenih medijih?

Kaj naredi geslo varno in zakaj je pomembna dvofaktorska avtentikacija?

- **Varno uporabljanje družbenih omrežij**

Kako prepoznati lažne profile in prevarante na družbenih omrežjih?

Katere informacije je treba zaščititi in česa ne smemo deliti na spletu?

Priloga 7 | Simulacije scenarijev

Izvedite simulacije scenarijev, v katerih se starejši soočajo z goljufivimi klici, e-poštnimi sporočili ali SMS-sporočili. Vprašajte jih, kako bi se odzvali, razpravljajte o čustvih in varnih odzivih ter vadite tehnike umirjanja, kot je dihanje.

Vsebina vaje

Priprava na vajo

Začnite sejo s kratko razpravo o pomembnosti ohranjanja mirnosti v težkih situacijah. Poudarite, da prevaranti pogosto poskušajo ustvariti paniko ali občutek nujnosti, da bi pritiskali na starejše, da sprejmejo hitre, nepremišljene odločitve.

Simulacije scenarijev groženj

- **Scenarij 1**
  Starejša oseba prejme telefonski klic od „bančnega uslužbenca“, ki trdi, da je bil njen račun blokiran, in jo prosi, naj namesti aplikacijo. Kaj stori starejša oseba?
- **Scenarij 2**
  Starejša oseba prejme e-poštno sporočilo, da je zmagala na nagradni igri, in jo prosijo, naj posreduje osebne podatke in klikne na povezavo. Kaj stori starejša oseba?
- **Scenarij 3**
  Starejša oseba prejme SMS s sumljivim sporočilom, da mora doplačati za paket. Kaj stori starejša oseba?

Po vsakem scenariju:

- Prosite starejše, naj na kratko povedo, kako bi se odzvali v takšni situaciji.
- Postavite reflektivna vprašanja, na primer
  Kaj čutite, ko prejmete takšna sporočila?
  Kakšna čustva se pojavijo?
  Kakšne misli vplivajo na vaše odločitve?

Nato v skupini razpravljajte o tem, kakšne ukrepe je treba sprejeti, da bi ostali mirni:
ne panikarite, ne delujte impulzivno, ustavite se in se pogovorite z nekom, ki vam je blizu, preverite informacije.

Vaja za ozaveščanje o čustvih:
Prosite starejše, naj zaprejo oči in se spomnijo situacije, ko so se počutili ogroženi na spletu (npr. prejeli sumljivo e-pošto).
Vprašajte: *Katere čustva ste občutili v tistem trenutku? Katere fizične signale je poslalo vaše telo (npr. pospešen srčni utrip, občutek nelagodja)?*
Spodbudite jih, naj poiščejo načine za obvladovanje teh čustev v ogrožajoči situaciji, npr. z uporabo prej obravnavanih dihalnih tehnik.

Povzetek vaje:
Poudarite, kako pomembno je, da se pred sprejetjem kakršnih koli odločitev ustavite, ko se soočate s potencialno nevarnostjo.
Poudarite, da ni vedno potrebno takoj ukrepati. Pametno je, da pred sprejetjem kakršnih koli ukrepov zaprosite za pomoč ali se posvetujete z bližnjimi ali strokovnjaki.

Nasveti za izobraževalce:

- **Bodite potrpežljivi:** starejši ljudje morda potrebujejo več časa, da razumejo grožnje in se ustrezno odzovejo. Potrpežljivo razložite vsako grožnjo in ponudite možne rešitve.
- **Prilagodite tempo:** poskrbite, da vsi udeleženci razumejo vsako vajo in imajo možnost postavljati vprašanja.
- **Bodite pozorni na čustva:** razumevanje, kako čustva vplivajo na odločanje, je bistveno. Zato so pomembne vaje za sprostitev in prepoznavanje čustev.

Redno vadite

Te seje je treba redno ponavljati, da se starejši počutijo bolj samozavestni in vedo, kako se odzvati, ko se soočijo z grožnjami.

Priloga 8 | Simulacijska vaja: Primeri poročil o kibernetskih grožnjah

Izvajajte vaje z igranjem vlog z vzorčnimi kibernetskimi grožnjami; pojasnite, opredelite tveganja in vadite varne odzive.

Scenarij naloge

Udeleženci delajo v parih in prevzamejo vlogo izobraževalca in starejšega.
Vsak par prejme opis enega od štirih vzorčnih poročil o kibernetskih grožnjah.
Naloga izobraževalca je, da s starejšim voditi miren in jasen izobraževalni pogovor, med katerim:

- pojasni naravo grožnje,
- pomoč starejši osebi pri razumevanju, kako prepoznati znake nevarnosti,
- skupaj s starejšim poišče rešitve in varne odzive na situacijo.

Udeleženci lahko zamenjajo vloge in delajo z novim poročilom.

Primeri štirih poročil o kibernetskih grožnjah, ki lahko zadevajo starejše osebe

Poročilo 1: SMS z zahtevo po dodatnem plačilu za paket

Opis situacije: Starejša oseba je prejela SMS, v katerem je bila obveščena, da je paket pripravljen za dostavo, vendar je potrebno dodatno plačilo v višini 2 EUR. Sporočilo je vsebovalo sumljivo povezavo, ki je vodila na neznano spletno stran.

Poročilo 2: Lažni telefonski klic iz banke

Opis situacije: Starejša oseba je prejela telefonski klic od osebe, ki je trdila, da je zaposlena v banki. Prevarant je trdil, da je bil račun blokiran, in predlagal namestitev aplikacije za njegovo zaščito.

Prijava 3: E-poštno sporočilo o domnevni nagradi

Opis situacije: Starejša oseba je prejela e-poštno sporočilo, v katerem je bilo navedeno, da je zmagala na nagradni igri. V e-poštnem sporočilu so zahtevali osebne podatke in starejšo osebo prosili, naj klikne na povezavo, ki je vodila na sumljivo spletno stran.

Prijava 4: Prevzem Facebook računa

Opis situacije: Prijatelji starejše osebe so prejeli čudna sporočila z njenega računa, vključno s povezavami ali prošnjami za posojilo. Starejša oseba teh sporočil ni poslala, kar kaže, da je njen račun prevzel prevarant.

Predlogi za vzgojitelje o tem, kako govoriti o grožnjah:

- **Razumevanje situacije:** Uporabite preprost jezik in analogije za pojasnjevanje groženj. Starejši ljudje pogosto bolje razumejo, če jim situacije predstavite v kontekstu vsakdanjega življenja (npr. primerjava kibernetske prevare s tradicionalnimi telefonskimi prevari).
- **Primeri in simulacije:** Redno izvajajte vaje s simuliranimi telefonskimi pogovori ali z analizo primerov sumljivih e-poštnih sporočil. To starejšim pomaga, da se učinkoviteje odzovejo na resnične grožnje.
- **Pomoč pri prijavljanju incidentov:** Pomagajte starejšim prijaviti kibernetske grožnje ustreznim institucijam, kot so CERT Poljska, banke ali policija. To lahko vadite med usposabljanjem, da okrepite njihovo samozavest.
- **Poudarjanje dvofaktorskega preverjanja pristnosti:** Nudite navodila za omogočanje dvofaktorskega preverjanja pristnosti, ki lahko starejšim pomaga zavarovati njihove spletne račune, zlasti pri uporabi družbenih medijev.
- **Ohranjanje mirnosti:** Izobraževalci naj starejše naučijo, da v ogrožajočih situacijah ostanejo mirni in se izogibajo impulzivnim dejanjem, kot so namestitev neznanih aplikacij ali deljenje osebnih podatkov.
- **Izobraževanje o varnostnih orodjih:** vredno je predstaviti uporabo protivirusne programske opreme, zaščito spletnih računov in preverjanje verodostojnosti virov informacij (npr. preverjanje uradnih telefonskih številk bank).

Priloga 9 | Kako starejše naučiti varne uporabe komunikacijskih aplikacij

Naučite varno uporabo aplikacij z enostavnim jezikom, vadite z ikonami in prepoznajte spam ali lažna sporočila.

Obseg vsebine in metode poučevanja

1. Razlaga osnovnih funkcij komunikacijskih aplikacij v vsakdanjem jeziku

Priporočila za izobraževalce

- Izogibajte se tehničnemu žargonu – namesto »prijavite se v svoj račun« recite »vpišite svoje ime in geslo, da odprete svojo poštno schránko«.
- Namesto »nastavitve zasebnosti« recite »kjer lahko izberete, kdo vas lahko vidi in kdo vam lahko pošilja sporočila«.
- Uporabite analogije, npr. »sporočilnik je kot telefon s sporočili in slikami«.

Primer vaje

- Razdelite kartice z ikonami priljubljenih aplikacij (npr. e-pošta, WhatsApp, Messenger, Zoom).
- Udeležence prosite, naj jih opišejo z lastnimi besedami.
- Skupaj ustvarite preprosto definicijo za vsako od njih.

Pomožno gradivo

- Ustvarite tiskani slovar preprostih izrazov (npr. »sporočilo«, »videoklic«, »priloga«).

2. Vaje za prepoznavanje nevarnih sporočil (spam, phishing)

Priporočila za izobraževalce

- Vedno uporabljajte resnične primere, da pokažete varna in lažna sporočila.

- Pogovorite se o tem, kako izgleda sumljiv e-poštni naslov, kaj pomeni »kliknite na to povezavo« in kako prepoznati prevaro »vnuk v tujini«.

Primer vaje

- Udeležence razdelite v skupine in jim dajte tri natisnjena e-sporočila:
  - Resnično vabilo na pogovor
  - Lažno e-poštno sporočilo s povezavo do „računa“
  - Sporočilo z gramatičnimi napakami in zahtevo po osebnih podatkih
- Naloga: Ugotovite, katera sporočila so sumljiva in zakaj.

Pomožno gradivo

- Ustvarite delovne liste z vzorčnimi e-poštnimi sporočili za analizo
- Predstavite 5 ključnih vprašanj za vsako sporočilo:
  - Ali poznam pošiljatelja?
  - Ali je sporočilo smiselno?
  - Ali so v njem napake?
  - Ali je e-poštni naslov pravilen?
  - Ali se povezava zdi sumljiva?

3. Predstavitev nastavitev zasebnosti in varnosti

Priporočila za izobraževalce

- Vsako nalogo prikazujte korak za korakom na velikem zaslonu ali projektorju.
- Ne pozabite: starejši se pogosto učijo z ponavljanjem – načrtujte, da boste vsak korak opravili skupaj.

Primer vaje

Za skupno izvedbo z udeleženci:

- Pojdite v nastavitve WhatsApp → »Zasebnost« → »Profilna fotografija« → izberite »Moji stiki«
- V Messengerju: pokažite, kako blokirati neznanca

Pomožno gradivo

- Ustvarite ilustrirane kartice s podrobnimi navodili, npr.:
  - „Kako spremeniti geslo“
  - „Kako nastaviti zasebnost“
  - „Kako blokirati uporabnika“

4. Interaktivne metode – utrjevanje znanja in odzivanje na grožnje

Priporočila za izobraževalce:

- Simulacije so učinkovite – starejši se najbolje učijo skozi realistične scenarije.
- Uporabite pare ali majhne skupine, da zgradite zaupanje in timsko delo.

Primeri vaj:

- Simulacija 1: »Prejel sem čudno sporočilo od banke« – kaj naj naredim?
- Simulacija 2: »Ne morem se povezati s hčerko prek Zoom« – kako preveriti nastavitve?
- Igra vlog: izobraževalec igra vlogo prevaranta, udeleženec igra vlogo starejše osebe – nato zamenjata vlogi.

Podporno gradivo:

- Ustvarite simulacijske scenarije
- Kartice vlog: izobraževalec/udeleženec/prevarant
- Kartice z nasveti za varnost, ki jih lahko vzamete domov (npr. za nalepitev na hladilnik)

Priloga 10 | Kako naučiti starejše uporabljati protivirusne programe in sistemsko posodabljanje

Starejšim naučite, kaj so virusi in posodobitve, jim pokažite, kako uporabljati protivirusni program, in jih naučite, kako izvajati skeniranje in namestiti posodobitve sistema korak za korakom.

Obseg vsebine in metode poučevanja

1. Uvod – Kaj so virusi, posodobitve in varnostne funkcije

Priporočila za učitelja:

- Pri razlagi zapletenih tem uporabite analogije.
- Pojasnite, kaj so »računalniški virusi« – uporabite primerjave z prehladom ali okužbo, ki lahko napade računalnik.
- Pojasnite, da so posodobitve kot „zdravilo“ za računalnik – pomagajo preprečevati okvare in napade.

Primer vaje

- Udeležencem zastavite naslednja vprašanja:
  - Ali ste že kdaj slišali za »računalniški virus«?
  - Kaj vam pride na misel, ko slišite besedo „posodobitev“?

2. Predstavitev protivirusne programske opreme

Priporočila za izobraževalca:

- Uporabite varen in intuitiven program (npr. Windows Defender, brezplačna različica Avast).
- Postopek opravite korak za korakom: odprite program, preverite posodobitve, opravite hiter pregled. Postopek lahko predstavite s pomočjo projektorja.

Primer vaje:

- Udeležence prosite, naj odprejo protivirusno programsko opremo na svojih napravah (ali na skupnem prenosnem računalniku).
- Skupaj izvedite skeniranje. Razpravljajte o pomenu rezultatov: „ni najdenih groženj“ v primerjavi z „zaznane grožnje“.

3. Naučite se, kako posodobiti operacijski sistem

Priporočila za izobraževalca:

- Pokažite, kako najti nastavitve za posodobitve (npr. v sistemu Windows: Nastavitve → Posodobitve in varnost).
- Poudarite, da se posodobitve običajno pojavijo samodejno – uporabnik mora samo klikniti »Namesti zdaj«.

Primer vaje:

- **Vsak udeleženec prejme kontrolni seznam:**
  - Odprite »Nastavitve«
  - Poiščite »Windows Update«
  - Preverite, ali so na voljo posodobitve
  - Namestite posodobitev, če je na voljo

- **Opomba: Če uporabljate skupni računalnik, lahko vajo izvedete kot demonstracijo s komentarjem.**

4. Metode utrjevanja – kontrolni seznami, igranje vlog, razprave

Priporočila za izobraževalca:

- Povzemite snov v obliki igre ali kviza.
- Udeležence spodbujajte, naj postavljajo vprašanja in delijo svoje izkušnje.

Primeri vaj:

- Seznam za varnost: Udeleženec korak za korakom preveri, ali je njegov računalnik/pametni telefon zaščiten (gesla, posodobitve, skeniranje).
- Simulacija telefonskega klica: Izobraževalec igra vlogo prevaranta, ki reče: »Vaš računalnik je ogrožen – prenesite naš program.« Naloga starejšega udeleženca je prepoznati grožnjo in odgovoriti: »Najprej bom preveril nastavitve protivirusnega programa.«

Podporno gradivo:

- Pripravljeni kontrolni seznami: »Varen računalnik – imam vse, kar potrebujem?«

Priloga 11 | Delovni list: Varno uporabljanje interneta: praktični nasveti in tehnike za starejše

Izpolnite delovni list z odgovori na vprašanja o varnem nakupovanju, varnosti naprav, zasebnosti na spletu in premagovanju strahu pred tehnologijo.

Varno spletno nakupovanje	
Kateri elementi spletne ponudbe bi morali biti starejšim poudarjeni kot potencialno nevarni ali sumljivi?	
Kako voditi starejše skozi proces spletnega nakupovanja – kako govoriti, kaj pokazati in na kaj paziti, da se bodo počutili varne?	
Varnost naprav	
Kakšne tehnike pomagajo starejšim razumeti, kako varno nastaviti svoje naprave?	
Kakšne aplikacije in nastavitve so potrebne za zaščito naprav starejših oseb?	
Zaščita zasebnosti na spletu	
Kakšne metode boste uporabili, da boste starejšim pomagali bolje razumeti koncept zaščite zasebnosti na spletu, zlasti v kontekstu uporabe komunikacijskih aplikacij, kot je WhatsApp?	
Premagovanje strahu pred tehnologijo	
Kateri elementi usposabljanja pomagajo starejšim premagati strah pred tehnologijo in okrepiti njihovo samozavest pri uporabi interneta?	
Kakšne metode za krepitev samozavesti je vredno uporabiti, da se starejši počutijo udobno v svetu novih tehnologij?	

Priloga 12 | Priporočila za nadaljnje branje in učenje za udeležence

Spletne strani o kibernetski varnosti: evropske in vladne organizacije, ki se ukvarjajo s kibernetsko varnostjo

1) **ENISA – Agencija Evropske unije za kibernetsko varnost**
   Spletna stran: https://www.enisa.europa.eu
   ENISA ponuja vodnike, poročila in izobraževalne kampanje o kibernetski varnosti. Vključuje izobraževalno gradivo za posamezne uporabnike, vključno s starejšimi, o varni uporabi e-pošte, gesel, pametnih telefonov in spletnega bančništva.
2) **Evropska komisija – Varnejši internet**
   Spletna stran: https://digital-strategy.ec.europa.eu/en/policies/safer-internet
   Program Evropske komisije za spodbujanje varne uporabe interneta za vse starostne skupine, vključno s starejšimi. Spletna stran vsebuje informativne kampanje in povezave do nacionalnih pobud.
3) **Mreža evropskih potrošniških centrov (ECC-Net)**
   Spletna stran: https://www.eccnet.eu
   Mreža potrošniških centrov v EU, ki ponuja nasvete o varnem spletnem nakupovanju, varstvu osebnih podatkov in preprečevanju spletnih prevar, kar je lahko še posebej koristno za starejše.
4) **Cyberprofilaktyka – Program digitalne preventive**
   Spletna stran: https://cyberprofilaktyka.pl/
   Program digitalne preventive, ki vključuje poglavje s svetovanjem za starejše o tem, kako se izogniti spletnim grožnjam. Vsebuje tudi izobraževalno gradivo, infografike in primere resničnih prevar, ki pomagajo bolje razumeti digitalna tveganja.

6.5 Modul V – Predhodni/naknadni test

1. Kakšen je glavni cilj modula 5?

A) Naučiti starejše, kako uporabljati družbene medije za zabavo
B) Usposobiti izobraževalce, da bodo lahko učinkovito podpirali starejše pri varni digitalizaciji
C) Izboljšati znanje starejših o umetni inteligenci
D) Razviti programerske veščine starejših

2. Katera od naslednjih ovir je najpogostejša pri učenju digitalnih veščin za starejše?

A) Radovednost glede novih tehnologij
B) Strah pred neuspehom ali pomanjkanje samozavesti
C) Prekomerna raba družbenih medijev
D) Dobro tehnično znanje

3. Katera je ena od učinkovitih metod poučevanja starejših?

A) Uporaba zapletenega žargona, da se zdiš profesionalen
B) Hitro izvajanje pouka
C) Razdelitev navodil na majhne, preproste korake
D) Osredotočanje le na teoretično znanje

4. Na kaj naj se izobraževalci osredotočijo pri poučevanju o spletnem bančništvu in nakupovanju?

A) Kako hitreje porabiti denar
B) Kako prepoznati varne spletne strani in zaščititi osebne podatke
C) Kako povečati spletno vidnost
D) Kako onemogočiti protivirusno programsko opremo

5. Kateri od naslednjih primerov je dober primer poskusa phishinga?

A) Prijatelj vam pošlje znano povezavo
B) E-poštno sporočilo vaše banke, v katerem vas prosijo za vaše uporabniško ime in geslo
C) Posodobitev iz zanesljivega programa
D) Opomnik iz vaše koledarjske aplikacije

6. Kaj naj najprej stori starejša oseba, ko prejme sumljiv telefonski klic od „bančnega uslužbenca“?

A) Takoj namestiti predlagano aplikacijo
B) Povezati in poklicati svojo banko na uradno številko
C) Posredovati svojo identifikacijsko številko in podatke o računu
D) Povsem ignorirati klic

7. Kateri je najboljši način, da učitelji starejšim pomagajo razumeti protivirusne programe?

A) Razložite z analogijami, na primer s primerjavo virusov z boleznimi
B) Izogibati se tehničnim pojasnilom
C) Preskočiti teme o protivirusnih programih, ker so preveč napredne
D) Prikazati samo besedilna pojasnila

8. Kaj pomeni „digitalna ozaveščenost” za starejše?

A) Vedeti, kako hitreje nakupovati na spletu
B) Razumevanje in prepoznavanje spletnih groženj
C) Izogibanje vsaki uporabi tehnologije
D) Naučiti se oblikovati spletne strani

9. Kaj naj stori učitelj, če starejša oseba med poukom ne razume aplikacije?

A) Preiti na naslednjo temo
B) Potrpežljivo ponoviti in poenostaviti razlago
C) Prosi drugega starejšega, naj ga nauči
D) Problem ignorirati

10. Kaj naj storijo starejši, če sumijo, da je bil njihov račun žrtev kibernetskega napada?

A) Počakati, da se problem sam odpravi
B) Prijaviti ga banki ali organom in takoj spremeniti gesla
C) Novico delijo na družbenih omrežjih
D) Izbrišejo vse svoje račune

Povzetek odgovorov

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

7. Anketa o oceni

Podatki, ki jih navedete v tej anketi, bodo služili kot smernice za izboljšanje ravni usposabljanja, v katerem sodelujete, ter ravni učinkovitosti in privlačnosti vaših naslednjih programov usposabljanja.

Anketo izpolnite sami ali v skladu z ocenjevalno lestvico spodaj, kjer je 1 najnižja ocena, 5 pa najvišja.

I. **Ocena delavnice:**

- Program usposabljanja ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Metode vodenja pouka ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Ozračje med poukom ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Koristnost usposabljanja ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Pripravljenost izvajalca usposabljanja ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Izbira vsebine usposabljanja ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Cilji usposabljanja so bili jasno opredeljeni ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1

1. **Katera vprašanja so bila za vas koristna in jih boste zagotovo uporabili?**
   .....
   .....

2. **Katera vprašanja so vam bila manj koristna?**
   .....
   .....

3. **Katera od tem, ki niso bila obravnavana v razredu, bi po vašem mnenju morala biti vključena v program in zakaj?**
   .....
   .....

4. **Menite, da bi bilo treba v program usposabljanja dodati ali iz njega odstraniti kakšno temo? Pojasnite, zakaj.**
   .....
   .....

II. **Ocena izobraževalnih gradiv:**

- Vsebina 54321 ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Dostopnost informacij ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Berljivost ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Uporabnost materialov ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1

III. **Dodatne informacije:**

1. **Splošna ocena usposabljanja** ☐ **POZITIVNA** ☐ **NEGATIVNA**

2. **Ali je usposabljanje izpolnilo vaša pričakovanja in zahteve – ali so bili doseženi zastavljeni cilji, izidi in rezultati?** ☐ **DA** ☐ **NE**

3. **Menite, da je bilo vredno organizirati takšno usposabljanje (in zakaj)?**
   .....
   .....

4. **Vaši dodatni komentarji in opažanja:**
   .....
   .....

5. **Kako ste izvedeli za usposabljanje?**
   .....
   .....

www.cybersafesenior.eu

Cyber-Safe-Senior

Funded by
the European Union

CYBER SAFE
SENIOR

Instytut
Nowych Technologii

iED

İLKSENOL
DERNEĞİ

SIMBIOZA
MED GENERACIJAMI

Financira Evropska unija. Izražena stališča in mnenja so last avtorja(-ev) in ne odražajo nujno stališč Evropske unije ali nacionalne agencije Erasmus+. Niti Evropska unija niti organ, ki dodeljuje sredstva, ne moreta biti odgovorna zanje.