DİJİTAL

DÜNYADA GÜVENLİK

Yaşlıların siber güvenliği konusunda eğitimciler için atölye senaryoları ve materyaller içeren eğitim programı

İÇİNDEKİLER

1. Giriş

"Cyber Safe Senior" (Siber Güvenlikli Yaşlılar), 65 yaş ve üstü yaşlıların dijital okuryazarlık, çevrimiçi güvenlik ve genel dijital yetkinliklerini geliştirmeyi amaçlayan, Avrupa Birliği tarafından finanse edilen bir projedir. Günümüzün giderek dijitalleşen dünyasında, yaşlılar çevrimiçi ortamlarda gezinirken özel engellerle karşılaşmaktadırlar, çünkü genellikle yeni teknolojiler, çevrimiçi riskler ve güvenli dijital davranışlar konusunda bilgi sahibi değildirler. Bunu fark eden Siber Güvenlikli Yaşlılar girişimi, organize, erişilebilir ve çok yönlü bir yaklaşım kullanarak dijital bilgi ve yetkinlik alanındaki önemli boşlukları kapatmayı amaçlamaktadır.

Proje, gerçek hayattan internet suçu vaka çalışmaları, pratik güvenlik tavsiyeleri ve güvenli çevrimiçi davranış için adım adım talimatlar içeren bilgilendirici bir e-kitap oluşturulmasını içermektedir. Ayrıca, girişim, yaşlı katılımcıların öğrenme hedeflerine ve tercihlerine özel olarak uyarlanmış sanal dersler, etkileşimli senaryo tabanlı alıştırmalar ve pilot eğitim oturumları sunmaktadır. Cyber Safe Senior, temel dijital deneyime sahip ancak çevrimiçi güvenlik konusunda farkındalığı eksik olan yaşlılara odaklanarak dijital dışlanmayı ortadan kaldırmayı, teknoloji kullanımına olan güveni artırmayı ve yaşlıların dijital ortamlara bağımsız ve güvenli bir şekilde katılmalarını sağlamayı amaçlamaktadır.

Projenin eğitimciler ve eğitmenler için hazırladığı eğitim programı, onlara yaşlılara yüksek kaliteli internet güvenliği eğitimi vermek için ihtiyaç duydukları bilgileri, metodolojiyi ve pratik araçları sağlar. Eğitmenler, sadece temel siber güvenlik kavramlarını öğretmekle kalmaz, aynı zamanda öğrencileri etkileşimli etkinliklere, gerçek hayattan senaryolara ve yaşlıların dijital dünyada karşılaşabilecekleri benzersiz sorunları vurgulayan alıştırmalara da dahil ederler. Bu, eğitimin hem pratik hem de katılımcıların günlük yaşamlarıyla doğrudan ilgili olmasını garanti eder.

Proje, Polonya, Slovenya, Türkiye ve Yunanistan'dan eğitim kurumları, toplum kuruluşları, kütüphaneler, kültür merkezleri ve yaşlılar topluluklarının bilgilerini bir araya getiren bir ortaklar konsorsiyumu tarafından yürütülür. Cyber Safe Senior, bu yerel ağları kullanarak hem kentsel hem de kırsal bölgelerdeki yaşlılara ulaşarak dijital okuryazarlık materyallerine ve desteğine adil erişim sağlar.

Yaşlıları çevrimiçi platformları güvenle kullanma, kişisel verilerini koruma, çevrimiçi riskleri belirleme ve dijital topluma aktif olarak katılma konusunda eğiterek, proje daha güvenli ve samimi bir dijital ortam yaratmayı amaçlamaktadır. Sonuç olarak, Cyber Safe Senior, eğitim materyallerini, uygulamalı etkinlikleri ve topluluk katılımını bir araya getirerek, yaşlıların dijital araçları güvenli, bağımsız ve verimli bir şekilde kullanmak için ihtiyaç duydukları bilgi, beceri ve özgüvene sahip oldukları bir ortam oluşturur.

Cyber Safe Senior eğitim programının önemli bir tamamlayıcı bileşeni, Genially kullanılarak geliştirilen etkileşimli Improve Vaka çalışmalarıdır. Bu senaryo tabanlı vakalar, her eğitim modülünün konuları ile tamamen uyumludur ve yaşlıların sıklıkla karşılaştığı gerçek hayattaki dijital durumları simüle etmek için tasarlanmıştır. Rehberli karar verme, pratik görevler ve görsel etkileşim yoluyla Improve Vakaları, teorik bilgileri pekiştirir ve deneyimsel öğrenmeyi destekler, böylece karmaşık çevrimiçi güvenlik kavramlarını yaşlı öğrenciler için daha erişilebilir ve ilgi çekici hale getirir.

Her eğitim modülü, öğrenme hedefleri, oturum planlaması, ek kaynaklar, eğitmen öz değerlendirmesi ve değerlendirme unsurları dahil olmak üzere modül arayüzüyle tutarlı yapılandırılmış bir formatı takip eder. Bilgi edinimini ve öğrenme sürecindeki ilerlemeyi ölçmek için her modülün başında ve sonunda ön ve son testler uygulanır. Ayrıca, katılımcıların ve eğitmenlerin geri bildirimlerini toplamak için değerlendirme anketleri kullanılır ve bu da kalite güvencesini ve eğitim programının sürekli iyileştirilmesini destekler.

1.1 Eğitim Programının Amacı

Siber Güvenlikli Yaşlılar Eğitim Programı, 65 yaş ve üstü yaşlılar arasında dijital okuryazarlık ve internet güvenliği konusunda artan ihtiyacı karşılamak için geliştirilmiştir. Yaşlılar, olası tehditler, çevrimiçi güvenlik önlemleri ve güvenli dijital alışkanlıklar hakkında genellikle çok az bilgiye sahip oldukları için günümüzün dijital dünyasında çevrimiçi ortamlarda gezinmekte zorluk çekmektedir. Bu eğitim programının amacı, yaşlılara dijital teknolojileri güvenli ve emin bir şekilde kullanmak için ihtiyaç duydukları araçları etkili, uygulamalı ve ilginç bir öğrenme ortamında sunarak bu eksiklikleri gidermektir.

Programın amaçları, yaşlıların internet güvenliği konusundaki bilgilerini artırmak, onlara gerekli becerileri kazandırmak ve dijital teknolojileri güvenli bir şekilde kullanma konusunda kendilerine güvenlerini artırmaktır. Kişisel verileri ve gizliliği korumaya yönelik pratik önlemlerin yanı sıra, eğitim programı yaygın çevrimiçi tehditler ve bunları nasıl tanıyacakları konusunda net bir farkındalık, güvenli çevrimiçi davranışlar konusunda tavsiyeler ve olası tehditleri ve çözümleri gösteren gerçek hayattan senaryolar hakkında bilgiler sunar. Her biri dört saat süren beş kapsamlı kurs ve çevrimiçi tehditlere karşı anlık tepkileri simüle eden on etkileşimli IMPROVE vakası ile program, siber güvenlik tehlikelerinin gerçek hayattaki örneklerini inceleyerek uygulamalı öğrenmeye büyük önem vermektedir. İçerik, talimatlarla birlikte kapsamlı alıştırmalar ve bu eğitim programını sunmak için gerekli araçlar ve kaynaklar her oturumda yer almaktadır.

Bu kaynaklar, öğretmenlere yaşlıların etkileşimli öğrenmeye ilgi duymalarını ve katılmalarını sağlamak için yararlı etkinlikler, malzemeler ve yöntemler sunar. Bu programı başarıyla tamamlayan öğretmenler, yaşlıların dijital yetkinliklerini ve özgüvenlerini geliştirmelerine yardımcı olacak donanıma sahip olacaklardır.

1.2.1 Programın Temel Hedefleri

Yaşlıların Çevrimiçi Tehditler Konusundaki Farkındalığını Artırmak
Katılımcılar, kötü amaçlı yazılım, kimlik avı, dolandırıcılık, kimlik hırsızlığı ve tehlikeli web siteleri gibi en yaygın çevrimiçi tehditleri kapsamlı bir şekilde kavrayacaklardır. Program, katılımcılara uyarı işaretlerini nasıl tanıyacaklarını öğretir ve gerçek hayattan örnekler kullanarak olası tehlikeleri gösterir.

Pratik Dijital Beceriler Geliştirme
Katılımcılar, sosyal medya kullanımı, çevrimiçi bankacılık, alışveriş ve internette gezinme gibi tipik internet görevlerini doğru bir şekilde nasıl gerçekleştirecekleri konusunda kapsamlı bir anlayış kazanacaklardır. Güvenli veri yönetimi, iki faktörlü kimlik doğrulama ve güçlü şifreler üzerinde durulmaktadır.

Güvenli Çevrimiçi Davranışları Teşvik Etmek
Program, gizlilik koruması, güvenli iletişim ve etik dijital etkileşim için en iyi uygulamaların benimsenmesini vurgular. Yaşlılar, kişisel bilgileri nasıl yöneteceklerini, sahte mesajları nasıl tanıyacaklarını ve şüpheli faaliyetlere nasıl uygun şekilde yanıt vereceklerini anlayacaklardır.

Eğitmenlere Uzmanlık Kazandırmak
Eğitimcileri ve kolaylaştırıcıları eğitmek, programın temel bir parçasıdır. Eğitmenler, yaşlılara odaklı çevrimiçi güvenlik eğitimi vermek için gerekli becerileri, kaynakları ve teknikleri edineceklerdir. Bu, grup dinamiklerini yönetme, senaryo tabanlı öğrenme ve etkileşimli öğretim teknikleri hakkında tavsiyeleri kapsar.

Dijital Dışlanmayı Azaltın
Program, dijital okuryazarlığı ve çevrimiçi güvenlik bilgisini geliştirerek, özellikle kentsel alanların dışında yaşayan yaşlıların sosyal ve teknolojik izolasyonunu azaltmayı amaçlamaktadır. Günümüzün dijital dünyasında, katılımcılar dijital cihazları kendi başlarına daha rahat kullanacak ve daha fazla kapsayıcılık sağlayacaklardır.

1.2.2 Beklenen Sonuçlar

- Yaşlılar, internet ortamlarında güvenli bir şekilde gezinmek için gerekli bilgi ve pratik becerileri edineceklerdir.
- Eğitmenler, yaşlılara ilginç ve yararlı siber güvenlik eğitimi verebilecek donanıma sahip olacaklardır.
- Çevrimiçi etkinliklere ve hizmetlere güvenli bir şekilde katılabilen, dijital olarak güçlendirilmiş yaşlılar, topluluklarına fayda sağlayacaktır.

Eğitim programı, öğrenenlerin yaparak öğrenmelerini sağlamak için teoriyi etkileşimli, senaryo tabanlı alıştırmalar, vaka çalışmaları ve grup etkinlikleriyle birleştirir. Her modül, yapılandırılmış bilgiler, pratik görevler ve tartışma fırsatları içerir, böylece yaşlılar bilgilerini anında kullanabilir ve gerçek hayattaki durumlarda güven kazanabilirler. Program ayrıca, öğrenme çıktılarının karşılanmasını sağlayan ve aynı zamanda hem eğitmenlerin hem de katılımcıların kendilerini sürekli geliştirmeleri için geri bildirim sunan değerlendirme ve yansıtma bileşenlerini de içerir.

1.2.3 İyileştirme Vakaları

IMPROVE Vakaları, Siber Güvenlikli Yaşlılar eğitim modüllerini tamamlamak amacıyla tasarlanmış, etkileşimli, senaryo tabanlı öğrenme etkinlikleridir. Bu senaryolar, Modül I-V ile doğrudan ilgilidir ve yaşlıların günlük dijital etkileşimlerinde karşılaşabilecekleri gerçek çevrimiçi durumları gösterir; örneğin, kimlik avı e-postaları, çevrimiçi alışveriş dolandırıcılığı, tehlikeli halka açık Wi-Fi kullanımı ve dolandırıcılık amaçlı yatırım sahtekarlıkları. Etkileşimli Genially içeriği aracılığıyla sunulan senaryolar, katılımcıların olası tehditleri belirlemelerine, bilinçli kararlar almalarına ve riskli çevrimiçi faaliyetlerin etkilerini anlamalarına olanak tanır. IMPROVE vakaları, gerçek hayattaki dijital tehditleri taklit ederek uygulamalı öğrenmeyi teşvik eder ve yaşlıların daha güvenli internet kullanımı için pratik beceriler geliştirmelerine olanak tanır.

IMPROVE vakaları, tematik odak noktalarına ve öğrenme hedeflerine göre eğitim modülleriyle uyumludur.

- **Modül I – Siber Güvenlik Temelleri: Bilgisayarınızı, E-postanızı ve Kişisel Verilerinizi Koruma:** Smishing; Halka Açık Wi-Fi İkilemi.
- **Modül II – Yaşlıları Hedef Alan Yaygın Çevrimiçi Dolandırıcılık Yöntemleri:** Büyükbaba Dolandırıcılığı; Hayırseverlik Dolandırıcılığı Tuzağı.
- **Modül III – Çevrimiçi Bankacılık ve Alışveriş Güvenliği:** Çevrimiçi Alışveriş Dolandırıcılığı; E-posta Kimlik Avı Dolandırıcılığı; Kripto Miraj: Anında Zenginlik İllüzyonu; Altın Getiri – Güvenin Bedeli.
- **Modül IV – Yaşlılar için Güvenli ve Sorumlu Sosyal Medya Kullanımı:** Deepfake Dolandırıcılığı; Çevrimiçi Hizmeti Türü Dolandırıcılığı.
- **Modül V – Yaşlıların Güvenli Dijitalleşmesi:** Genel eğitim içeriği ve faaliyetleri boyunca çapraz olarak ele alınır.

İyileştirme Örneklerine Erişim:

- Kripto Serabı: Anında Zenginlik İllüzyonu
- Çevrimiçi Alışveriş Dolandırıcılığı
- Hayırseverlik Dolandırıcılığı Tuzağı
- SMS Dolandırıcılığı
- Halka Açık Wi-Fi İkilemi
- E-posta Oltalama Dolandırıcılığı
- Büyükanne-büyükbaba Dolandırıcılığı
- Çevrimiçi Hizmet Türü Dolandırıcılığı
- Deepfake Dolandırıcılığı
- Altın Getiriler – Güvenin Bedeli: Bir Yatırım Dolandırıcılığı Vakası

MODÜL I

Siber güvenliğin temelleri: bilgisayarlarınızı, e-postanızı ve kişisel verilerinizi koruma

2. Modül I - Bilgisayarlarınızı, e-postalarınızı ve kişisel verilerinizi koruyan siber güvenlik temelleri

"Siber Güvenlik Temelleri" modülü, teorik bilgileri pratik uygulamalarla birleştirerek dijital güvenlik konusunda eksiksiz bir genel bakış sunar. Katılımcılar, bilgisayar güvenliği, e-posta gizliliği ve kişisel veri korumanın temel ilkeleri hakkında kapsamlı bilgi edineceklerdir. Modül, bilgisayar güvenliği ve e-posta yönetimi gibi önemli alt konuları kapsar ve öğrenciler bu modülde işletim sistemlerini ve yazılımlarını nasıl koruyacaklarını, antivirüs programlarını ve güvenlik duvarlarını nasıl kullanacaklarını ve potansiyel siber tehditleri nasıl tespit edeceklerini öğrenirler. Modül ayrıca şifre güvenliği ve yönetimine odaklanır ve kullanıcılara güçlü şifreler oluşturmayı ve şifre yöneticilerini başarılı bir şekilde kullanmayı öğretir.

Pratik e-posta güvenliği alıştırmaları sunulur ve katılımcılara kimlik avı girişimlerini nasıl tanıyacakları, şüpheli bağlantıları veya dosyaları nasıl belirleyecekleri ve iki faktörlü kimlik doğrulama kullanımı da dahil olmak üzere, yetkisiz etkinlikler için posta kutularını nasıl izleyecekleri öğretilir. Programda ayrıca, ekran kilitleme, kayıp cihazları izleme, yetkisiz fiziksel erişimi önleme ve gelişen tehditlere karşı koruma sağlamak için yazılımları güncel tutma taktikleri de dahil olmak üzere, bilgisayarlar, cep telefonları ve tabletler gibi kişisel cihazların nasıl güvenli hale getirileceği de ele alınır. Son olarak, program kişisel veri yönetimi ve çevrimiçi gizliliğe odaklanarak, öğrencilere sosyal medyada gizlilik ayarlarını nasıl değiştireceklerini, kritik bilgileri nasıl koruyacaklarını ve VPN'leri kullanarak halka açık Wi-Fi ağlarını nasıl güvenli bir şekilde kullanacaklarını öğretir.

Bu alt konuları bir araya getiren eğitim, yaşlıların dijital ortamdaki potansiyel tehditleri anlamalarını sağlamakla kalmaz, aynı zamanda kendilerini savunmak için pratik yöntemler de öğretir. Katılımcılar, modülü daha fazla farkındalık, siber güvenlik sorunlarıyla başa çıkma konusunda daha fazla güven ve gerçek hayattaki senaryolarda edindikleri çözümleri uygulama becerisiyle tamamlayacaklardır.

2.1 Öğrenim Hedefleri

Bu modülün ana hedefi, katılımcılara bilgisayarları, e-posta hesaplarını ve kişisel verileri siber uzaydaki tehditlerden etkili bir şekilde korumak için gerekli pratik bilgi ve becerileri kazandırmaktır. Katılımcılar, potansiyel tehditleri nasıl belirleyeceklerini, riskleri nasıl en aza indireceklerini ve hem kişisel hem de profesyonel yaşamlarında dijital güvenliği artırmak için stratejileri nasıl uygulayacaklarını öğreneceklerdir.

- Saldırıları önlemeye ve verileri yetkisiz erişimden korumaya yardımcı olan siber güvenliğin temel ilkelerini anlamak.
- Güçlü şifreler oluşturma ve bunları güvenli bir şekilde saklama becerilerini geliştirerek ihlallere karşı direnci artırmak.
- Çevrimiçi dolandırıcılığın en yaygın yöntemlerinden biri olan kimlik avı saldırılarını tanımak ve önlemek.
- Şifreleme, ekran kilidi ve konum izleme özellikleri gibi araçları kullanarak kişisel cihazları ve bu cihazlarda depolanan verileri etkili bir şekilde koruyun.
- Kişisel veri sızıntı riskini azaltmak için sosyal medya platformlarındaki gizlilik ayarlarını bilinçli bir şekilde yönetin.
- VPN'ler ve diğer koruyucu araçları kullanarak halka açık Wi-Fi ağlarını güvenli bir şekilde kullanmak için bilgi ve beceriler edinin.

2.2 Yapı, İçerik ve Öğrenim Çıktıları

Bu modülü başarıyla tamamlayan öğrenciler şunları yapabileceklerdir:

- Temel bilgisayar güvenliğine giriş: işletim sistemi ve yazılımı güncelleme, antivirüs programları ve güvenlik duvarları kullanma, bilgisayara yönelik olası saldırıların belirtilerini tanımlama ve bunların meydana gelme riskini en aza indirme.
- Güvenli şifreler oluşturma ve saklama: harf, rakam ve sembollerin benzersiz kombinasyonlarından oluşan güçlü şifreler oluşturma, şifreleri kağıt gibi güvenli olmayan bir şekilde saklamaktan kaçınmak için şifre yöneticilerini kullanma.
- E-posta kimlik avını tespit etmek için pratik senaryolar: örnek kimlik avı mesajlarını analiz etmek ve şüpheli bağlantıları, ekleri veya dil hatalarını nasıl tanıyacağını, şüpheli e-postaları ilgili hizmetlere nasıl bildireceğini öğrenmek.
- Posta kutunuzu izleme ve yetkisiz erişime karşı koruma: iki aşamalı doğrulamayı nasıl kuracağınız, posta kutunuzdaki olağandışı etkinlikleri nasıl izleyeceğiniz ve hackleme girişimlerine nasıl yanıt vereceğiniz.
- Kişisel cihazları (bilgisayarlar, akıllı telefonlar, tabletler) koruma: ekranı kilitleme ve kayıp cihazları bulmanızı sağlayan uygulamaları kullanma, cihazlarınızı yetkisiz kişilerin fiziksel erişiminden koruma.
- Kişisel cihazları (bilgisayarlar, akıllı telefonlar, tabletler) koruma: ekranı kilitleme ve kayıp cihazları bulmanızı sağlayan uygulamaları kullanma, cihazlarınızı yetkisiz kişilerin fiziksel erişiminden koruma.
- Güvenliği artırmak için düzenli yazılım güncellemeleri: cihazlarınızı yeni tehditlerden korumak için düzenli güncellemelerin neden gerekli olduğu ve sistemi otomatik güncellemeler için nasıl yapılandıracağınız.
- Sosyal medyada gizliliğinizi koruma: Popüler sosyal medya platformlarında gizlilik ayarlarını nasıl yapacağınız, hangi bilgilerin gizli tutulması gerektiği ve istenmeyen şekillerde kullanılabilecek verilerin paylaşılmasını nasıl önleyeceğiniz.
- Halka açık Wi-Fi ağlarını güvenli bir şekilde kullanma kuralları: açık Wi-Fi ağlarını kullanmanın riskleri ve halka açık yerlerde internete bağlanırken verilerinizi korumak için VPN'i nasıl kullanacağınız.

2.3 Gündem | Ayrıntılı Oturum Planı

MODÜL I
Siber güvenlik temelleri | Bilgisayarlarınızı, e-postalarınızı ve kişisel verilerinizi koruma

1. Oturum

Hoş geldiniz
Süre *5 dakika*

Öğrenim Hedefleri

- Aktif katılımı teşvik eden açık ve ilgi çekici bir atmosfer yaratmak.

İçerik/ Yöntem

- Katılımcıları karşılamak ve eğitmeni kısaca tanıtmak.
- Eğitim gündemini ve çalışma kurallarını sunmak.
- Katılımcıları kendilerini tanıtmaya teşvik etmek (ad ve siber tehditlerle ilişkili bir kelime).

Materyal
Ek materyal yoktur.

Yorum
Atölyenin amacını basit bir dille sunmak faydalı olabilir.

2. Oturum

Buz kırıcı etkinlik: "Siber güvenlik temelleri"
Süre *15 dakika*

Öğrenim Hedefleri

- Temel siber güvenlik terimlerini öğrenmek ve anlamak.
- Siber güvenlik bilgisini güçlendirmek.

İçerik/Yöntem

- Kavramları tanımlarla eşleştirme alıştırması yapmak.
- Katılımcılara bir çalışma kağıdı verilir (Ek 1). Katılımcıların görevi, her kavramı karşılık gelen tanımla doğru şekilde eşleştirmektir. Alıştırma, liderin kararına bağlı olarak bireysel veya takım bazında yapılır. Görev tamamlandıktan sonra, eğitmen kısa bir tartışma yönetir ve bu tartışma sırasında cevaplar tartışılır, belirsizlikler açıklığa kavuşturulur ve alıştırmanın konusuyla ilgili konular ele alınır. Katılımcıların kendilerini tanıtmaları teşvik edilir (adları ve siber tehditlerle ilişkili bir kelime).

Materyal

- Çalışma kağıdı, Buz kırıcı: "Siber Güvenlik Temelleri" (Ek 1)

Yorum
Bu görev, konuyu tanıtır ve katılımcıların başlangıçtaki bilgi düzeyini değerlendirmenizi sağlar.

3. Oturum

Ders 1: Bilgisayar güvenliği ve e-posta
Süre *20*

Öğrenim Hedefleri

- Sistem ve yazılımınızı güncel tutmanın önemini anlamak.
- Kötü amaçlı yazılım, casus yazılım ve fidye yazılımı dahil olmak üzere farklı türdeki siber tehditleri tanımak.
- Güvenliğinizi sağlamada antivirüs yazılımının rolünü anlamak.
- VPN'ler ve diğer güvenlik araçlarını kullanarak halka açık Wi-Fi ağlarını güvenli bir şekilde kullanmak için gerekli bilgi ve becerileri edinmek.

İçerik/Yöntem

- Temel kavramları açıklayan bir ders: düzenli sistem güncellemelerinin neden önemli olduğu, kötü amaçlı yazılımların sistemlere nasıl sızdığı, antivirüs yazılımının rolü ve güvenli bir Wi-Fi ağını nasıl tanıyacağınız.
- Gerçek hayattan örnekler (ör. bilinen fidye yazılımı saldırıları) kullanarak eski sistemler ve güvenli olmayan cihazlarla ilişkili riskleri açıklayın.
- Otomatik güncellemeleri etkinleştirme ve şüpheli indirmelerden kaçınma gibi en iyi uygulamaları vurgulamak. Konferansı uygulamak için eğitmen, Ek 2'de verilen konu önerilerini kullanabilir.

Materyal

- Tartışılacak konu önerileri (Ek 2)

Yorum

Katılımcıların soru sormalarına izin vererek derslere aktif olarak katılmalarını teşvik etmek faydalı olacaktır.

Etkinlik 1 "Test: Doğru/Yanlış"
Süre *20 dakika*

Öğrenim Hedefleri

- Ders sırasında edinilen bilgilerin pekiştirilmesi, tehditlere karşı farkındalığın geliştirilmesi.

İçerik/Yöntem

- Kurs, katılımcıların eğitmen tarafından verilen çalışma kağıdı (Ek 3) temelinde gerçekleştirilen "Doğru mu, Yanlış mı?" adlı bir test şeklinde bir alıştırma içerir.
- Katılımcılar, cevaplarını bağımsız olarak işaretlemek için 5 dakikaya sahiptir. Bu aşamayı tamamladıktan sonra, eğitmen kısa bir tartışma yönetir ve bu tartışma sırasında doğru cevaplar grup ile tartışılır, önemli konular açıklanır ve yanlış anlaşılmalar düzeltilir. Son olarak, eğitmen testte ele alınan temel içeriği özetler, anlayışı pekiştirir ve dijital güvenlikle ilgili iyi uygulamaları pekiştirir.

Materyal

- Çalışma Kağıdı Test: Doğru/Yanlış (Ek 3)

Yorum

Katılımcıların temel güvenlik uygulamalarına ilişkin anlayışlarını pekiştirmek için testin ardından önemli noktaları özetleyin.

Ara | Süre *5 dakika*

- **Katılımcıların dinlenip düşünmeleri için zaman tanıyın.**
- **Dinlenmek için kısa bir ara verin.**
- **Katılımcıları, bir sonraki ders öncesinde dinlenmeleri ve bir şeyler içmeleri için teşvik edin.**

4. Oturum

Ders 2: E-posta güvenliği ile ilgili pratik alıştırmalar
Süre *30 dakika*

Öğrenim Hedefleri

- Güçlü ve güvenli şifreler oluşturmak için en iyi uygulamaları öğrenin (örneğin, büyük ve küçük harfler, özel karakterler ve sayılar kullanmak).
- Zayıf şifre depolamanın risklerini anlayın ve şifre yöneticileri hakkında bilgi edinin.

İçerik/Yöntem

- Güçlü parolalar oluşturmak için "üç bileşenli kuralı" (uzunluk, karmaşıklık, benzersizlik) açıklayın. Parola yöneticilerinin nasıl çalıştığını gösterin ve avantajlarını tartışın (örneğin, artırılmış güvenlik, kolaylık). Parolaları yeniden kullanmak veya güvenli olmayan dosyalarda saklamak gibi yaygın hataları vurgulayın.

Materyal

- Tartışılacak konuların önerisi (Ek 4)

Yorum

Hatırlanması kolay ancak benzersiz bir cümleye dayalı bir şifre oluşturmak gibi, ilişkilendirilebilir, pratik ipuçları verin.

Etkinlik 2: Güçlü şifreler oluşturma
Süre *20 dakika*

Öğrenme Hedefleri

- Tartışılan yönergeleri izleyerek güçlü ve benzersiz şifreler oluşturma alıştırması yapın.

İçerik/Yöntem

- Alıştırma iki aşamada gerçekleştirilir – önce bireysel olarak, sonra çiftler halinde. Alıştırma için bir çalışma kağıdı (Ek 5) hazırlanmıştır.
- Katılımcılar, güvenlik ilkelerine uygun olarak en az üç güçlü şifre oluşturur ve bunları kartlara yazar. Ardından, bunları eşlerine gösterir ve eşleri şifrelerin uzunluğunu, karmaşıklığını ve benzersizliğini değerlendirir, geri bildirimde bulunur ve iyileştirme önerilerinde bulunur. Sonunda, eğitmen güvenli bir şifrenin özelliklerini tartışır ve tüm grupla bir tartışma başlatarak düşüncelerin ve iyi uygulamaların paylaşılmasını sağlar.

Materyal

- Güçlü Parolalar Oluşturma Çalışma Kağıdı (Ek 5)

Yorum

Katılımcıların, eğitmenlerin talimatlarına göre şu anda kullandıkları şifrelerin güvenli olup olmadığına dikkat etmeleri teşvik edilmelidir.

Ara | Süre *5 dakika*

- **Dinlenmek ve hazırlanmak için zaman tanıyın.**
- **Dinlenmek için kısa bir ara.**
- **Dinlenmek ve rahatlamak için kısa bir mola.**

5. Oturum

Ders 3: Kişisel cihazların ve bilgilerin güvenliği

Süre *30 dakika*

Öğrenim Hedefleri

- Kimlik avı e-postalarını nasıl tanıyacağınız konusunda bilgi edinmek.
- Temel e-posta güvenlik ayarlarının nasıl yapılandırılacağını anlamak.

İçerik/Yöntem

- Yazım hataları, bilinmeyen gönderen adresleri ve acil mesajlar gibi kimlik avının belirgin işaretlerini açıklar. Gmail ve Outlook gibi platformlarda e-posta güvenlik ayarlarının nasıl değiştirileceğini gösterir. Kimlik avı e-postalarına örnekler gösterir ve uyarı işaretlerini nasıl tanıyacağınızı tartışır.

Materyal

Ek materyal gerekmez.

Yorum

İçeriği daha çekici hale getirmek için popüler hizmetlerden (ör. PayPal, Amazon) gerçek kimlik avı vakaları gösterilir.

Etkinlik 3: Kimlik avı e-postalarını analiz etme

Süre *20 dakika*

Öğrenim Hedefleri

- Pratik e-posta analizi – düzensizlikleri tespit etme.

İçerik/Yöntem

- Eğitmen, katılımcılara dağıtılmadan önce örnek bağlantılar, tanınmış şirketlerin isimleri (ör. bankalar, kurye hizmetleri veya alışveriş platformları) gibi ayrıntılarla zenginleştirilmesi gereken bir dizi e-posta şablonuna sahiptir (Ek 6).
- Alıştırma ikili veya küçük gruplar halinde yapılır. Katılımcılar çalışma kağıdındaki (Ek 6) hazırlanan e-postaları analiz eder, şüpheli unsurları belirler ve işaretler. Analiz tamamlandıktan sonra, liderin moderatörlüğünde ortak bir tartışma yapılır.

  Tartışma için önerilen sorular:
  - Bu e-postada hangi uyarı sinyalleri bulunur?
  - Bu tür bir saldırıdan kendinizi nasıl koruyabilirsiniz?
  - Bu tür şüpheli bir e-posta alırsanız ne yapmalısınız?
  - Cevapları grupla tartışmaya hazırlanın.

Materyal

- Çalışma kağıdı, Kimlik Avı E-postası Analizi (Ek 6)

Yorum

Grup analiz sonuçlarının özeti, gerçek ve sahte e-postalar arasındaki temel farkları vurgulayarak.

Ara

Süre 5 dakika

- **Dinlenmek ve hazırlanmak için zaman tanıyın.**
- **Dinlenmek için kısa bir ara.**
- **Dinlenmek ve rahatlamak için kısa bir mola.**

6. Oturum

Ders 4: Kişisel verilerin ve çevrimiçi gizliliğin yönetimi

Süre *30 dakika*

Öğrenim Hedefleri

- Gizlilik politikaları, gizlilik ayarları, kilitler ve güncelleme hakkında bilgi verme. Cihazları korumak için temel güvenlik ayarları hakkında bilgi verme (ör. ekran kilitlerini ve otomatik güncellemeleri etkinleştirme).
- Çevrimiçi gizlilik ayarlarını etkili bir şekilde yönetmeyi anlamak.

İçerik/Yöntem

- Sosyal medyada (Instagram, Facebook) verilerinizi korumanın yollarını, akıllı telefonlardaki gizlilik ayarlarını ve uygulama paylaşım kısıtlamalarını tartışın.
- Eğitmen, Android ve iOS'ta ekran kilitleri, veri şifreleme, uygulama yönetimi ve izin ayarları gibi akıllı telefonlarda ve bilgisayarlarda önemli güvenlik ayarlarını tartışır.
- Çevrimiçi gizlilik yönetimini tartışın – sosyal medya platformlarında gizlilik ayarlarını nasıl yapacağınızı, gönderileri ve kişisel bilgileri kimlerin görebileceğini ve hangi uygulamaların verilerinize erişebileceğini kontrol etmeyi öğrenin.
- Wi-Fi güvenliğini kontrol etme ilkelerini tartışın – güvenli olmayan bağlantıları nasıl tanıyacağınızı, korumasız kamu ağlarından neden kaçınmanız gerektiğini ve evinizdeki internet ağının güvenliğini nasıl artırabileceğinizi.
- Gizlilik ayarlarını düzenli olarak gözden geçirmenin önemini vurgulayın – değişen ihtiyaçlara ve yeni çevrimiçi tehditlere uyum sağlamak için gizlilik ayarlarını periyodik olarak gözden geçirme ve güncelleme önemini vurgulayın.

Materyal

Ek materyal gerekmez.

Yorum

Cihaz güvenliğini ve gizliliğini artırmak için pratik, uygulaması kolay adımlara odaklanın.

Etkinlik 4: Güvenli cihaz yapılandırması
Süre *20 dakika*

Öğrenim Hedefleri

- Kişisel cihazlarda güvenlik ayarlarını yapılandırarak bilgileri uygulamak.

İçerik/Yöntem

- Katılımcılar ekran kilidi kurma, iki aşamalı doğrulamayı etkinleştirme ve gizlilik ayarlarını düzenleme alıştırmaları yapar. Eğitmen gerektiğinde bireysel destek sağlar.

Malzeme

- Akıllı telefonlar ve/veya bilgisayarlar.

Yorum

Katılımcıları, cihazlarını yapılandırırken sorunları gidermeye ve sorular sormaya teşvik edin.

7. Oturum

Tartışma
Süre *10 dakika*

Öğrenme Hedefleri

- Önemli dersleri düşünün.
- Katılımcıları en değerli çıkarımlarını ve kalan sorularını paylaşmaya teşvik edin.

İçerik/Yöntem

- Katılımcıların gözlemlerini, deneyimlerini ve açıklığa kavuşturulması gereken sorularını paylaştıkları, moderatörlü bir tartışma. Eğitmen, önemli noktaları özetler ve soruları yanıtlar.

Malzeme

Ek materyal gerekmez.

Yorum

Katılımcıları, öğrendikleri kavramları günlük çevrimiçi davranışlarıyla ilişkilendirmeleri için teşvik edin.

Özet
Süre *5 dakika*

Öğrenme Hedefleri

- Önemli öğrenme noktalarını özetleyin ve daha fazla öğrenme için kaynaklar sağlayın.
- Katılımcılara teşekkür edin ve oturumu kapatın.

İçerik/Yöntem

- Eğitimden elde edilen temel öğrenme noktalarının özeti.
- Ek kaynakların paylaşılması (ör. siber güvenlik web siteleri, makaleler).
- Katılımcılara katılımları için teşekkür edin ve siber güvenlik uygulamalarını geliştirmeye devam etmeleri için onları teşvik edin.

Materyal

- ❖ Katılımcılar için daha fazla okuma ve öğrenme önerileri (Ek 7)
- ❖ Siber güvenlik web siteleri: Avrupa ve hükümet siber güvenlik kuruluşları

Yorum

Son olarak, kısa bir değerlendirme anketi yapmak faydalı olacaktır.

2.4 Ek Bilgiler

2.4.1 Eğitmenlerin Kendi Kendine Değerlendirmesi

- ➢ Katılımcılara çevrimiçi güvenliğin ve sosyal medyanın bilinçli kullanımının önemini açık ve etkili bir şekilde aktardım mı?
- ➢ Dijital tehditleri daha iyi anlamalarına yardımcı olacak pratik örnekler kullandım mı?
- ➢ Katılımcıların gizlilik ayarlarının ve dolandırıcılık tanıma tekniklerinin teknik yönlerini anladıklarından emin oldum mu?
- ➢ Katılımcıların gizlilik ayarlarının teknik yönlerini anladıklarından ve kimlik avı gibi dolandırıcılıkları tanıyabildiklerinden emin oldum mu?
- ➢ Verilen bilgileri katılımcıların ilerleme düzeyine uyarladım mı?
- ➢ Etkinlikler ve tartışmalar sırasında katılımcıları nasıl dahil ettim?
- ➢ Aktif katılımı, deneyim paylaşımını ve soru sormayı teşvik ettim mi?
- ➢ Kullanılan materyaller ve kaynaklar (ör. sunumlar, testler, pratik alıştırmalar) katılımcılar için yararlı ve uygun muydu?
- ➢ Hazırlanan materyaller açık ve anlaşılır mıydı?

2.4.2 Eğitmenlerin Program Değerlendirmesi

- ➢ Eğitim içeriği yaşlıların ihtiyaçlarıyla ilgili miydi ve onların bilgi ve deneyim düzeylerine uygun şekilde uyarlanmış mıydı?
- ➢ Katılımcılar, siber güvenlik ve çevrimiçi gizliliğin temel ilkelerini anlama fırsatı buldular mı?
- ➢ Testler, pratik alıştırmalar ve kimlik avı örneklerinin analizi gibi etkinlikler, katılımcıların öğrenme sürecini destekledi mi?
- ➢ Tartışmalar, dijital güvenlik konusunda bilginin derinleştirilmesine ve düşünmeye teşvik edilmesine olanak sağladı mı?
- ➢ Elde edilen sonuçlar (örneğin, dijital tehditleri anlama, güvenlik ayarlarını yapılandırma becerisi) modülün amaçlanan eğitim hedefleriyle uyumlu mu?
- ➢ Katılımcılar, güçlü şifreler oluşturma, dolandırıcılığı tanıma ve çevrimiçi gizliliği yönetme gibi temel becerileri edinmişler mi?

2.4.3 Materyaller, Ek Kaynaklar

Ek 1 | Çalışma Sayfası Buz Kırıcı Etkinlik: "Siber Güvenlik Temelleri"

Kavramı doğru tanımla eşleştirin:

Oltalama	**Hassas verileri çalmak için güvenilir kuruluşların kimliğine bürünen dolandırıcılık yöntemi.**
Fidye yazılımı	**Verileri şifreleyen ve serbest bırakılması için fidye talep eden kötü amaçlı yazılım. Hassas verileri çalmak.**
İki Faktörlü Kimlik Doğrulama (2FA)	**İkinci bir kimlik doğrulama faktörü gerektiren ek bir güvenlik katmanı.**
Şifreler ve Parola Yöneticileri	**Farklı hizmetler için güçlü ve benzersiz şifreleri yönetme stratejileri.**
Güvenlik duvarı	**Ağa yetkisiz erişime karşı koruma sağlayan bir güvenlik sistemi.**
Veri Şifreleme	**Verileri okunamaz bir koda dönüştürerek yetkisiz erişime karşı koruma yöntemi.**
VPN (Sanal Özel Ağ)	**Güvenli ve özel internet bağlantıları sağlayan bir teknoloji.**
Güvenli E-posta	**E-posta mesajlarını spam filtreleme ve şifreleme gibi saldırılardan korumak için kullanılan uygulamalar.**
SOC (Güvenlik Operasyon Merkezi)	**siber güvenlik tehditlerini izlemek ve bunlara yanıt vermekten sorumlu bir operasyon merkezi.**

Ek 1 | Çalışma Sayfası Buz Kırıcı Etkinliği: "Siber Güvenlik Temelleri"

Doğru cevaplar

1. **Oltalama** – hassas verileri çalmak için güvenilir kuruluşların kimliğine bürünen dolandırıcılık yöntemi.
2. **Fidye yazılımı** – verileri şifreleyen ve serbest bırakılması için fidye talep eden kötü amaçlı yazılım.
3. **İki Faktörlü Kimlik Doğrulama (2FA)** – ikinci bir kimlik doğrulama faktörü gerektiren ek bir güvenlik katmanı.
4. **Şifreler ve Şifre Yöneticileri** – farklı hizmetler için güçlü ve benzersiz şifreleri yönetme stratejileri.
5. **Güvenlik duvarı** – bir ağa yetkisiz erişime karşı koruma sağlayan bir güvenlik sistemi.
6. **Veri Şifreleme** – verileri okunamaz bir koda dönüştürerek yetkisiz erişimden koruma yöntemi.
7. **Kötü Amaçlı Yazılım** – kullanıcılara veya bilgisayar sistemlerine zarar vermek için tasarlanmış yazılım.
8. **VPN (Sanal Özel Ağ)** – güvenli ve özel internet bağlantıları sağlayan bir teknoloji.
9. **Güvenli E-posta** – spam filtreleme ve şifreleme gibi e-posta mesajlarını saldırılardan korumak için kullanılan uygulamalar.
10. **SOC (Güvenlik Operasyon Merkezi)** – siber güvenlik tehditlerini izlemek ve bunlara yanıt vermekten sorumlu bir operasyon merkezi.

Ek 2 | Tartışılması Önerilen Konular Ders 1 | Bilgisayar ve E-posta Güvenliği

- İşletim sistemleri ve uygulamaların düzenli olarak güncellenmesinin önemi.
- Eski sistemlerin ve güvenli olmayan cihazların riskleri.
- Kötü amaçlı yazılım türleri: virüsler, Truva atları, fidye yazılımları ve nasıl çalıştıkları.
- Kötü amaçlı yazılımların sistemlere sızmasına olanak tanıyan mekanizmalar.
- Siber tehditlere karşı korumada antivirüs yazılımının rolü.
- Saldırılara karşı koruma sağlamak için güvenlik duvarı kullanımı.
- Şifre yöneticilerinin kullanımı dahil olmak üzere şifre yönetimi uygulamaları.
- E-postalardaki tehlikeli ekleri ve şüpheli bağlantıları önlemek için kurallar.
- Gizlilik ve güvenliği korumada veri şifrelemenin önemi.
- Güvenliği sağlamada en iyi uygulama olarak otomatik güncellemeler.
- VPN'ler ve çevrimiçi gizliliği korumadaki rolleri.
- Neden her ücretsiz Wi-Fi ağı güvenli değildir?
- Kimlik avı ve spam'e karşı temel e-posta koruması.
- Güçlü şifreler oluşturmak için en iyi uygulamalar ve bunların güvenlik üzerindeki etkisi.
- Mobil cihaz ve uygulama güvenliği.
- Siber saldırıları önlemede kullanıcı eğitimi ve farkındalığının önemi.

Ek 3 | Çalışma Kağıdı Testi: Doğru/Yanlış

Hangi ifadelerin doğru, hangilerinin yanlış olduğunu işaretleyin.

- İşletim sistemi ve uygulamaların düzenli olarak güncellenmesi yalnızca yeni cihazlar için gereklidir. **Doğru/Yanlış**
- Virüsler veya truva atları gibi kötü amaçlı yazılımlar, güncel olmayan yazılımlar ve güvenlik açıkları yoluyla sistemlere sızabilir. **Doğru/Yanlış**
- Sistem düzenli olarak güncelleniyorsa antivirüs yazılımı gereksizdir. **Doğru/Yanlış**
- Güvenlik duvarı yalnızca cihazlara yönelik fiziksel saldırılara karşı koruma sağlamak için kullanılır. **Doğru/Yanlış**
- Şifre yönetimi ve şifre yöneticilerinin kullanımı, çeşitli hizmetler için güçlü ve benzersiz şifreler oluşturmak açısından çok önemlidir. **Doğru/Yanlış**
- Antivirüs yazılımı yüklüyse, e-postalardaki şüpheli eklerden kaçınmak önemli değildir. **Doğru/Yanlış**
- Veri şifreleme, yetkisiz erişimden gizlilik ve güvenliği korumaya yardımcı olur. Doğru/Yanlış
- Otomatik güncellemeler isteğe bağlıdır, çünkü sistemi manuel olarak güncellemek güvenliği sağlamak için her zaman yeterlidir. **Doğru/Yanlış**
- VPN (Sanal Özel Ağ), çevrimiçi etkinliklerimizi gizleyerek internete güvenli bir bağlantı sağlar. **Doğru/Yanlış**
- Kimlik avı, güvenilir görünen e-postalar yoluyla şifreleri çalmak için kullanılan bir saldırı tekniğidir. **Doğru/Yanlış**
- Güçlü bir şifre yalnızca harflerden oluşmalı ve kullanımı zor olmaması için hatırlanması kolay olmalıdır. Mobil cihazlar, saldırılara daha az maruz kaldıkları için masaüstü bilgisayarlara göre daha az güvenlik önlemi gerektirir. **Doğru/Yanlış**
- Mobil cihazlar, saldırılara daha az maruz kaldıkları için masaüstü bilgisayarlara göre daha az güvenlik önlemi gerektirir. **Doğru/Yanlış**
- Çevrimiçi tehditler hakkında kullanıcı bilgisi, siber saldırıları önlemede çok önemlidir.
- Fidye yazılımı, bir sisteme veya dosyalara erişimi engelleyen ve kilidi açmak için fidye talep eden bir yazılımdır. **Doğru/Yanlış**
- Eski bir işletim sistemi güvenlidir, çünkü eski yazılım sürümleri nadiren saldırıların hedefi olur. **Doğru/Yanlış**

Ek 3 | Çalışma Kağıdı Testi: Doğru/Yanlış

Doğru cevaplar

1. İşletim sistemi ve uygulamaların düzenli olarak güncellenmesi yalnızca yeni cihazlar için gereklidir. **Yanlış**
2. Virüsler veya truva atları gibi kötü amaçlı yazılımlar, eski yazılımlar ve güvenlik açıkları yoluyla sistemlere sızabilir. **Doğru**
3. Sistem düzenli olarak güncelleniyorsa antivirüs yazılımı gereksizdir. **Yanlış**
4. Güvenlik duvarı yalnızca cihazlara yönelik fiziksel saldırılara karşı koruma sağlamak için kullanılır. **Yanlış**
5. Şifre yönetimi ve şifre yöneticilerinin kullanımı, çeşitli hizmetler için güçlü ve benzersiz şifreler oluşturmak açısından çok önemlidir. **Doğru**
6. Antivirüs yazılımı yüklüyse, e-postalardaki şüpheli eklerden kaçınmak önemli değildir. **Yanlış**
7. Veri şifreleme, yetkisiz erişimden gizlilik ve güvenliği korumaya yardımcı olur. **Doğru**
8. Otomatik güncellemeler isteğe bağlıdır, çünkü sistemi manuel olarak güncellemek güvenliği sağlamak için her zaman yeterlidir. **Yanlış**
9. VPN (Sanal Özel Ağ), çevrimiçi etkinliklerimizi gizleyerek internete güvenli bir bağlantı sağlar. **Doğru**
10. Kimlik avı, güvenilir görünen e-postalar yoluyla şifreleri çalmak için kullanılan bir saldırı tekniğidir. **Doğru**
11. Güçlü bir şifre yalnızca harflerden oluşmalı ve kullanımı zor olmaması için hatırlanması kolay olmalıdır. **Yanlış**
12. Mobil cihazlar, saldırılara daha az maruz kaldıkları için masaüstü bilgisayarlara göre daha az güvenlik önlemi gerektirir. **Yanlış**
13. Çevrimiçi tehditler hakkında kullanıcı bilgisi, siber saldırıları önlemede çok önemlidir. **Doğru**
14. Fidye yazılımı, bir sisteme veya dosyalara erişimi engelleyen ve kilidi açmak için fidye talep eden bir yazılımdır. **Yanlış**
15. Eski bir işletim sistemi güvenlidir, çünkü eski yazılım sürümleri nadiren saldırıların hedefi olur. **Yanlış**

Ek 4 | Ders 2 "E-posta Güvenliği Pratik Alıştırmaları" için Önerilen Konular

- Güvenli Şifreler Oluşturma – farklı karakter türleri (büyük harf, küçük harf, rakamlar, özel karakterler) kullanmak da dahil olmak üzere, kırılması zor güçlü şifreler oluşturmanın ilkeleri.
- Parola Yönetimi – Parolaları kağıt notlar gibi güvenli olmayan yerlerde saklamaktan kaçınmak ve güvenli saklama için parola yöneticilerini kullanmak.
- Üç Bileşenli İlke – yüksek güvenlik sağlamak için şifrenin neden uygun uzunlukta, karmaşık ve benzersiz olması gerektiğini açıklamak.
- Parola Yöneticilerinin Rolü – parola yöneticilerinin nasıl çalıştığı ve birden fazla parolayı yönetmede güvenlik ve kolaylık gibi sunduğu avantajlar.
- Yaygın Şifre Yönetimi Hataları – aynı şifreleri farklı hizmetlerde yeniden kullanmanın veya güvenli olmayan dosyalarda saklamanın ne kadar tehlikeli olduğu.
- E-posta Güvenliği Uygulamaları – şüpheli bağlantıları ve ekleri nasıl önleyeceğiniz ve şifreleme gibi ek koruma yöntemlerini nasıl kullanacağınız.

Ek 5 | Çalışma Sayfası "Güçlü Parolalar Oluşturma"
Aşağıdaki ilkelere göre güçlü ve güvenli şifreler oluşturun:

· Uygun uzunluk (en az 12 karakter),
· Karmaşıklık (büyük ve küçük harfler, rakamlar, özel karakterler),
· Benzersizlik (doğum tarihi gibi belirgin kalıplar olmaması).

Bireysel çalışma: En az üç farklı şifre yazın:

Ek 5 | Çalışma Sayfası | Güçlü Şifreler Oluşturma

Çiftler halinde çalışın:

· Bireysel çalışmayı tamamladıktan sonra, başka bir katılımcıyla eşleşin.
· Onlara şifrelerinizi gösterin.
· Şifrelerin tüm kriterleri karşılayıp karşılamadığını işaretlemelerini isteyin (örneğin artı işareti ile).
· Eğitmen, olası iyileştirmeler için yorum ve önerilerde bulunabilir.

Sifre 1

Uzunluk

Karmaşıklık

Çok yönlülük

Notlar

Sifre 2

Uzunluk

Karmaşıklık

Çok yönlülük

Notlar

Sifre 3

Uzunluk

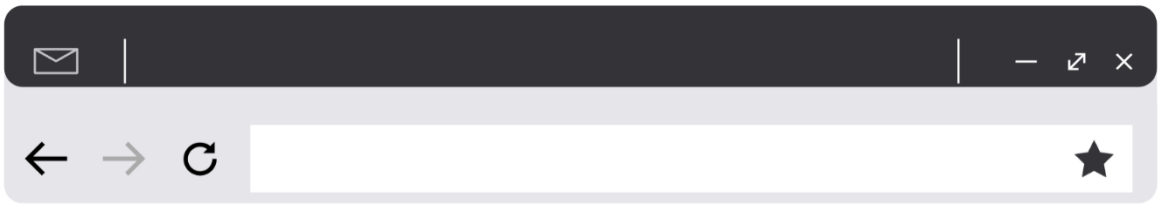
Karmaşıklık

Çok yönlülük

Notlar

Ek 6 | Çalışma Sayfası | Kimlik Avı E-postası Analizi

Aşağıdaki e-postaları dikkatlice okuyun. Bunların kimlik avı e-postaları olduğunu gösteren unsurları belirleyin.



Subject : **Acil! Hesabınız engellendi!**

Sayın kullanıcı

Hesabınızda şüpheli etkinlikler tespit edildiğinden, kişisel verilerinizi korumak amacıyla hesabınız geçici olarak bloke edilmiştir. Kalıcı bloke edilmesini önlemek için lütfen hesabınızı hemen doğrulayın.

Bilgilerinizi doğrulamak ve hesabınızın kilidini açmak için buraya tıklayın: [Kimlik avı bağlantısı]

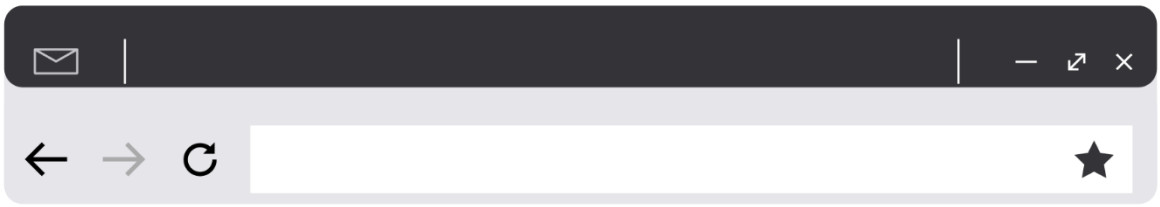
Bu işlemi 24 saat içinde tamamlamazsanız, hesabınız kalıcı olarak bloke edilecektir. Herhangi bir rahatsızlık yaşamamak için lütfen hızlı bir şekilde harekete geçin.

Herhangi bir sorunuz varsa, lütfen teknik destek ekibimizle iletişime geçin.

Saygılarımızla,
Güvenlik Ekibi
[Sahte Şirket]

Ek 6 | Çalışma Sayfası | Kimlik Avı E-postası Analizi

Aşağıdaki e-postaları dikkatlice okuyun. Bunların kimlik avı e-postaları olduğunu gösteren unsurları belirleyin.



Subject : **Bilgilerinizi Güncelleyin! Hesabınızın Doğrulanması Gerekiyor**

Merhaba [Ad],

[Sahte Şirket]'teki hesabınız için kişisel bilgilerinizin derhal güncellenmesi gerekmektedir. Rutin güvenlik kontrolü nedeniyle, hizmetlerimize tam erişim sağlayabilmeniz için verilerinizin güncel olduğundan emin olmamız gerekmektedir. Bilgilerinizi güncellemek için aşağıdaki bağlantıya tıklayın ve hesabınıza giriş yapın:

[Kimlik avı bağlantısı – bilgilerinizi güncellemek için buraya tıklayın]

Bağlantıya tıkladıktan sonra, giriş bilgilerinizi, kredi kartı numaranızı ve diğer hassas bilgilerinizi girmeniz gereken bir sayfaya yönlendirileceksiniz.

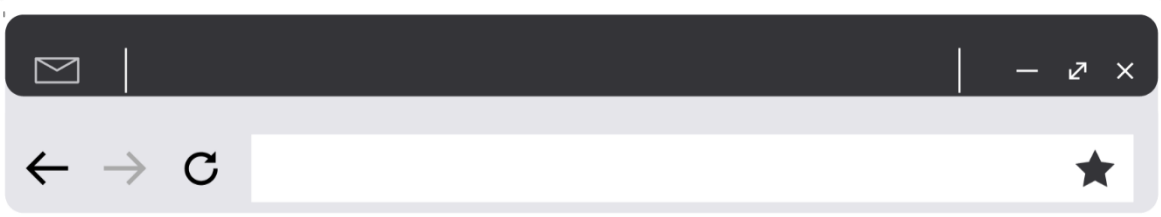
UYARI: Bilgilerinizi 48 saat içinde güncellemezseniz, hesabınız kalıcı olarak askıya alınacaktır.

Anlayışınız ve işbirliğiniz için teşekkür ederiz.

Saygılarımızla
[Sahte Şirket]
Müşteri Destek Ekibi

Ek 6 | Çalışma Sayfası | Kimlik Avı E-postası Analizi

Aşağıdaki e-postaları dikkatlice okuyun. Bunların kimlik avı e-postaları olduğunu gösteren unsurları belirleyin.



Subject : **Gönderi onayı - paket teslim edilemedi**

İyi günler,

Adres bilgilerinizin yanlış olması nedeniyle paketinizi teslim edemedik. Teslimatı yeniden denememiz için lütfen bilgilerinizi hemen doğrulayın.

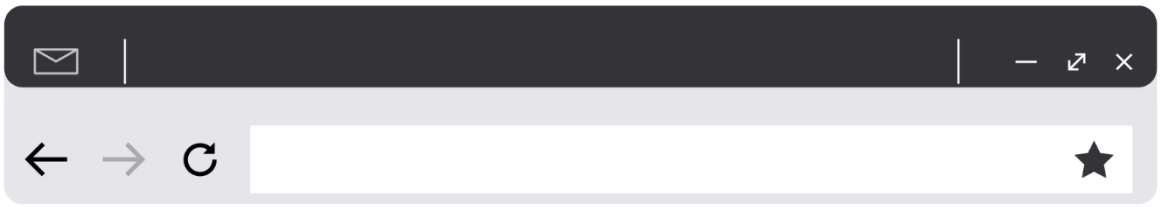
Teslimat bilgilerinizi güncellemek için buraya tıklayın: [oltalama bağlantısı]

24 saat içinde adresinizi onaylamazsanız, paket gönderene iade edilecek ve ek masraflar doğacaktır.

Hızlı yanıtınız için teşekkür ederiz.
Nakliye Ekibi
[Sahte Kurye Şirketi]

Ek 6 | Çalışma Sayfası | Kimlik Avı E-postası Analizi

Aşağıdaki e-postaları dikkatlice okuyun. Bunların kimlik avı e-postaları olduğunu gösteren unsurları belirleyin.



Subject : **Bir e-hediye kartı aldınız! Hemen talep edin!**

Tebrikler!

Rastgele promosyonumuzun kazananı olarak seçildiniz. [Popüler Perakende Ağı]'nda kullanabileceğiniz 500 PLN değerinde bir e-hediye kartı kazandınız.

Ödülünüzü almak için aşağıdaki bağlantıya tıklayın ve bilgilerinizi onaylayın:
[oltalama bağlantısı - e-kartı talep et]

Teklif sadece 12 saat geçerlidir.
Bu fırsatı kaçırmayın!

İyi günler!
Promosyon Departmanı
[Sahte Şirket veya Perakende Ağı]

Ek 7 | Katılımcılar için daha fazla okuma ve öğrenme önerileri

Siber güvenlik web siteleri: Siber güvenlikle ilgilenen Avrupa ve hükümet kuruluşları

1) **ENISA (Avrupa Birliği Siber Güvenlik Ajansı)**
   Web sitesi: https://www.enisa.europa.eu/
   ENISA, siber tehditlerle ilgili raporlar, kılavuzlar ve uyarılar yayınlayan, siber güvenlikle ilgilenen AB ajansıdır.

2) **CERT-EU (AB Kurumları için Bilgisayar Acil Durum Müdahale Ekibi)**
   Web sitesi: https://cert.europa.eu/
   Bu kuruluş, siber tehditleri izler ve Avrupa kurumlarına yönelik siber saldırılara müdahale eder.

3) **EC3 – Europol Siber Suç Merkezi**
   Web sitesi: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime
   Europol, siber suçlar ve veri güvenliği hakkında bilgi sunar.

4) **NCSC UK (Ulusal Siber Güvenlik Merkezi)**
   Web sitesi: https://www.ncsc.gov.uk/
   İngiltere hükümetinin siber güvenlik portalı, vatandaşlar, işletmeler ve kamu kurumları için kılavuzlar, uyarılar ve çevrimiçi kurslar sunmaktadır.

2.5 Modül I - Ön/Son Test

1. Aşağıdakilerden hangisi "oltalama"yı en iyi şekilde tanımlamaktadır?

A) Bilgisayar performansını iyileştirmek için güncellemeleri yüklemek
B) Sahte e-postalar yoluyla insanları kişisel bilgilerini ifşa etmeye ikna etme yöntemi
C) Bir tür antivirüs programı
D) Verileri şifreleme işlemi

2. Düzenli yazılım güncellemeleri neden önemlidir?

A) Bilgisayarınızı yavaşlatır
B) Bilgisayarınızın tasarımını değiştirir
C) Güvenlik açıklarını giderir ve yeni tehditlere karşı koruma sağlar
D) Antivirüs yazılımını kaldırırlar

3. Güvenlik duvarının temel işlevi nedir?

A) İnternet bağlantınızı hızlandırmak
B) Ağa yetkisiz erişime karşı koruma sağlamak
C) Şifreleri güvenli bir şekilde saklamak
D) Spam e-postaları otomatik olarak silmek

4. Aşağıdakilerden en güvenli şifre hangisidir?

A) password123
B) 12345678
C) MyDogIsCute
D) M@rK_82!x

5. Bilinmeyen bir göndericiden kişisel verilerinizi isteyen bir e-posta alırsanız ne yapmalısınız?

A) Hemen bilgilerinizi içeren bir cevap gönderin
B) Bağlantıya tıklayarak ne olduğunu kontrol edin
C) E-postayı silin veya kimlik avı olarak bildirin
D) Arkadaşlarınıza ileterek onları uyarın

6. "İki faktörlü kimlik doğrulama (2FA)" ne için kullanılır?

A) Aynı anda iki şifre kullanmanıza olanak tanır
B) İki tür doğrulama gerektirerek ekstra bir güvenlik katmanı ekler
C) E-postalarınızı otomatik olarak şifreler
D) Giriş verilerinizi saklar

7. Kamuya açık Wi-Fi ağları hakkında aşağıdaki ifadelerden hangisi DOĞRU'dur?

A) Bağlantı ücretsizse her zaman güvenlidir
B) Halka açık Wi-Fi kullanırken hassas verileri girmekten kaçınmalısınız
C) Şifre olmadan güvenle kullanabilirsiniz
D) Verilerinizi otomatik olarak şifreler

8. VPN'in (Sanal Özel Ağ) amacı nedir?

A) İnternet hızınızı artırmak
B) Pop-up reklamları engellemek
C) İnternete güvenli ve özel bir bağlantı sağlamak
D) Şifrelerinizi yönetmek

9. Aşağıdakilerden hangisi fidye yazılımına bir örnektir?

A) Dosyalarınızı şifreleyen ve kilidini açmak için ödeme talep eden yazılım
B) Sisteminizi tarayan bir antivirüs programı
C) Spam e-postaları engelleyen bir araç
D) Bir güvenlik duvarı uygulaması

10. Sosyal medyada gizliliğinizi korumak için iyi bir uygulama nedir?

A) Tam adresinizi ve telefon numaranızı paylaşmak
B) Tüm gönderileri "herkese açık" olarak ayarlamak
C) Gizlilik ayarlarını düzenli olarak gözden geçirmek ve ayarlamak
D) Tüm hesaplar için aynı şifreyi kullanmak

Cevap Anahtarı Özeti

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

MODÜL II

Yaşlıları Hedef Alan Yaygın Çevrimiçi Dolandırıcılık Yöntemleri

3. Modül II - Yaşlıları hedef alan yaygın çevrimiçi dolandırıcılık yöntemleri

Bu dört saatlik modül, yaşlıların çevrimiçi dolandırıcılık ve siber güvenlik tehditlerini tanımalarını, anlamalarını ve kendilerini bunlardan korumalarını sağlar. Pratik stratejiler ve önleyici tedbirler aracılığıyla yaşlıların kendine özgü savunmasızlıklarını ele alır ve dijital teknolojileri güvenli bir şekilde kullanma konusunda güvenlerini artırır. Katılımcılar dolandırıcılıkların nasıl işlediğini öğrenecek, dijital iletişimde uyarı işaretlerini tanımlayacak ve sosyal mühendislik gibi manipülasyon taktiklerini anlayacaklardır. Modül, yaygın dolandırıcılık türlerini (phishing, smishing, vishing) ve teknik tehditleri (kötü amaçlı yazılım, fidye yazılımı, casus yazılım) ele alarak koruma stratejileri sunar. Ayrıca, kişisel veri güvenliğine vurgu yaparak yaşlıların hassas bilgileri güvenle saklama, paylaşma ve yedekleme konusunda kendilerini güçlendirir.

3.1 Öğrenim Hedefleri

Bu modülün amacı, yaşlıların yaygın çevrimiçi dolandırıcılık yöntemlerini, dolandırıcıların kullandığı taktikleri ve dijital tehditleri tanımlama ve önlemenin önemini daha iyi anlamalarını sağlamaktır. Katılımcılara, kimlik avı, smishing, vishing ve kötü amaçlı yazılımlar dahil olmak üzere siber güvenlik risklerinden kendilerini korumak için pratik beceriler ve önleyici tedbirler kazandırmak. Yaşlılara kişisel verilerini nasıl koruyacaklarını, manipülasyon taktiklerini nasıl tanıyacaklarını ve dijital teknolojileri güvenli bir şekilde nasıl kullanacaklarını öğreterek güven ve dijital okuryazarlık becerilerini geliştirmek.

- Dolandırıcılıkların nasıl işlediğini anlamak ve dolandırıcıların kullandığı psikolojik ve teknolojik yöntemleri tanımak.
- Şüpheli içeriği tanımak ve meşru iletişimi sahte iletişimden ayırt etmek.
- Yaygın dolandırıcılık türleri hakkında bilgi edinmek ve siber tehditlerden korunmak için stratejiler öğrenmek.
- Kişisel verileri koruma, yedekleme oluşturma ve dijital araçları güvenli bir şekilde kullanma konusunda güven oluşturmak.

3.2 Yapı, İçerik ve Öğrenim Çıktıları

Bu modülü başarıyla tamamlayan öğrenciler şunları yapabileceklerdir:

- Dolandırıcılıkta kullanılan yaygın teknikleri, teknolojileri ve hedefleri tanımlayabilir ve dolandırıcıların hedeflerini nasıl kandırdıklarını açıklayabilir.
- E-postalar, SMS mesajları, web siteleri ve reklamlar gibi dijital içerikteki uyarı işaretlerini tanımak ve meşru ile şüpheli iletişimler arasında ayrım yapmak.
- Sosyal mühendisliği tanımlayabilir, dolandırıcılar tarafından kullanılan yaygın taktikleri belirleyebilir, yaşlıların neden sıklıkla hedef alındığını anlayabilir ve sosyal mühendislik saldırılarına karşı koruma sağlamak için önleyici tedbirler uygulayabilir.
- Dolandırıcıların yaşlıların duygularını ve yaygın davranış kalıplarını nasıl kullandığını açıklamak ve duygusal baskı altında sakin ve dikkatli kalmak için stratejiler uygulamak.
- Oltalama, smishing, vishing ve sahte kimlik veya finansal dolandırıcılık dahil olmak üzere en yaygın dolandırıcılık türlerini belirleyin ve her birinde kullanılan manipülatif teknikleri açıklayın.
- Kötü amaçlı yazılım, fidye yazılımı, casus yazılım, virüs ve truva atı gibi farklı kötü amaçlı yazılım türlerini belirleyin, bunlara karşı korunma yöntemlerini açıklayın, tehlikeli pop-up'ları tanıyın, bunları güvenli bir şekilde kapatın ve pop-up'ları engellemek ve web sitelerinin güvenliğini doğrulamak için araçlar kullanın.

- Kişisel verileri tanımlayın, dolandırıcılar için hangi türlerin değerli olduğunu ve bunların nasıl istismar edildiğini belirleyin ve kişisel verileri güvenli bir şekilde depolamak ve paylaşmak için en iyi uygulamaları uygulayın.
- Veri yedeklemenin önemini açıklayın, veri kaybına karşı savunmasızlığı azaltmak için ipuçları uygulayın ve teknolojiyi güvenli bir şekilde kullanma konusunda güven oluşturun.

3.3 Gündem I Ayrıntılı Oturum Planı

MODÜL II
Yaşlıları Hedef Alan Yaygın Çevrimiçi Dolandırıcılık Yöntemleri

1. Oturum

Hoş geldiniz
Süre *5 dakika*

Öğrenim Hedefleri

- Konuyu tanıtın ve samimi bir ortam yaratın.

İçerik/ Yöntem

- Oturuma kısa bir giriş yapın, hedefleri özetleyin ve beklentileri belirleyin.
- Modülü ve önemini özetleyerek eğitim için zemin hazırlamak.

Malzeme

- Oturum hedefleri için beyaz tahta veya flip chart.
- Marker kalemler.
- Oturumu özetleyen basılı gündem veya sunum slaytları.

2. Oturum

Buz kırıcı etkinlik: "İki Gerçek ve Bir Yalan"
Süre *10 dakika*

Öğrenim Hedefleri

- Bu etkinliği tamamladıktan sonra, öğrenciler doğru çevrimiçi güvenlik uygulamaları ile dolandırıcılıkta kullanılan yaygın yanılgıları ayırt edebileceklerdir.

İçerik/Yöntem

- Dolandırıcılık ve internet güvenliği ile ilgili temel kavramları sunmayı amaçlayan "İki gerçek ve bir yalan" adlı oyun biçiminde interaktif bir grup egzersizi. Katılımcılar kısa ifadeleri analiz eder, ikili veya küçük gruplar halinde tartışır ve hangisinin yanlış olduğunu (yalan veya efsane) belirler. Eğitmen hızlı geri bildirim sağlar ve şüpheleri giderir.
- Katılımcı, üç ifade içeren bir kart alır ve hangisinin dolandırıcılık olduğunu belirlemelidir. Ardından, katılımcı kendini tanıtır ve adını söyledikten sonra ifadelerini okur ve hangisinin

dolandırıcılık olduğunu düşündüğünü söyler. Diğer herkes dinler ve katılıp katılmadığını belirtir. Katılmayanlar ayağa kalkar ve hangi ifadenin gerçek bir dolandırıcılık olduğunu düşündüklerini açıklar. Sonunda, eğitmen katılımcılara bu dolandırıcılıklardan herhangi biriyle karşılaşıp karşılaşmadıklarını veya bunlardan haberdar olup olmadıklarını sorar.

Malzeme

- Basılı veya dijital ifade setleri listesi (2 doğru + 1 dolandırıcılık) – Ek 1, 2
- Kalem ve kağıt (isteğe bağlı, not almak veya grup tahminleri için)
- Beyaz tahta veya ekran (isteğe bağlı, cevapları ve açıklamaları görüntülemek için)

3. Oturum

Ders 1: Dolandırıcılığı Tanımak

Süre *30 dakika*

Öğrenim Hedefleri

- Katılımcıların dolandırıcılıkların temel mekanizmalarını, dolandırıcıların kullandığı hileleri ve amaçlarını anlamalarına yardımcı olun.

İçerik/Yöntem

- Eğitmen, yaşlıları hedef alan en yaygın dolandırıcılık yöntemlerini slaytlar kullanarak sunar ve bu dolandırıcılık yöntemlerinin amaçlarını ve mekanizmalarını açıklar. Son olarak, eğitmen katılımcılara hangi mekanizmanın onları en çok korkuttuğunu sorar.

Materyal

- Yaşlıları hedef alan farklı olası çevrimiçi dolandırıcılık türlerini ele alan sunum slaytları.
- Sunum için projektör ve dizüstü bilgisayar.
- Dolandırıcılıkların farklı mekanizmalarını ve bu hedeflere ulaşmak için kullanılan hileleri özetleyen el broşürleri - Ek 3.

Etkinlik 1: Şüpheli İçeriği Belirleme

Süre *15 dakika*

Öğrenim Hedefleri

- Katılımcıları e-postalarda, SMS mesajlarında, web sitelerinde ve reklamlarda yer alan uyarı işaretleri konusunda bilgilendirmek.

İçerik/Yöntem

- Katılımcılara gerçek SMS mesajları, e-postalar, web siteleri ve tehlikeli pop-up'ların gerçek ekran görüntüleri gösterilecektir. Katılımcılardan tutarsızlıkları belirlemeleri ve hangi örneklerin meşru, hangilerinin dolandırıcılık olduğunu tespit etmeleri istenecektir. Her kararın ardından, bir şeyin neden dolandırıcılık olduğu ve neden olmadığı açıklanacaktır.
- Eğitmen, iki ekran görüntüsünü yan yana gösterir ve gruptan dolandırıcılık örneği ile gerçek örnek arasındaki farkları belirlemelerini ve hangisinin dolandırıcılık olduğunu tespit etmelerini

ister. Eğitmen, grubun dikkatini ve katılımını sürdürmek için hafif ve ilgi çekici bir üslup kullanarak tüm örnekler için aynı şekilde devam eder. Katılımcılar düşüncelerini paylaştıktan sonra eğitmen her bir örnek çiftini açıklar. Onlara dolandırıcılık olarak tespit edilmesi en zor örnek hangisiydi diye sorar. Ardından eğitmen, el broşürlerini dağıtır.

Materyal

- SMS mesajları, e-postalar, web siteleri ve pop-up'ların gerçek ve sahte ekran görüntülerinin görsel örneklerini içeren sunum slaytları.
- Sunum için projektör ve dizüstü bilgisayar.
- Katılımcıların cevapları işaretlemeleri veya notlar yazmaları için çalışma kağıtları.
- Gerçek örnekleri sahte örneklerden ayırt etmek için kılavuz içeren el broşürleri - Ek 4.

Ara | Süre *5 dakika*

- **Katılımcıların dinlenip düşünmeleri için zaman tanıyın.**
- **Dinlenmek için kısa bir ara.**

4. Oturum

Ders 2: Manipülasyonu anlamak
Süre *30 dakika*

Öğrenim Hedefleri

- Katılımcıların sosyal mühendisliği anlamalarına yardımcı olmak.

İçerik/ Yöntem

- Katılımcılara sosyal mühendislik hakkında bilgi vermek - En yaygın taktiklere genel bakış, dolandırıcıların yaşlıları hedef almasının nedenleri ve bu tür dolandırıcılıklardan korunma yolları. Sosyal mühendislik dolandırıcılığına maruz kalan kişilerin sakin ve soğukkanlı kalmalarını ve baskı altında pes etmemelerini sağlayacak şekilde durumu tanımlamak.
- Eğitmen, korku ve endişe uyandıran phishing ve smishing mesajlarının örneklerini sunar, ardından bu mesajların genellikle kolay ve hızlı bir çözüm önerdiğini belirtir (örneğin, bir bağlantıya tıklayıp banka bilgilerinizi veya kişisel bilgilerinizi girmeniz ya da hatta bir dizi komutu izlemeniz gerekir, böylece "onlar" sorunu sizin için çözebilir). Eğitmen, katılımcılara sosyal mühendislik saldırısı durumunda ne yapacaklarını sorar. Eğitmen, sosyal mühendislik taktikleri ve bunları nasıl tanıyacağınız hakkında ek bilgiler içeren basılı materyaller dağıtır.

Materyal

- Sosyal mühendisliği açıklayan sunum slaytları.
- Gizlilik ayarlarının canlı olarak gösterilmesi için projektör ve dizüstü bilgisayar.
- Sosyal mühendisliğin açıklaması ve bu tür bir dolandırıcılığın hedefi olan kişiler için uyarı işaretleri ve önleyici tedbirler hakkında kılavuz içeren basılı el broşürleri - Ek 5.

Etkinlik 2: Sosyal Mühendislik Canlı
Süre *20 dakika*

Öğrenim Hedefleri

- Katılımcılara güvenli bir ortamda farklı sosyal mühendislik yöntemlerini deneyimleme fırsatı vermek.

İçerik/Yöntem

- Katılımcılara, bazıları sosyal mühendislik olan, bazıları ise olmayan farklı senaryolar sunulacaktır. Sosyal mühendislik senaryoları, katılımcıların duygularını ve davranışlarını hedef alacaktır.
- Eğitmen, katılımcılardan beş kişilik gruplar oluşturmalarını ister. Eğitmen çalışma kağıtlarını dağıtır ve gruplara talimatlar verir. Görevleri, hangilerinin dolandırıcılık hangilerinin gerçek olduğunu belirlemek ve kararlarının gerekçelerini yazmaktır. Gruplar tüm senaryoları inceleyip kararlarını verdikten sonra, eğitmen bulgularını grupla paylaşmalarını ister. Eğitmen, senaryolar hakkında tartışmayı yönetir ve katılımcılara neden bazılarının gerçek, bazılarının ise dolandırıcılık olduğunu düşündüklerini, kendileri bu durumun içinde olsaydı hangi senaryonun en çok korku uyandıracağını ve nedenini sorar.

Materyal

- Farklı senaryoların bulunduğu basılı el broşürleri.
- Katılımcıların hangi senaryoların dolandırıcılık olduğunu ve hangilerinin olmadığını not ettikleri çalışma kağıdı – Ek 6.

Ara | Süre *5 dakika*

- **Dinlenmek ve bir sonraki oturuma hazırlanmak için zaman tanıyın.**
- **Dinlenmek için kısa bir ara.**

5. Oturum

Ders 3: En yaygın dolandırıcılık türleri
Süre *30 dakika*

Öğrenim Hedefleri

- Daha önce bahsedilen dolandırıcılık türlerini tazelemek için, smishing, vishing ve phishing gibi en yaygın dolandırıcılık türlerine hızlı bir genel bakış.
- Önceki derslerde verilen bilgilere kötü amaçlı yazılımlar eklenir.

İçerik/Yöntem

- En yaygın dolandırıcılık yöntemlerine hızlı bir genel bakış. Phishing, smishing, wishing, sahte kimlikler ve para dolandırıcılığı. Ayrıca katılımcılara kötü amaçlı yazılımlar, bunların ne olduğu ve nasıl tespit edileceği hakkında bilgi verilmesi.
- Eğitmen, en yaygın dolandırıcılık yöntemleri ve kötü amaçlı yazılımlar hakkında en önemli bilgileri slaytlar kullanarak açıklar. Ardından, bunları açıklayan materyaller dağıtır ve herkesin

her şeyi olabildiğince net bir şekilde anladığından emin olmak için eğitim katılımcılarıyla bu materyalleri tartışır. Son olarak, katılımcılara internette hangi işaretlere dikkat etmeleri gerektiğini bilip bilmediklerini sorar.

Materyal

- Phishing, vishing, smishing dolandırıcılıklarının örneklerini gösteren sunum slaytları.
- En yaygın dolandırıcılık örneklerini göstermek için projektör ve dizüstü bilgisayar.
- En yaygın dolandırıcılık ve kötü amaçlı yazılımları, bunların ne olduğunu, kurbana nasıl zarar verebileceğini ve nasıl tanınabileceğini ayrıntılı olarak açıklayan basılı el broşürleri - Ek 7.

Etkinlik 3: Kötü Amaçlı Yazılımları Tespit Etme
Süre *20 dakika*

Öğrenim Hedefleri

- Farklı türdeki kötü amaçlı yazılımları tanıma becerisini geliştirmek.

İçerik/Yöntem

- Katılımcıların el broşürleri aracılığıyla farklı türdeki kötü amaçlı yazılımları tanımlayıp tartıştıkları grup etkinliği.
- Eğitmen, katılımcıların üçer kişilik gruplar halinde kötü amaçlı yazılımlar hakkındaki bilgilerini test edeceklerini açıklar. Eğitmen senaryoları dağıtır ve katılımcılardan bunları okumalarını ister. Katılımcıların görevi, hangi tür yazılımın kullanıldığını (Truva atı, virüs, reklam yazılımı, fidye yazılımı veya casus yazılım) belirlemek ve her senaryonun altındaki soruları cevaplamaktır. Her grup cevaplarını diğer gruplarla paylaşır. Eğitmen daha sonra cevap kağıtlarını dağıtır ve katılımcılardan cevapları gözden geçirmelerini ve kullanılan yazılımı tanıma ve bu tür saldırılara karşı korunma yöntemlerinin temel unsurlarını analiz etmelerini ister. Son olarak, eğitmen katılımcılara hangi yazılım türünün en zararlı, hangisinin en az zararlı olduğunu sorar.

Materyal

- Kötü amaçlı yazılımların açıklamalarını içeren el broşürleri.
- Katılımcıların verilen örnek için yazılımın ne olduğunu, cihaza ne yaptığını ve verilen örnek için önleyici tedbirlerin neler olduğunu yazmaları için çalışma kağıtları.
- Katılımcı El Broşürü – Kötü Amaçlı Yazılımları Tespit Etme - Ek 8

Ara | Süre 5 dakika

- **Dinlenmek ve hazırlanmak için zaman tanıyın.**
- **Dinlenmek için kısa bir ara.**

6. Oturum

Ders 4: Temel Veri Koruma ve Veri Yedekleme
Süre *30 dakika*

Öğrenim Hedefleri

- Katılımcılar, kişisel verileri ve dolandırıcılar için hangi verilerin değerli olduğunu tanımlayabileceklerdir. Ayrıca veri yedeklemenin öneminin de farkında olacaklardır.

İçerik/Yöntem

- Kişisel verilerin açıklanmasıyla sunum. Katılımcılar, verilerin paylaşılmasının güvenli olduğu ve olmadığı konular hakkında bilgilendirilecek, kendilerine karşı kullanılabilecek verileri belirlemenin önemi konusunda bilgilendirileceklerdir. Katılımcılar ayrıca hangi verilerin yedeklenmesi gerektiği ve nedeni hakkında da bilgilendirileceklerdir.
- Eğitmen, basılı materyaller dağıtır ve slaytlar kullanarak öğrencilere içeriği anlatır, şunları açıklar: kişisel bilgi kategorileri, hangi verilerin yanlış ellerde zararlı olabileceği ve nedeni, kişisel verileri çevrimiçi olarak nerede paylaşabileceğimiz, çevrimiçi olarak asla paylaşmamamız gerekenler, yedekleme nedir, yedeklemeler sizi kötü amaçlı yazılım saldırılarından nasıl koruyabilir, güvenli yedekleme için en iyi uygulamalar ve verilerinizi güvende tutmak için ipuçları.
- Eğitmen tartışmayı teşvik eder ve katılımcılara, yazılım kullanılarak gerçekleştirilen bir siber saldırı girişimine tanık olup olmadıklarını veya böyle bir saldırıya katılıp katılmadıklarını sorar. Son olarak, eğitmen katılımcılara önemli verilerin yedek kopyalarını artık alacaklarını sorar.

Materyal

- Kişisel veriler, çevrimiçi ortamda nerede ve neyi paylaşabileceğimiz ve veri yedekleme hakkında gerekli bilgilerle ilgili sunum.
- Kişisel verilerle ilgili kılavuzlar, nerede paylaşılabileceği, nerede paylaşılamayacağı ve önemli bilgilerin yedeklenmesinin neden önemli olduğu hakkında broşürler - Ek 9.

Etkinlik 4: Dosyaları bir bulut hizmetine ve harici bellek depolama alanına yedekleme.
Süre *20 dakika*

Öğrenim Hedefleri

- Bu bilgiler, katılımcıların doğrulanmış bulut hizmetleri ve harici sabit sürücüler kullanarak dosyaları güvenli bir şekilde yedeklemelerine yardımcı olacaktır.

İçerik/Yöntem

- Katılımcılar, kendilerine tanıdık bir bulut hizmetine (Google Drive, Dropbox, iCloud, OneDrive) sahte dosyaları yedekleyeceklerdir. Aynı sahte dosyaları bir USB sürücüsüne de yedekleyeceklerdir.
- Eğitmen, dosyaları harici bir sürücüye ve bir bulut hizmetine yedekleme hakkında bilgi içeren materyalleri dağıtır. Eğitmen, bir ekran veya projektörde gösterim yapar ve katılımcılar, dosyaları bilgisayardan harici bir sürücüye kopyalama ve dosyaları bir bulut hizmetine yükleme

sürecini takip eder. Eğitmen, yardıma ihtiyaç duyanlara yardımcı olur. Sonunda düşünülmesi gereken sorular: "Dosyalarınızı kendi başınıza yedekleyebileceğinizi düşünüyor musunuz, yoksa ek bilgiye ihtiyaç duyan var mı?", "Bugünün konusu olan çevrimiçi dolandırıcılık hakkında sormak istediğiniz veya görüşlerinizi paylaşmak istediğiniz bir şey var mı?"

Malzeme

- Yedeklenebilecek sahte dosyalar.
- Bilgisayarlar ve USB sürücüler.
- Öğretmenin sürecin bir örneğini gösterebilmesi için dizüstü bilgisayar ve projektör.
- Dış sürücüye ve bulut hizmetine dosya yedekleme talimatlarını içeren el broşürleri - tüm büyük bulut sağlayıcıları için özel olarak hazırlanmış talimatlar - Dosyalarınızı Yedekleme - Ek 10

7. Oturum

Tartışma | Süre *10* dakika

Öğrenim Hedefleri

- Çevrimiçi dolandırıcılık konusunda farkındalık dolu proaktif bir zihniyet teşvik etmek.
- Eğitimi özetlemek ve katılımcıların çevrimiçi dolandırıcılıklardan kendilerini nasıl koruyacaklarını anlamalarını sağlamak.

İçerik/ Yöntem

- En yaygın çevrimiçi dolandırıcılıkların temel noktalarını gözden geçirin. Aşırı derecede zaman hassasiyeti olan bir şekilde iletilen bir şey varsa, bunun olası bir dolandırıcılık olabileceğinin farkında olunması gerektiği konusunda farkındalık oluşturun.
- Çevrimiçi dolandırıcılıkla karşılaşılan bir durumun nasıl ele alınacağına ilişkin grup tartışması. Karşılaşabileceğimiz şüpheli faaliyetlerin temel belirtileri nelerdir ve bu tür senaryolarda ne yapmalıyız?
- Eğitmen, çevrimiçi dolandırıcılık kurbanı olursanız ne yapmanız gerektiğine dair en önemli bilgileri özetler ve şüpheli faaliyetlerin temel belirtilerini listeler. Eğitmen katılımcılara teşekkür eder ve destekleyici materyaller sağlar, ardından çevrimiçi dolandırıcılığı nasıl tanıyacağınız ve bu konuda ne yapmanız gerektiğine dair bir kontrol listesi dağıtır. Eğitmen katılımcılara açık uçlu sorular sorar: "Bugün çevrimiçi dolandırıcılık ve bundan kendinizi nasıl koruyacağınız konusunda öğrendiğiniz en önemli şey nedir?" "Artık dolandırıcılığı fark etme ve önleme konusunda kendinizi daha güvende hissediyor musunuz?" "Bugünkü oturumda daha fazla bilgi almak istediğiniz bir konu veya soru var mı?"

Malzeme

- Dolandırıcılıkları tanımak için beyin fırtınası yapmak üzere beyaz tahta ve kalemler.
- El broşürü: çevrimiçi dolandırıcılıklarla ilgili kontrol listesi - Ek 11.
  El broşürleri Çevrimiçi güvenlik kontrol listesi.

Özet
Süre 5 dakika

Öğrenme Hedefleri

- Oturumu özetleyin ve katılımcıları güvenli bir şekilde uygulamaya devam etmeleri için teşvik edin.

İçerik/Yöntem

- Önemli noktaların son özeti, gelecekteki öğrenim için ek kaynaklar sağlayın.

Materyal

- Önemli noktalar ve kaynakları içeren el broşürleri.

3.4 Ek Bilgiler

3.4.1 Eğitmenlerin Kendi Kendilerini Değerlendirmeleri

- Çevrimiçi tehlikelerin önemini etkili bir şekilde aktardım mı?
- Katılımcıların önleyici tedbirleri anladığından emin oldum mu?
- Katılımcıları etkinliklere ve tartışmalara nasıl dahil ettim?
- Kaynaklar ve materyaller katılımcılar için yararlı mıydı?

3.4.2 Eğitmenlerin Program Değerlendirmesi

- Eğitimin içeriği yaşlılar için uygun ve açık mı?
- Etkinlikler ve tartışmalar, katılımcıların materyali öğrenmelerine yardımcı olmak açısından etkili miydi?
- Sonuçlar modülün öğrenme hedefleriyle uyumlu mu?

3.4.3 Materyalleri, Ek Kaynaklar

Ek 1 | İki gerçek ve bir aldatmaca

Set 1

Dolandırıcılar genellikle güvendiğiniz biri gibi davranırlar.

Meşru şirketler size asla e-posta göndermez.

Kimlik avı e-postaları genellikle aciliyet hissi yaratır.

Set 2

Banka PIN kodunuzu asla kimseyle paylaşmamalısınız.

"Https" ile başlayan tüm web siteleri %100 güvenlidir.

Dolandırıcılar sizi kandırmak için resmi görünümlü logolar

Set 3

Fidye yazılımı bilgisayarınızı kilitleyebilir.

Yabancı pop-up'lara tıklamak, kötü amaçlı yazılım yüklemesine yol

Bir arkadaşınızdan gelen ekleri kontrol etmeden açmak güvenlidir.

Set 4

Sosyal mühendislik genellikle duygusal manipülasyonu içerir.

Devlet kurumları her zaman önce telefonla sizinle iletişime geçer.

Yaşlılar, algılanan savunmasızlıkları nedeniyle sıklıkla hedef alınır.

Set 5

Aynı şifreyi birden fazla hesapta kullanmak sorun değildir.

Güçlü bir şifre harfler, rakamlar ve semboller içerir.

İki faktörlü kimlik doğrulama kullanmak ekstra koruma sağlar.

Set 6

Dolandırıcılar, gerçek bir numara gibi arayan kimliğini sahte olarak

Çevrimiçi bir çekilişte tam adresinizi vermek güvenlidir.

İstenmeyen tekliflere karşı her zaman dikkatli olun.

Set 7

Smishing, kısa mesaj yoluyla gönderilen bir dolandırıcılık türüdür.

Kötü amaçlı yazılımlar yalnızca eski bilgisayarları etkiler.

Antivirüs yazılımı, kötü amaçlı saldırılara karşı koruma sağlar.

Set 8

Dolandırıcılar teknik destek personeli gibi davranabilir.

Aktif olup olmadığını kontrol etmek için bilinmeyen bağlantılara tıklamalısınız.

Kişisel bilgilerinizi girmeden önce her zaman URL'leri kontrol edin.

Set 9

Sahte iş teklifleri, kişisel bilgilerinizi çalmak için kullanılabilir.

Dolandırıcılık sadece teknolojiye aşina olmayan kişilere olur.

Çevrimiçi reklamlar bazen dolandırıcı sitelere yönlendirebilir.

Set 10

Bazı dolandırıcılık yöntemlerinde ödeme olarak hediye kartları istenir.

Güvenilir uygulama mağazalarından uygulama indirmek

Giriş bilgilerinizi yakın arkadaşlarınızla paylaşmalısınız.

Set 11

Dolandırıcılar bazen sizi

Her açılır pencere uyarısı gerçek bir virüs uyarısıdır.

Harekete geçmeden önce mesajları doğrulamak önemlidir.

Set 12

Meşru şirketler e-posta yoluyla kişisel bilgi istemez.

Halka açık Wi-Fi ağları her zaman güvenli ve kullanımı

Cihazınızı güncellemek, güvenlik açıklarını gidermeye yardımcı olur.

Set 13

Dolandırıcılık, sosyal medya platformlarında da gerçekleşebilir.

Dolandırıcı amaçlı bir e-postadaki "abonelikten çık"a tıklamak zararsızdır.

Şüpheli etkinlikleri platforma

Set 14

Seyahat planlarınızı çevrimiçi olarak herkese açık bir şekilde paylaşabilirsiniz.

Dolandırıcılar sosyal medya paylaşımlarınızı izleyebilir.

Yabancılardan gelen arkadaşlık

Set 15

Yedek kopyalar, saldırı durumunda verilerinizi korur.

Yazılım güncelleme hatırlatmalarını görmezden gelmelisiniz.

Her hesap için güçlü ve benzersiz şifreler kullanın.

Ek 2 | Doğru Cevaplar

Set 1

- Doğru – Dolandırıcılar genellikle güvendiğiniz biri gibi davranırlar.
- Yanlış – Meşru şirketler size asla e-posta göndermez. (Bu bir efsanedir. Meşru şirketler kullanıcılarla e-posta yoluyla iletişime geçebilir, ancak hassas kişisel veya finansal bilgiler talep etmezler.)
- Doğru – Kimlik avı e-postaları genellikle aciliyet hissi yaratır.

Set 2

- Doğru – Banka PIN kodunuzu asla kimseyle paylaşmamalısınız.
- Yanlış – "https" ile başlayan tüm web siteleri tamamen güvenlidir. (Bu bir efsanedir. "https", şifrelemeyi gösterir, meşruiyeti değil.)
- Doğru – Dolandırıcılar, kullanıcıları aldatmak için resmi görünümlü logolar kullanabilir.

Set 3

- Doğru – Fidye yazılımı, kullanıcıların bilgisayarlarına erişimini engelleyebilir.
- Doğru – Bilinmeyen pop-up'lara tıklamak kötü amaçlı yazılım yükleyebilir.
- Yanlış – Bir arkadaşınızdan gelen ekleri kontrol etmeden açmak güvenlidir. (Bu bir efsanedir. Güvenilir kişilerden gelen ekler de virüs bulaşmış olabilir.)

Set 4

- Doğru – Sosyal mühendislik genellikle duygusal manipülasyona dayanır.
- Yanlış – Devlet kurumları her zaman önce telefonla bireylerle iletişime geçer. (Bu bir efsanedir. Resmi iletişim genellikle posta yoluyla yapılır.)
- Doğru – Yaşlılar, savunmasız oldukları düşünülerek sıklıkla hedef alınırlar.

Set 5

- Yanlış – Aynı şifreyi birden fazla hesapta kullanmak kabul edilebilir. (Bu bir efsanedir. Şifrelerin tekrar kullanılması güvenlik risklerini artırır.)
- Doğru – Güçlü şifreler harf, rakam ve sembollerin bir kombinasyonunu içerir.
- Doğru – İki faktörlü kimlik doğrulama, ek bir güvenlik katmanı sağlar.

Set 6

- Doğru – Dolandırıcılar arayan kimliği bilgilerini sahte olarak gösterebilirler.
- Yanlış – Çevrimiçi hediye çekilişlerinde tam adresinizi paylaşmak güvenlidir. (Bu bir efsanedir. Kişisel bilgiler dolandırıcılık için kötüye kullanılabilir.)
- Doğru – İstenmeyen tekliflere her zaman dikkatle yaklaşılmalıdır.

Set 7

- Doğru – Smishing, kısa mesaj yoluyla gönderilen dolandırıcılık anlamına gelir.
- Yanlış – Kötü amaçlı yazılımlar yalnızca eski bilgisayarları etkiler. (Bu bir efsanedir. Herhangi bir cihaz etkilenebilir.)
- Doğru – Antivirüs yazılımı, kötü amaçlı tehditlere karşı koruma sağlar.

Set 8

- Doğru – Dolandırıcılar teknik destek hizmetleri gibi davranabilirler.
- Yanlış – Bilinmeyen bağlantılar, meşru olup olmadıklarını kontrol etmek için tıklanmalıdır. (Bu bir efsanedir. Bilinmeyen bağlantıları tıklamak tehlikeli olabilir.)
- Doğru – Kişisel bilgileri girmeden önce URL'ler her zaman kontrol edilmelidir.

Set 9

- Doğru – Sahte iş teklifleri kişisel bilgileri çalmak için kullanılabilir.
- Yanlış – Dolandırıcılar yalnızca dijital becerileri düşük kişileri hedef alır. (Bu bir efsanedir. Herkes hedef alınabilir.)
- Doğru – Çevrimiçi reklamlar bazen kullanıcıları dolandırıcılık sitelerine yönlendirebilir.

Set 10

- Doğru – Bazı dolandırıcılık yöntemlerinde hediye kartlarıyla ödeme talep edilir.
- Doğru – Güvenilir uygulama mağazalarından uygulama indirmek genellikle daha güvenlidir.
- Yanlış – Giriş bilgileri yakın arkadaşlarla paylaşılmalıdır. (Bu bir efsanedir. Giriş bilgileri asla paylaşılmamalıdır.)

Set 11

- Doğru – Dolandırıcılar genellikle kurbanları baskı altına almak için korkuyu kullanır.
- Yanlış – Her açılır pencere uyarısı gerçek bir virüs tehdidini gösterir. (Bu bir efsanedir. Birçok uyarı sahte olabilir.)
- Doğru – Mesajlar, harekete geçmeden önce her zaman doğrulanmalıdır.

Set 12

- Doğru – Meşru şirketler e-posta yoluyla kişisel bilgi talep etmez.
- Yanlış – Halka açık Wi-Fi ağları her zaman güvenlidir. (Bu bir efsanedir. Halka açık ağlar kişisel verileri açığa çıkarabilir.)
- Doğru – Düzenli yazılım güncellemeleri, güvenlik açıklarının giderilmesine yardımcı olur.

Set 13

- Doğru – Sosyal medya platformlarında dolandırıcılık meydana gelebilir.
- Yanlış – Dolandırıcılık e-postalarında "abonelikten çık" seçeneğine tıklamak zararsızdır. (Bu bir efsanedir. Kullanıcının aktif bir hedef olduğunu teyit edebilir.)
- Doğru – Şüpheli etkinlikler ilgili platforma bildirilmelidir.

Set 14

- Yanlış – Seyahat planlarını çevrimiçi olarak paylaşmak güvenlidir. (Bu bir efsanedir. Bu tür bilgiler dolandırıcılar tarafından istismar edilebilir.)
- Doğru – Dolandırıcılar sosyal medya faaliyetlerini izleyebilir.
- Doğru – Tanımadığınız kişilerden gelen arkadaşlık isteklerine dikkatli yaklaşılmalıdır.

Set 15

- Doğru – Veri yedeklemeleri, siber saldırı durumunda bilgileri korur.
- Yanlış – Yazılım güncelleme hatırlatıcıları göz ardı edilmelidir. (Bu bir efsanedir. Güncellemeler güvenlik açısından çok önemlidir.)
- Doğru – Her hesap için güçlü ve benzersiz şifreler kullanılmalıdır.

Ek 3 | Yaşlıları Hedef Alan Çevrimiçi Dolandırıcılıkta Kullanılan Mekanizmalar

1. Kimlik Avı (E-posta Dolandırıcılığı)

Yaşlılar, güvenilir kaynaklardan (bankalar, sağlık hizmetleri vb.) gelmiş gibi görünen e-postalar alırlar.

Hile: Sahte bağlantılar veya giriş sayfaları

Amaç: Kişisel veya finansal bilgileri çalmak

2. Smishing (SMS Dolandırıcılığı)

Dolandırıcılar sahte teslimat bildirimleri, ödül uyarıları veya uyarılar içeren SMS mesajları gönderir.

Hile: Acil dil + kötü amaçlı siteye bağlantı

Amaç: Kötü amaçlı yazılım yüklemek veya özel verileri toplamak

3. Vishing (Sesli Arama Dolandırıcılığı)

Dolandırıcılar, banka, teknik destek veya devlet kurumlarından arıyormuş gibi davranarak telefon görüşmeleri yaparlar.

Hile: Sahte arayan kimliği + duygusal baskı

Amaç: Banka bilgilerini veya uzaktan erişim elde etmek

4. Sahte Web Siteleri (Spoofing)

Yaşlılar, gerçek web sitelerine (bankalar, mağazalar, tıbbi portallar) benzeyen sahte web sitelerine yönlendirilir.

Hile: Hafifçe değiştirilmiş URL'ler (ör. paypa1.com)

Amaç: Giriş veya ödeme bilgilerini ele geçirmek

5. Teknik destek dolandırıcılığı (e-posta dolandırıcılığı)

Pop-up'lar veya aramalar, "virüs" veya bilgisayar sorunu olduğu konusunda uyarıda bulunur ve yaşlıları yardım almaya teşvik eder.

Hile: Sahte hata mesajları + uzaktan erişim talepleri

Amaç: Cihazı kontrol etmek veya kredi kartı verilerini çalmak

6. Romantik Dolandırıcılık

Sosyal medya veya tanışma sitelerinde dolandırıcılar, kurbanları manipüle etmek için duygusal bağlar kurar.

Hile: Sahte fotoğraflar, hikayeler ve sevgi gösterileri

Amaç: Yaşlıları para göndermeleri için ikna etmek

7. Yatırım veya piyango dolandırıcılığı

Büyük kazanç vaatleri veya ön ödeme gerektiren "kazandınız" mesajları.

Hile: Sahte belgeler, aciliyet veya resmi gibi görünen isimler

Amaç: Havale, kripto para veya hediye kartları elde etmek

Ek 4 | Dolandırıcılığı Tespit Etme: Hızlı Kılavuz El Broşürü

Bu kontrol listesini kullanarak bir mesajın, e-postanın, web sitesinin veya reklamın gerçek mi sahte mi olduğuna karar verin.

1. Göndereni veya kaynağı kontrol edin

- *E-posta adresi / telefon numarası: Gönderenin bilgileri şüpheli veya tanıdık gelmiyor mu?*

✗ ***Sahte:*** *support@paypal-secure123.com*

✓ ***Gerçek:*** *support@paypal.com*

- *Yanlış yazılmış marka adları veya garip URL'ler:*

✗ *netfflix-billing.com*

✓ *netflix.com*

2. Aciliyet veya baskı olup olmadığına bakın

- Mesaj sizi korkutmaya veya acele ettirmeye çalışıyor mu?
  "Hemen harekete geçin, yoksa hesabınız kilitlenecek!"
  "Yasal işlemden önce son uyarı!"

Gerçek şirketler sizi bu şekilde tehdit etmez veya baskı yapmaz.

3. Dil ve Tonu İnceleyin

- Yazım ve dilbilgisi hatalarını arayın
- Üslup çok mu rahat ya da çok mu agresif?
- Kulağa doğal gelmiyor mu veya çeviri gibi mi geliyor?
  ✗ **Sahte:** "Sayın Müşteri, hesabınız acilen bloke edilmiştir, lütfen hemen harekete geçin."
  ✓ **Gerçek:** "Hesabınızda olağandışı bir hareketlilik tespit ettik. Lütfen kontrol ediniz."

4. Tıklamadan önce bağlantıyı kontrol edin

- Bağlantıların üzerine fareyi getirerek bağlantının gerçekte nereye yönlendirdiğini görün
- URL, gerçek şirketin web sitesiyle eşleşiyor mu?
  ✗ **Sahte:** http://paypal.verify-now-support.com
  ✓ **Gerçek:** https://www.paypal.com

5. Kişisel Bilgi İsteğine Dikkat Edin

Gerçek şirketler asla şunları istemez:

- Şifreler
- PIN kodları
- Banka hesabı veya kart numaraları
- Sosyal güvenlik numaraları

✗ "Hesabınızı doğrulamak için lütfen giriş bilgilerinizi gönderin."

✓ "E-posta yoluyla şifrenizi asla sormayız."

6. Logolara ve Tasarıma Bakın

- Logolar bulanık, uzamış veya renkleri soluk mu?
- Düzen garip veya tutarsız mı?

Gerçek şirketler temiz, profesyonel ve tutarlı tasarımlar kullanır.

7. Gerçek olamayacak kadar iyi mi? Muhtemelen öyledir.

"Yeni bir iPhone kazandınız!"

"1.000 dolarlık hediye kartı kazanmaya hak kazandınız!"

Gerçek ödüller için önceden ödeme veya hassas bilgi istenmez.

✓ Gerçek mi, ✗ Sahte mi?

Kendinize sorun:

- **Kaynağa güveniyor muyum?**
- **Aceleye getiriliyor veya korkutularak harekete geçiriliyor muyum?**
- **Herhangi bir şey tuhaf veya olağandışı geliyor mu?**

Şüphe duyduğunuzda, tıklamayın, yanıt vermeyin ve bildirin!

Ek 5 | Sosyal Mühendislik Dolandırıcılığı – Bilmeniz Gerekenler

Sosyal Mühendislik Nedir?

Sosyal mühendislik, dolandırıcıların manipülasyon, baskı ve duyguları kullanarak sizi kişisel bilgilerinizi, paranızı veya hesaplarınıza erişim bilgilerinizi vermeye ikna etmeleridir.

Sosyal Mühendisliğin Tehlikeleri

Dolandırıcılar, aşağıdaki gibi güvenilir kaynaklardan geliyormuş gibi davranabilirler:

- Bankalar (örneğin, "Hesabınız kilitlendi!")
- Kurye hizmetleri (ör. "Bir paketinizi kaçırdınız. Hemen ödeyin!")
- Devlet kurumları (ör. "Ödenmemiş vergileriniz var.")
- Polis veya Adalet Bakanlığı (örneğin, "Hakkınızda soruşturma açılmıştır.")
- Teknik destek (örneğin, "Bilgisayarınızda bir virüs tespit ettik.")
- Aile veya arkadaşlar (örneğin, "Başım belada, lütfen para gönderin!")

Genellikle aciliyet veya korku hissi yaratarak düşünmeden hızlıca hareket etmenizi sağlarlar.

Dikkat Edilmesi Gereken Uyarı İşaretleri

- **Hemen** harekete geçmeniz gerektiği, aksi takdirde sonuçlarına katlanmanız gerektiği söylenir
- **Kişisel bilgileriniz**, şifreleriniz veya banka bilgileriniz isteniyor
- **Hediye kartları**, **kripto para veya banka havalesi ile ödeme** yapmanız istenir
- Mesajlarda **garip gramer veya imla hataları** vardır
- Tanımadığınız biri aniden sizinle iletişime geçiyor

Önleyici Tedbirler

Her zaman aşağıdakileri yapın:

1. Sakin olun. Bir dakika nefes alın ve acele etmeyin.
2. Telefon, e-posta veya kısa mesaj yoluyla asla kişisel bilgilerinizi vermeyin.
3. Şüpheli hissediyorsanız telefonu kapatın veya mesajı silin.
4. Talebi kendiniz doğrulayın:

Birisi banka, teslimat şirketi, devlet dairesi veya teknik destekten aradığını iddia ederse, her zaman doğrudan ilgili kurumu arayın.
Mesajda veya e-postada verilen numarayı değil, resmi web sitesini veya telefon numarasını kullanın.

Örnek:

- **Banka kartınızda veya resmi web sitesinde bulunan numarayı kullanarak bankanızı arayın.**
- **Vergiyle ilgili mesajlardan emin değilseniz resmi devlet sitesini ziyaret edin**
- **Bir paketin gerçek olup olmadığını kontrol etmek için kurye şirketinin resmi destek birimine başvurun**

Unutmayın

- **Gerçek şirketler sizi tehdit etmez veya baskı yapmaz**
- **Gerçek kurumlar sizden asla şifre veya PIN numarası istemez**
- **Gerçek mesajlar profesyonel ve saygılıdır.**
- **Dolandırıcılık korku, kafa karışıklığı ve hızdan yararlanır**

Bir şey "tuhaf" geliyorsa, durun ve güvendiğiniz birine danışın. Tuzağa düşmektense iki kez kontrol etmek her zaman daha iyidir.

Ek 6 | Senaryolar: Dolandırıcılığı Fark Etmek

Senaryo 1: Banka Acil Mesajı

Görünüşte bankanızdan bir e-posta alırsınız. Konu satırı şöyledir: 'ACİL: Hesap Erişimi Sorunu'. Mesajda, hesabınızda şüpheli bir hareketlilik olduğu ve kişisel ve banka bilgilerinizi derhal doğrulamanız gerektiği iddia edilmektedir. Bir bağlantı verilir ve 24 saat içinde yanıt vermezseniz hesabınızın kalıcı olarak askıya alınacağı konusunda uyarıda bulunulur.

Senaryo 2: Telefon Depolama Alanı Dolu Uyarısı

İnternette gezinirken veya bir uygulamayı kullanırken, "Uyarı! Telefonunuzun depolama alanı dolu. Cihazınızı temizlemek ve veri kaybını önlemek için buraya dokunun" şeklinde bir açılır mesaj belirir. Mesaj acil görünür, telefonunuzun sistem stilini taklit eder ve dokunduğunuzda, cihazınızı optimize etme sözü veren üçüncü taraf bir uygulamayı indirmenize yönlendirir.

Senaryo 3: Teknik Destek Çağrısı

Microsoft teknisyeni olduğunu iddia eden birinden bir arama alırsınız. Bilgisayarınızın tehlikeli bir virüs bulaştığını ve hata mesajları gönderdiğini söylerler. Sorunu uzaktan gidermeyi teklif ederler ve bilgisayarınıza erişim sağlamak için yazılım indirme konusunda size rehberlik ederler. Bağlantı kurulduktan sonra, bilgisayarınızı "tararlar" ve virüsü kaldırmak için ödeme talep ederler, genellikle kredi kartı veya çevrimiçi bankacılık erişiminizi isterler.

Senaryo 4: Fatura Ödeme Dolandırıcılığı

Elektrik sağlayıcınızdan gelmiş gibi görünen bir e-posta veya kısa mesaj alırsınız. Mesajda, son ödemenizin başarısız olduğu ve 12 saat içinde ödenmemiş bakiyeyi ödemediğiniz takdirde elektriğinizin kesileceği iddia edilir. Mesajda, gerçek kamu hizmeti web sitesine çok benzeyen ancak kredi kartı ve kişisel bilgilerinizi isteyen bir ödeme sayfasına bağlantı bulunur.

Senaryo 5: Banka İşlemi Bildirimi

Bankanızdan "İşlem Onayı – MERKUR'da 74,60 €" konulu bir e-posta alırsınız. Mesaj, bugün 13:45'te yapılan bir işlemi onaylar. Bu ücreti tanımazsanız, bankanın web sitesinde listelenen resmi numaradan bankanın dolandırıcılık departmanını aramanız istenir. E-posta tıklanabilir bağlantılar içermez ve sakin ve profesyonel bir üslup kullanır.

Senaryo 6: Google Depolama Uyarısı

Google'dan şu e-postayı alırsınız: "Google Hesabınızın depolama alanı %98 dolu. 15 GB depolama alanınızın 14,8 GB'ını kullanıyorsunuz. E-postaları almaya ve Google Drive'ı kullanmaya devam etmek için lütfen depolama alanınızı yönetin veya yükseltin." Mesajda iki düğme bulunur: biri depolama alanınızı yönetmek, diğeri yükseltmek içindir ve her ikisi de resmi Google web sitelerine yönlendirir.

Ek 7 | Yaygın Çevrimiçi Dolandırıcılık Türleri ve Kendinizi Koruma Yöntemleri

1. Smishing (SMS Kimlik Avı)
Bankanızdan, teslimat hizmetinden veya bir devlet kurumundan gelmiş gibi görünen bir kısa mesaj alırsınız. Mesajda, hesabınızda veya paketinize ilişkin bir sorun olduğu iddia edilebilir ve bir bağlantı içerebilir.

Smishing: Kısa mesaj yoluyla yapılan kimlik avı, genellikle sizi bir bağlantıya tıklamaya veya kişisel bilgilerinizi vermeye yönlendiren acil mesajlar içerir.

Kırmızı Bayraklar:
- Acil dil kullanımı ('hesabınız kapatılacaktır')
- Şüpheli bağlantılar
- Kişisel veya banka bilgilerinin istenmesi

Ne yapmalı:
- Bilinmeyen numaralardan gelen bağlantılara asla tıklamayın.
- Resmi telefon numarasını veya web sitesini kullanarak doğrudan şirketle iletişime geçin.
- Göndereni engelleyin ve bildirin.

2. Vishing (Sesli Kimlik Avı)
Bankanızdan, polisten veya teknik destekten arıyormuş gibi davranan birinden telefon alırsınız. Kişisel bilgilerinizi isterler veya şüpheli bir faaliyet olduğunu iddia ederler.

Vishing: Dolandırıcıların, bilgi çalmak için telefonda meşru kuruluşları taklit ettikleri sesli kimlik avı.

Varyasyon: AI kullanılarak sahte ses
Dolandırıcılar artık AI kullanarak sevdiklerinizin sesini taklit edebilir. Torununuz veya çocuğunuz gibi davranarak sizi arayıp acil yardım veya para isteyebilirler.

Kırmızı bayraklar:
- Arayan kişi sizi hızlı hareket etmeye zorlar
- Duygusal manipülasyon ("Başım belada!")
- Para veya bilgi ister

Ne yapmalı:
- Telefonu kapatın ve bilinen bir numaradan doğrudan geri arayın.
- Hikayeyi doğrulamak için başka bir aile üyesiyle iletişime geçin.
- Asla telefonla kişisel veya banka bilgilerinizi vermeyin.

3. Kimlik Avı (E-posta Dolandırıcılığı)
Resmi görünümlü bir e-posta alırsınız (bankanızdan, PayPal'dan, vergi dairesinden vb.) ve bu e-postada bilgilerinizi onaylamanız, şifrenizi sıfırlamanız veya bir bağlantıya tıklamanız istenir.

Kimlik Avı: Sizi gizli bilgilerinizi (şifreler veya banka bilgileri gibi) ifşa etmeye yönlendiren sahte e-postalar veya kısa mesajlar.

Kırmızı bayraklar:
- E-postada gramer hataları var
- Korku unsuru kullanılır ('yetkisiz giriş tespit edildi')
- Kişisel bilgi talep ediyor

Ne yapmalı:
- Şüpheli bağlantılara tıklamayın.
- Gönderenin e-posta adresini dikkatlice kontrol edin.
- Şirketin resmi web sitesi üzerinden iletişime geçin.

4. Finansal Dolandırıcılık

Dolandırıcılar yatırım danışmanı, sahte hayır kurumu veya hatta romantik ilgi gibi davranırlar. Güven oluşturduktan sonra para, bağış veya yardım isterler.

Finansal dolandırıcılık: Dolandırıcılar, genellikle ödül vaat ederek veya sonuçlarla tehdit ederek, sahte bahanelerle para isterler.

Kırmızı bayraklar:
- Gerçek olamayacak kadar iyi yatırım getirileri
- Duygusal manipülasyon
- Doğrulanamayan hayır kurumları veya amaçlar

Ne yapmalı
- Hiç tanışmadığınız kişilere asla para göndermeyin.
- Her zaman şirketi veya kişiyi araştırın.
- Finansal kararlar vermeden önce güvendiğiniz bir aile üyesine veya danışmana danışın.

5. Sahte Kimlikler ve Kimlik Hırsızlığı

Dolandırıcılar, devlet memuru, banka çalışanı veya hatta aile üyesi gibi olmadıkları bir kişi gibi davranabilirler. Sahte belgeler, e-postalar veya yapay zeka tarafından üretilen sesler kullanarak insanları hassas bilgilerini vermeye veya para göndermeye ikna ederler.

Sahte kimlikler: Dolandırıcılar, güven oluşturmak ve kurbanları para veya kişisel bilgilerini vermeye ikna etmek için sahte çevrimiçi profiller oluşturur.

Kırmızı bayraklar:
- Beklenmedik kişisel veri veya para talepleri
- Aciliyet hissi veya duygusal baskı
- Resmi olmayan veya şüpheli kanallar aracılığıyla kurulan iletişim

Ne yapmalı:
- Her zaman resmi iletişim bilgilerini kullanarak gerçek kişi veya kurumu arayarak kimliğini doğrulayın.
- Telefonu kapatıp önce kontrol etmekten çekinmeyin.
- Şüphe duyduğunuzda, güvendiğiniz birinden durumu değerlendirmenize yardım etmesini isteyin.

6. Kötü amaçlı yazılım veya malware

Bilgisayara zarar vermek veya kişisel bilgileri çalmak için tasarlanmış herhangi bir yazılımdır. Dolandırıcılar genellikle sahte e-postalar, bağlantılar veya açılır reklamlar yoluyla kullanıcıları bu yazılımları indirmeye ikna eder. Kötü amaçlı yazılımlar, bir kez yüklendikten sonra şifreleri çalabilir, dosyaları kilitleyebilir ve hatta cihazınızın kontrolünü ele geçirebilir. Bilinmeyen bağlantılara veya ek dosyalara karşı her zaman dikkatli olun ve bilgisayarınızda sizi korumak için güncel bir antivirüs yazılımı bulunduğundan emin olun.

Ek 8 | Katılımcı El Broşürü – Kötü Amaçlı Yazılımları Tespit Etme

Amaç

Bu gerçekçi senaryoları okuyup analiz ederek yaygın kötü amaçlı yazılım türlerini (virüsler, truva atları, casus yazılımlar, fidye yazılımları, reklam yazılımları) tanıyın.
Her dolandırıcılık için bunun ne tür bir dolandırıcılık olduğunu (truva atı, virüs, reklam yazılımı, fidye yazılımı, casus yazılım) yazın ve soruyu yanıtlayın.

Senaryo 1

"Güvenilir bir arkadaşınızdan 'Önemli Belge' başlıklı bir e-posta eki alırsınız. Eki açtığınızda bilgisayarınız yavaşlamaya başlar ve garip pop-up'lar görünmeye başlar."

Soru: Sizce bu ne tür bir kötü amaçlı yazılımdır? Kendinizi nasıl korursunuz?

Senaryo 2

"İnternette gezinirken 'Cihazınız güncel değil! Güncellemeyi indirmek için buraya tıklayın' şeklinde bir pop-up penceresi açılır. Bağlantıya tıklarsınız ve farkında olmadan güncelleme gibi görünen kötü amaçlı bir yazılım indirirsiniz."

Soru: Buradaki tehlike nedir? Bunun yerine ne yapmalısınız?

Senaryo 3

"Tanıdık olmayan bir web sitesinden ücretsiz bir fotoğraf düzenleme uygulaması indiriyorsunuz. Bir süre sonra, tarayıcınızda reklamlar göründüğünü fark ediyorsunuz ve istenmeyen pazarlama e-postaları almaya başlıyorsunuz."

Soru: Sizce ne olmuştur? Bundan sonra ne yapmalısınız?

Senaryo 4

"Netflix aboneliğinizin süresi dolmak üzere, ödemeyi onaylamak için buraya tıklayın" yazan bir e-postadaki bağlantıya tıkladıktan sonra, dosyalarınızı kilidini açmak için fidye ödemenizi isteyen bir mesaj belirir.

Soru: Bunun bir dolandırıcılık olduğunu nasıl anlayabilirsiniz? Böyle bir durumla karşılaşırsanız ne yapmalısınız?

Senaryo 5

"Netflix aboneliğinizin süresi dolmak üzere, ödemeyi onaylamak için buraya tıklayın" yazan bir e-postadaki bağlantıya tıkladıktan sonra, dosyalarınızı kilidini açmak için fidye ödemenizi isteyen bir mesaj belirir.

Soru: Bu tehlikeli bir yazılım türü mü? Bundan kurtulmanın çözümü nedir?

Ek 9 | Kişisel Verilerin Korunması

1. Kişisel Veriler Nedir?

Kişisel veri, sizi doğrudan veya dolaylı olarak tanımlamak için kullanılabilecek her türlü bilgidir. Buna şunlar dahildir:

- **Temel veriler:** Ad, soyad, doğum tarihi, adres
- **İletişim bilgileri:** E-posta adresi, telefon numarası
- **Kimlik numaraları:** Kimlik numarası, vergi numarası, pasaport numarası
- **Finansal veriler:** Banka hesap numaraları, kredi kartı numaraları
- **Giriş bilgileri:** Kullanıcı adları, şifreler
- **Sağlık verileri:** Tıbbi kayıtlar, reçeteler
- **Biyometrik veriler:** Parmak izleri, yüz tanıma, ses
- **Konum verileri:** GPS izleme, IP adresi
- **Kişisel tercihler:** Arama geçmişi, sosyal medya etkinliği

2. Hangi veriler yanlış ellerde zararlı olabilir (ve neden)?

Dolandırıcılar ve siber suçlular, aşağıdakiler için kullanılabilecek belirli verileri hedef alır:

- **Kimliğinizi çalmak**
- **Banka hesaplarınıza erişmek**
- **Adınıza dolandırıcılık yapmak**
- **Sizi duygusal veya finansal olarak manipüle etmek**

Dolandırıcılar için en değerli veriler:

- **Kişisel kimlik (pasaport vb.) -** Kimlik hırsızlığı veya sahte hesap açmak için kullanılır.
- **Giriş bilgileri -** E-postalara, sosyal medyaya, çevrimiçi bankacılığa erişim sağlar.
- **Banka ve kredi kartı bilgileri -** Yetkisiz satın alımlar veya para transferleri için kullanılır.
- **Telefon numaraları ve e-postalar -** Kimlik avı, smishing, spam ve kimlik sahtekarlığı için kullanılır.
- **Sosyal medya içeriği -** Sahte profiller oluşturmak veya sizi manipüle etmek için kullanılır.

3. Kişisel Bilgilerimizi Çevrimiçi Olarak Nerede Paylaşabiliriz?

Kişisel verilerinizi nerede ve ne zaman güvenle paylaşabileceğinizi bilmek önemlidir. Bazı platformlar güvenilirdir, bazıları ise daha yüksek riskler taşır.

Kişisel verilerinizi paylaşmanın genellikle güvenli olduğu yerler (dikkatli olunmalıdır):

- Doğrulanmış çevrimiçi mağazalar (ör. Amazon, Zalando, Mimovrste): Satın alımlar için, yalnızca web sitesinde HTTPS şifreleme ve güvenli ödeme yöntemleri varsa.
- Resmi devlet web siteleri (ör. IRS, Sosyal Güvenlik portalları, e-Devlet portalları): Belge, vergi ve başvuru gönderimi için.
- Saygın hizmet sağlayıcılar (ör. bankanız, sağlık hizmetleri sağlayıcınız): Yalnızca resmi web siteleri veya uygulamaları aracılığıyla.
- Güvenilir e-posta sağlayıcıları ve bulut hizmetleri (ör. Gmail, Outlook, Dropbox): Hesap oluştururken, verileri yedeklerken.

Herhangi bir bilgi göndermeden önce sitenin resmi, HTTPS şifrelemesi olan ve tanınmış bir site olduğundan emin olun.

Son derece dikkatli olmanız veya kişisel bilgilerinizi paylaşmaktan kaçınmanız gereken yerler:

- Doğrulanmamış çevrimiçi mağazalar veya reklamlar (genellikle pop-up'lar veya sosyal medya aracılığıyla bulunur)
- Bilinmeyen anketler, çevrimiçi testler veya hediye çekilişleri
- Güvenli olmayan halka açık Wi-Fi ağları
- İstenmeyen e-postalarda veya kısa mesajlarda yer alan bağlantılar
- Sosyal medya platformları, özellikle yorumlar veya doğrudan mesajlar

İpucu: Platform tanıdık gelse bile, web adresini her zaman iki kez kontrol edin ve kesinlikle gerekli ve güvenli olmadıkça kimlik numaraları veya finansal bilgiler gibi hassas verileri paylaşmaktan kaçının.

4. Hangi bilgileri paylaşabiliriz ve çevrimiçi ortamda asla paylaşmamamız gereken bilgiler nelerdir?

- **Paylaşılabilir (dikkatli olunarak):** Ad, şehir ve genel konum, genel ilgi alanları veya hobiler, mesleki bilgiler (ör. iş unvanı), genel e-posta adresi (iş için), profil fotoğrafları
- **Çevrimiçi olarak ASLA paylaşılmaması gerekenler:** Şifreler ve PIN'ler, tam adres (doğrulanmış devlet kurumları ve web mağazaları hariç), kimlik numaraları, vergi numaraları, banka veya kredi kartı bilgileri, tıbbi kayıtlar veya sağlık bilgileri, hassas aile bilgileri veya seyahat planları

Temel kural: Bilgiler paranız, kimliğiniz veya özel hayatınıza erişmek için kullanılabilecekse, kim sorarsa sorsun, çevrimiçi olarak paylaşmayın.

5. Verilerinizi yedeklemek, önemli dosya, belge, fotoğraf ve ayarların bir kopyasını güvenli ve ayrı bir yerde saklamak anlamına gelir. Bu, harici bir sabit sürücü, USB bellek veya güvenli bir bulut depolama hizmeti olabilir.

Yedekleme Neden Önemlidir?

Verileriniz aşağıdaki nedenlerle aniden kaybolabilir veya tehlikeye girebilir:

- Cihaz arızası (ör. bilgisayar çökmesi, telefon bozulması)
- Telefonunuzun veya bilgisayarınızın çalınması veya kaybolması
- Dosyalarınızı kilitleyen veya yok eden fidye yazılımı veya kötü amaçlı yazılım saldırıları
- Yanlışlıkla silme veya formatlama
- Doğal afetler (yangın, sel vb.)

Yedekleme sizi kötü amaçlı yazılım saldırılarından nasıl korur?

Fidye yazılımı gibi kötü amaçlı yazılımlar dosyalarınızı şifreleyebilir ve kilidini açmak için ödeme talep edebilir. Güvenli bir yedeğiniz varsa, fidye ödemenize gerek kalmaz; cihazınızı sıfırlayabilir ve dosyalarınızı yedekten güvenli bir şekilde geri yükleyebilirsiniz.

Benzer şekilde, virüsler ve truva atları dosyalarınıza veya işletim sisteminize zarar verebilir. Dosyalarınız yedeklenmişse, sisteminizi yeniden yükleyebilir ve önemli verilerinizi hiçbir şey kaybetmeden geri yükleyebilirsiniz.

Güvenli Yedekleme için En İyi Uygulamalar:

- Hem yerel hem de bulut yedeklemeyi kullanın: Bir kopyasını harici bir sabit sürücüde, diğerini güvenilir bir bulut hizmetinde (Google Drive, Dropbox, iCloud, OneDrive gibi) saklayın.
- Hassas yedeklemeleri şifreleyin: Hassas veriler için parola koruması veya şifreleme kullanın.
- Düzenli olarak yedekleme yapın: Dosyalarınızı ne sıklıkta güncellediğinize bağlı olarak haftalık veya aylık bir program belirleyin.
- Kullanmadığınızda harici sürücülerin bağlantısını kesin: Fidye yazılımı saldırısı durumunda, bağlı sürücüler de hedef alınabilir.
- Yedeklemelerinizi test edin: Ara sıra dosyaları geri yüklemeyi deneyerek yedekleme sisteminizin çalıştığından emin olun.

6. Verilerinizi Güvende Tutmak İçin İpuçları

- Güçlü, benzersiz şifreler kullanın (ve bunları düzenli olarak değiştirin)
- İki faktörlü kimlik doğrulamayı (2FA) etkinleştirin
- Yazılım ve antivirüs programlarını güncel tutun
- Şüpheli bağlantılara veya ekleri tıklamaktan kaçının
- Doğrulanmadıkça kişisel bilgilerinizi telefon veya e-posta yoluyla paylaşmayın
- Verilerinizi düzenli olarak yedekleyin (bulut veya harici sabit sürücü)
- Halka açık Wi-Fi ağlarında dikkatli olun – hassas hesaplara giriş yapmaktan kaçının
- Sosyal medyadaki gizlilik ayarlarınızı kontrol edin
- Paylaşmadan önce düşünün – bir kez çevrimiçi olduğunda, kopyalanabilir veya kötüye kullanılabilir

Ek 10 | Dosyalarınızı Yedekleme

1. Dosyaları Harici Sürücüye Yedekleme

Adım 1: Harici Sürücünüzü Bağlayın

- Harici sabit sürücünüzü veya USB belleğinizi uygun kablo veya bağlantı noktasını kullanarak bilgisayarınıza takın.
- Cihazın bilgisayarınız tarafından tanındığından emin olun (Windows için "Bu Bilgisayar" veya "Bilgisayarım" klasörünü, Mac için Finder'ı kontrol edin).

Adım 2: Yedeklemek İstediğiniz Dosyaları Seçin

- Yedeklemek istediğiniz dosyaların bulunduğu klasörü açın.
- Belirli dosyaları veya tüm klasörleri seçebilirsiniz. Birden fazla dosya veya klasör seçmek için, öğeleri tıklarken Ctrl (Windows) veya Cmd (Mac) tuşunu basılı tutun.

Adım 3: Dosyaları Kopyalayın

- Seçilen dosyalara sağ tıklayın ve Kopyala'yı seçin (veya Windows için **Ctrl+C**, Mac için **Cmd+C** klavye kısayolunu kullanın).
- "Bu Bilgisayar" (Windows) veya Finder (Mac) içinde harici sürücüye gidin.
- Harici sürücüye sağ tıklayın ve Yapıştır'ı seçin (veya Windows için **Ctrl+V**, Mac için **Cmd+V** kullanın) dosyaları kopyalamak için.

Adım 4: Harici Sürücüyü Güvenli Bir Şekilde Çıkarın

- Dosyalar kopyalandıktan sonra, dosyalara zarar vermemek için harici sürücünüzü güvenli bir şekilde çıkarın.
- Windows'ta, "Bu Bilgisayar"da harici sürücüyü sağ tıklayın ve Çıkar'ı seçin.
- Mac'te, harici sürücü simgesini Çöp Kutusu'na sürükleyin veya Finder'da sürücünün yanındaki çıkarma düğmesine tıklayın.
- Apple cihazınızda (Mac veya iPhone), **Ayarlar'a** gidin ve Apple Kimliğinizle oturum açın.
- Mac'te, **Sistem Tercihleri** > **Apple Kimliği** > **iCloud'dan** iCloud'a erişebilirsiniz.
- iPhone'da **Ayarlar** > [Adınız] > **iCloud**'a gidin.

2. Dosyaları Bulut Hizmetine Yedekleme

Google Drive kullanma

Adım 1: Google Hesabınıza Giriş Yapın

- Bir web tarayıcısı açın ve Google Drive'a gidin.
- Google hesabı kimlik bilgilerinizle oturum açın (veya hesabınız yoksa yeni bir hesap oluşturun).

Adım 2: Dosyaları Google Drive'a yükleyin

- Sol kenar çubuğundaki Yeni düğmesine tıklayın.
- Yedeklemek istediğiniz öğeye göre Dosya yükle veya Klasör yükle seçeneğini belirleyin.
- Yüklemek istediğiniz dosyaları veya klasörleri bulun ve Aç'ı tıklayın.

Adım 3: Dosyalarınızı Düzenleyin (İsteğe Bağlı)

- Yedeklemenizi düzenli tutmak için Google Drive'da klasörler oluşturabilirsiniz. Yeni > Klasör'e tıklayın, klasöre bir ad verin ve dosyaları sürükleyip bırakarak klasöre taşıyın.

Adım 4: Yüklemeyi Kontrol Edin

- Dosyalarınızın yükleme işleminin tamamlandığından emin olun. Yükleme işlemi devam ederken Google Drive bir durum çubuğu gösterir.

Dropbox'ı kullanma

Adım 1: Dropbox Hesabınıza Giriş Yapın

- Bir tarayıcı açın ve Dropbox'a gidin.
- Henüz bir hesabınız yoksa, oturum açın veya yeni bir Dropbox hesabı oluşturun.

Adım 2: Dosyaları Dropbox'a yükleyin

- Giriş yaptıktan sonra Dosyaları yükle düğmesine tıklayın.
- Bilgisayarınızdan yedeklemek istediğiniz dosyaları veya klasörleri seçin ve Aç'ı tıklayın.
- Dosyaları doğrudan Dropbox web sitesine sürükleyip bırakabilirsiniz.
- iPhone'da, Ayarlar > [Adınız] > iCloud'a giderek iCloud depolama alanınızı kontrol edin.

Yedekleme için Önemli İpuçları:

- Düzenli olarak yedekleme yapın: Önemli dosyalarınızı kaybetmemek için verilerinizi en az haftada bir kez yedeklemeyi alışkanlık haline getirin.
- Hem yerel hem de bulut yedeklemelerini kullanın: Ekstra güvenlik için verilerinizin bir kopyasını hem harici bir sabit sürücüde hem de bulutta saklayın.
- Hassas dosyaları şifreleyin: Hassas verileri (ör. finansal kayıtlar, kişisel belgeler) depolarken, buluta yüklemeden veya harici bir sürücüye kaydetmeden önce şifrelemeyi düşünün.
- Yedeklemenizi test edin: Her şeyin düzgün çalıştığından emin olmak için ara sıra bazı dosyaları geri yükleyerek yedeklemenizi test edin.

Dosyalarınızı yedeklemek, cihaz arızası, siber saldırı veya kazara silme durumunda verilerinizin güvenli ve kurtarılabilir olmasını sağlamak için çok önemlidir. Hem harici sürücüler hem de bulut hizmetleri, verilerinizi güvenli bir şekilde depolamak için güvenilir yollar sunar. Herhangi bir sorunuz varsa, yedekleme sisteminizi kurmak için yardım veya destek isteyebilirsiniz!

Ek 11| Çevrimiçi Güvenlik Kontrol Listesi

1. Kişisel Bilgilerin Korunması

- **Çevrimiçi paylaştığınız kişisel bilgileri gözden geçirin** – Sosyal medya ve diğer platformlarda paylaştıklarınız konusunda her zaman dikkatli olun. Yalnızca gerekli bilgileri paylaşın.
- **Hassas bilgileri gizli tutun** – Şifreleri, PIN kodlarını, banka hesap numaralarını veya kimlik numaralarını asla çevrimiçi olarak paylaşmayın.
- Hesaplarınız için **güçlü, benzersiz şifreler kullanın** ve bunları düzenli olarak değiştirin. Mümkünse, özellikle bankacılık, e-posta ve sosyal medya hesaplarınızda **iki faktörlü kimlik doğrulamayı etkinleştirin**.

2. Dolandırıcılıkları Tanımak

- **Yaygın çevrimiçi dolandırıcılık yöntemlerinin farkında olun** – Kimlik avı, SMS dolandırıcılığı, sesli dolandırıcılık ve finansal dolandırıcılık gibi dolandırıcılık yöntemlerini tanımayı öğrenin.

- **Dolandırıcılık için uyarı işaretleri**:

  - Acil dil kullanımı (ör. "Acilen işlem yapmanız gerekiyor!")
  - Kişisel, banka veya giriş bilgilerinin istenmesi
  - Şüpheli bağlantılar veya telefon numaraları
  - Duygusal manipülasyon veya tehditler (ör. "Hesabınız kapatılacak")

- **Meşru ve sahte talepler arasındaki farkı bilin** – Yanıt vermeden önce aldığınız tüm telefon görüşmelerinin, e-postaların veya mesajların gerçekliğini doğrulayın.

- **Şüphe durumunda,** talebi doğrulamak için **her zaman** kuruluşun resmi iletişim bilgilerini kullanarak **doğrudan kuruluşla iletişime geçin**.

3. Dolandırıcılık ve Kötü Amaçlı İçerikle Başa Çıkma

- **Şüpheli bağlantılara tıklamayın veya** bilinmeyen gönderenlerden gelen **ekleri açmayın**. Bunlar kimlik avı girişimleri olabilir veya kötü amaçlı yazılım içerebilir.

- **Şüpheli e-postaları, mesajları veya telefon görüşmelerini** ilgili makamlara (örneğin, Slovenya'da SI-CERT) **bildirin**.

- **Herhangi bir finansal talebi** (para transferleri, kredi kartı bilgileri) **her zaman** doğrudan ilgili kişi veya kuruluşu arayarak **iki kez kontrol edin**.

- **İstenmeyen telefon aramalarına karşı dikkatli olun**, özellikle arayan kişi sizden para veya kişisel bilgiler için baskı yapıyorsa. Telefonu kapatın ve bilinen bir numarayı arayarak geri arayın.

4. Cihazlarınızı Kötü Amaçlı Yazılımlardan Koruma

- Cihazınızı virüslerden, kötü amaçlı yazılımlardan ve casus yazılımlardan korumak için **antivirüs yazılımı yükleyin ve güncelleyin**.
- Doğrulanmamış kaynaklardan **uygulama veya yazılım indirmekten kaçının**. Resmi uygulama mağazalarını (Google Play Store, Apple App Store) kullanın.
- Olası bir saldırıdan kaynaklanan veri kaybını önlemek için **verilerinizi düzenli olarak** harici bir sürücüye veya bulut hizmetine **yedekleyin**.
- **Yazılımlarınızı ve cihazlarınızı** en son güvenlik yamalarıyla **güncel tutun**.
- **Halka açık Wi-Fi kullanırken dikkatli olun** – Halka açık ağlara bağlıyken hassas hesaplara erişmekten kaçının.

5. Güvenli Çevrimiçi Alışveriş

- **Yalnızca doğrulanmış, güvenilir web sitelerinden alışveriş yapın** – Tarayıcı çubuğunda asma kilit simgesini ve URL'de "https" ifadesini arayın.
- Çevrimiçi alışveriş yaparken, dolandırıcılık koruması sağlayan kredi kartı gibi **güvenli ödeme yöntemlerini kullanın**.
- Yeni bir çevrimiçi mağazadan alışveriş yapmadan önce **yorumları ve puanları kontrol edin**.

6. Verilerinizi Yedekleyin

- **Önemli dosyaları** (belgeler, fotoğraflar, kişiler) düzenli olarak harici bir sürücüye veya bulut hizmetine **yedekleyin**. Bu, verilerinizi cihaz arızalarından veya fidye yazılım saldırılarından koruyacaktır.
- Ek güvenlik için **güvenilir bir bulut yedekleme hizmeti** (Google Drive, Dropbox, OneDrive) **kullanın**.
- Verilerinizin her zaman güncel ve güvenli olmasını sağlamak için **bir yedekleme programı oluşturun**.

7. Sosyal Medya Güvenliği

- Sosyal medya platformlarında (Facebook, Instagram vb.) **paylaştıklarınıza dikkat edin**. Tam adresiniz, telefon numaranız ve finansal bilgileri gibi hassas bilgileri paylaşmaktan kaçının.
- **Gizlilik ayarlarınızı,** gönderilerinizi ve kişisel bilgilerinizi kimlerin görebileceğini kontrol etmek için **ayarlayın**.
- Yabancılardan gelen **arkadaşlık isteklerini** veya mesajları **kabul etmeyin**. Kişiyi tanımıyorsanız, isteği görmezden gelmek daha güvenlidir.

8. Sosyal Mühendislik Saldırısı ile Nasıl Başa Çıkılır

- Şüpheli bir mesaj veya telefon aldığınızda **sakin olun ve aceleci davranmayın**.
- Konuştuğunuz kişinin **kimliğinden emin olmadıkça, telefon, e-posta** veya **kısa mesaj yoluyla asla kişisel bilgi vermeyin**.
- Resmi iletişim numaralarını (örneğin, bankanızın resmi numarası veya şirketin web sitesi) kullanarak geri arayarak **arayanın kimliğini doğrulayın**.
- **Baskıya girmeyin** – Dolandırıcılar genellikle sizi hızlı hareket etmeye zorlamak için aciliyet hissi yaratır. Acele etmeyin ve talebi doğrulayın.

9. Acil Durum Müdahalesi

- **Bir dolandırıcılık şüphesi varsa veya kişisel bilgileriniz tehlikeye girmişse**, derhal bankanızla veya kredi kartı şirketinizle iletişime geçerek hesaplarınızı dondurun.
- **Dolandırıcılık vakalarını** Slovenya'daki SI-CERT gibi **yetkililere** veya gerekirse yerel polise **bildirin**.
- Bir durumdan emin değilseniz, **güvendiğiniz bir arkadaşınızdan veya aile** üyesinden **tavsiye alın**.

10. Bilgilenin

- En son dolandırıcılık olayları hakkında güncel bilgi edinin – SI-CERT veya diğer güvenlik platformları gibi güvenilir kaynakların haber bültenlerine veya uyarılarına abone olun.
- Çevrimiçi tehditler ve kendinizi nasıl koruyabileceğiniz konusunda düzenli olarak bilgi edinin.

Unutmayın
İnternet harika bir araç olabilir, ancak potansiyel riskler konusunda uyanık ve bilgili olmak önemlidir. Bu kontrol listesini takip ederek, savunmasızlığınızı önemli ölçüde azaltabilir ve kişisel bilgilerinizi ve cihazlarınızı güvende tutabilirsiniz. Şüphe duyduğunuzda, her zaman güvendiğiniz birinden yardım veya tavsiye isteyin. Güvenliğiniz ve huzurunuz en önemli önceliğimizdir!

Ek 12 | Katılımcılar için daha fazla okuma ve öğrenme önerileri

Siber güvenlik web siteleri: Siber güvenlikle ilgilenen Avrupa ve hükümet kuruluşları

1) **OLAF - AVRUPA DOLANDIRICILIKLA MÜCADELE OFİSİ**
   Web sitesi: https://anti-fraud.ec.europa.eu/olaf-and-you/report-fraud_en
   OLAF, AB kurumları ve fonları içindeki dolandırıcılık, yolsuzluk ve ciddi suistimalleri araştıran bir AB kurumudur.

2) **Avrupa Mağdur Desteği**
   Web sitesi: https://victim-support.eu/help-for-victims/info-on-specific-types-of-victims/fraud-victims/
   Victim Support Europe, tüm suç mağdurlarının haklarını savunan ve ulusal üye kuruluşlarından oluşan ağı aracılığıyla destek hizmetleri sunan bir Avrupa çatı kuruluşudur.

3) **EC3 – Europol Siber Suç Merkezi**
   Web sitesi: https://www.europol.europa.eu/crime-areas/cybercrime
   Europol, siber suçlar ve veri güvenliği hakkında bilgi sunar.

4) **CERT-EU (AB Kurumları için Bilgisayar Acil Durum Müdahale Ekibi)**
   Web sitesi: https://cert.europa.eu/
   Bu kuruluş, siber tehditleri izler ve Avrupa kurumlarına yönelik siber saldırılara müdahale eder.

3.5 Modül II – Ön/Son Test

1. Aşağıdakilerden hangisi güvenli internet davranışına bir örnektir?

A) Sosyal medyada kişisel adresinizi paylaşmak
B) Her hesap için güçlü ve benzersiz şifreler kullanmak
C) Tanımadığınız kişilerden gelen arkadaşlık isteklerini kabul etmek
D) İlginç görünen her bağlantıya tıklamak

2. Sosyal medyayı kullanırken yaygın bir risk nedir?

A) Yeni arkadaşlar edinmek
B) Bilgi bombardımanı
C) Kötüye kullanılabilecek kişisel bilgileri aşırı paylaşmak
D) Gizlilik ayarlarınızı düzenli olarak güncellemek

3. Çevrimiçi bilgi paylaşmadan önce kaynağı neden doğrulamalısınız?

A) Yanlış bilgilerin yayılmasını veya dolandırıcılığı önlemek için
B) Beğeni ve takipçi sayısını artırmak için
C) Bilgisayarınızın performansını artırmak için
D) Profil güvenlik düzeyinizi değiştirmek için

4. Aşağıdaki şifrelerden hangisi en güçlüdür?

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

5. Bir arkadaşınızın hacklenmiş hesabından şüpheli bir mesaj alırsanız ne yapmalısınız?

A) Ne olduğunu görmek için bağlantıya tıklayın
B) Hesabı bildirin veya engelleyin ve arkadaşınızı bilgilendirin
C) Daha fazla bilgi isteyerek cevap verin
D) Tamamen görmezden gelin

6. "Dijital ayak izi" ne anlama gelir?

A) Bilgisayarınızda depolanan toplam veri miktarı
B) Çevrimiçi etkinliklerinizin ve paylaştığınız bilgilerin kaydı
C) Hesaplarınız için kullandığınız şifre
D) Bilgisayarınızı koruyan yazılım

7. Tüm hesaplar için aynı şifreyi kullanmak neden risklidir?

A) Oturum açma işlemini çok yavaşlatabilir
B) Bir hesap hacklenirse, diğerleri de kolayca tehlikeye girebilir
C) Çok fazla zaman kazandırır
D) Şifre yöneticileri kullanmayı gerektirir

8. Sosyal medyada gizliliğinizi korumak için en iyi yol nedir?

A) Profilinizi "herkese açık" olarak ayarlayın
B) Tüm kişisel bilgilerinizi paylaşın
C) Gizlilik ayarlarını düzenli olarak gözden geçirin ve ayarlayın
D) Her gönderide gerçek doğum tarihinizi ve adresinizi kullanın

9. Sahte veya dolandırıcı bir web sitesinin belirtisi nedir?

A) "https://" ile başlar
B) Yazım hataları ve gerçekçi olmayan teklifler içerir
C) Tarayıcıda kilit simgesi gösterir
D) İletişim bilgileri sağlar

10. Paylaşımlı veya halka açık bilgisayarlarda hesaplarınızdan neden çıkış yapmalısınız?

A) Bir sonraki kullanıcı için yer açmak için
B) Verilerinize yetkisiz erişimi önlemek için
C) Pil gücünden tasarruf etmek için
D) Şifrenizi otomatik olarak güncellemek için

Cevap Anahtarı Özeti

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

MODÜL III

Çevrimiçi Bankacılık ve Alışveriş Güvenliği

4. Modül III - Çevrimiçi Bankacılık ve Alışveriş Güvenliği

Bu modülün amacı, yaşlılara dijital finansal faaliyetleri yönetmek için gerekli bilgi ve pratik becerileri sağlayarak çevrimiçi bankacılık ve alışveriş platformlarını güvenle kullanmalarını sağlamaktır. Modül, katılımcıların çevrimiçi bankacılık ve e-ticaret hizmetlerinin nasıl işlediğini anlamalarını güçlendirirken, dolandırıcılık, sahtekarlık ve siber tehditlere karşı korunmak için güvenli ve sorumlu uygulamaları vurgular.

Modül, pratik rehberlik ve gerçek hayattan örnekler aracılığıyla dijital okuryazarlığın gelişimini destekler ve yaşlıları çevrimiçi ödeme yaparken, hesaplarını yönetirken ve kişisel bilgilerini paylaşırken güvenli alışkanlıklar edinmeye teşvik eder. Modülün sonunda, katılımcılar finansal bağımsızlıklarını korumak, dijital hizmetlerden yararlanmak ve güven, güvenlik ve özerklikle çevrimiçi bankacılık ve alışveriş yapmak için daha donanımlı hale gelirler.

Ayrıca modül, yaşlıların dijital finansal hizmetleri kullanırken yaşayabilecekleri yaygın korku ve belirsizlikleri ele alarak, çevrimiçi işlemlerle ilgili endişeleri azaltmayı amaçlamaktadır. Katılımcılar, güvenilir platformları tanımak, temel güvenlik kontrollerini uygulamak ve şüpheli faaliyetlere uygun şekilde yanıt vermek konusunda yönlendirilir. Uygulama ve net açıklamalarla güveni pekiştiren modül, yaşlıların dijital finansal kararlarını daha iyi kontrol edebilmelerine yardımcı olur ve çevrimiçi bankacılık ve alışverişe güvenli ve bilinçli bir şekilde uzun vadede devam etmelerini destekler.

4.1 Öğrenme Hedefleri

Bu modülün ana hedefi, yaşlılara çevrimiçi bankacılık ve e-ticaret platformlarını güvenli bir şekilde kullanmak için gerekli pratik bilgi ve becerileri kazandırmaktır. Modül, teknolojiyle ilgili korku ve endişeleri azaltırken dijital güveni artırmaya odaklanarak, katılımcıların finansal işlemleri güvenli ve bağımsız bir şekilde yönetmelerini sağlar. Katılımcılar, kişisel ve finansal bilgilerini nasıl koruyacaklarını, çevrimiçi riskleri nasıl tanıyacaklarını ve günlük dijital finansal faaliyetlerinde etkili güvenlik uygulamalarını nasıl uygulayacaklarını öğreneceklerdir.

- Güvenli gezinme, hesap yönetimi ve dijital işlemleri destekleyen çevrimiçi bankacılık ve e-ticaret temellerini anlamak.
- Çevrimiçi hesapların güvenliğini artırmak için güçlü şifreler oluşturma ve İki Faktörlü Kimlik Doğrulama (2FA) özelliğini etkinleştirme becerilerini geliştirin.
- HTTPS, asma kilit simgeleri, müşteri yorumları ve güvenilir ödeme yöntemleri gibi güvenlik göstergelerini tanıyarak güvenilir çevrimiçi alışveriş platformlarını ve satıcıları belirleyin.
- Sahte web siteleri, kimlik avı girişimleri ve aldatıcı teklifler dahil olmak üzere çevrimiçi dolandırıcılık ve finansal dolandırıcılıkları tanıyın ve bunlardan kaçının.
- Antivirüs yazılımı kullanarak, işlemleri izleyerek ve şüpheli etkinlikler için uyarılar ayarlayarak kişisel ve finansal verilerinizi koruyun.
- Halka açık ağları kullanırken, halka açık Wi-Fi'nin risklerini anlamak ve bağlantıları güvenli hale getirmek için VPN kullanmak dahil olmak üzere güvenli internet uygulamalarını uygulayın.
- Öğrendiğiniz becerileri gerçek hayattaki çevrimiçi bankacılık ve alışveriş durumlarına uygulayarak, dijital araçlara olan güveninizi artırın ve endişenizi azaltın, böylece dijital güven ve finansal bağımsızlık kazanın.

4.2 Yapı, İçerik ve Öğrenim Çıktıları

Bu modülü başarıyla tamamlayan öğrenciler şunları yapabileceklerdir:

- Çevrimiçi bankacılığın nasıl çalıştığını anlamak, çevrimiçi hesap yönetiminin avantajlarını öğrenmek ve popüler bankacılık platformlarına genel bir bakış elde etmek.
- E-ticaret web sitelerinde gezinmek, çevrimiçi alışverişin ve popüler platformların avantajlarını öğrenmek.
- Güçlü şifreler ve iki faktörlü kimlik doğrulama (2FA) ayarlama: güvenliği artırmak için güçlü şifreler oluşturma ve 2FA kullanma ipuçları.
- Bankacılık uygulamalarını ve web sitelerini güvenli bir şekilde kullanmak: yalnızca resmi uygulamaları/web sitelerini kullanmak, güvenli bağlantıları (https) kontrol etmek.
- Güvenilir web sitelerinde alışveriş yapmak: bir web sitesinin gerçekliğini doğrulamak ve yorumları ve puanlamaları anlamak.
- Güvenli ödeme seçeneklerini tanıyın: güvenli ödeme yöntemlerini (kredi kartları) belirleyin ve güvenli olmayan ödemelerden (banka havaleleri) kaçının.
- Cihazları güvenli hale getirin: antivirüs yazılımını kullanma ve yazılımı güncelleme.
- Finansal işlemler için halka açık Wi-Fi ağlarını güvenli bir şekilde kullanın: halka açık ağlarla ilişkili riskler ve güvenliği sağlamak için VPN kullanımı.

4.3 Gündem I Ayrıntılı Oturum Planı

MODÜL III
İnternet Bankacılığı ve Çevrimiçi Alışveriş Güvenliği

1. Oturum

Hoş geldiniz
Süre 5

Öğrenim Hedefleri

- Konuyu tanıtın ve sıcak bir ortam yaratın.

İçerik/ Yöntem

- Oturuma kısa bir giriş yapın, hedefleri özetleyin ve beklentileri belirleyin. Modülü ve önemini özetleyerek eğitimin zeminini hazırlayın.

Malzeme

- Oturum hedefleri için beyaz tahta veya flip chart.
- Marker kalemler.
- Oturumu özetleyen basılı gündem veya sunum slaytları.

2. Oturum

Buz kırıcı etkinlik: "İlk çevrimiçi bankacılık deneyimim"

Süre 10 dakika

Öğrenim Hedefleri

- Ortak deneyimler aracılığıyla bağlantı kurun ve konuyu tanıtın.

İçerik/Yöntem

- Eğitmen, katılımcılardan çevrimiçi bankacılıkla ilgili ilk deneyimleri hakkında, ne yaptıklarını ve nasıl hissettiklerini de dahil olmak üzere kısa bir hikaye paylaşmalarını ister. Katılımcılar deneyimlerini paylaşırken, eğitmen aktif olarak dinler ve önemli duyguları ve düşünceleri flipchart veya beyaz tahtaya yazar (örneğin, gerginlik, heyecan, kafa karışıklığı), grubun ortak deneyimlerini ve duygularını görsel olarak yakalar. Son olarak, eğitmen katılımcıların paylaştığı duyguları ve deneyimleri kısaca özetler.

Malzeme

- Anahtar kelimeleri yazmak için flipchart veya beyaz tahta (örneğin, gergin, heyecanlı), kalemler.

3. Oturum

Ders 1: Çevrimiçi Bankacılık ve Alışverişin Temellerini Anlamak

Süre 30

Öğrenim Hedefleri

- Katılımcıların çevrimiçi bankacılık ve alışverişin nasıl çalıştığını anlamalarına ve güvenli ile güvenli olmayan platformları ayırt etmelerine yardımcı olmak.

İçerik/ Yöntem

- Eğitmen, Monzo veya Revolut (bankacılık) ve Zalando veya Coolblue (alışveriş) gibi kullanıcı dostu örnekleri ele alarak güvenlik, gezinme ve kullanılabilirlik gibi temel özellikleri vurgular. Öğrenmeyi pekiştirmek için katılımcılar, gerçek bir web sitesini sahte bir web sitesi ile karşılaştırarak, bilgilerini kullanarak güvenilirlik ve dolandırıcılık belirtilerini tespit ederler.
- Eğitmen, ekran görüntüleri ve canlı gösterimler kullanarak çevrimiçi bankacılık ve alışverişin temellerini tanıtır. Eğitmen, katılımcılara basit bir bankacılık platformunu göstererek çevrimiçi bankacılığın nasıl çalıştığını açıklar ve onlara bakiyelerini kontrol etmeyi, para transferi yapmayı ve diğer temel özellikleri kullanmayı gösterir. Ardından eğitmen, aynı şeyi bir alışveriş sitesi için de yapar ve katılımcılara platformda gezinmeyi, ürünleri seçmeyi ve satın alma sürecini tamamlamayı gösterir. Eğitmen, biri güvenli diğeri sahte olmak üzere iki web sitesi gösterir ve katılımcılardan hangisinin güvenli olduğunu belirlemelerini ve nedenini açıklamalarını ister, böylece web sitesi güvenliği konusundaki bilgilerini uygulamaya teşvik eder. Sonunda, eğitmen oturumdan çıkarılacak önemli dersleri tartışır: güvenli bağlantıları (HTTPS) kontrol etmenin önemi, meşru platformları tanıma ve dolandırıcılıktan kaçınma yolları.

Materyal

- ❖ PowerPoint sunumu, görsel el broşürleri,
- ❖ Dizüstü bilgisayar, projektör.

Etkinlik 1: Platform Keşfi
Süre 20

Öğrenim Hedefleri

- ❖ Çevrimiçi platformları kullanma ve temel özellikleri belirleme alıştırması.

İçerik/Yöntem

- ❖ Eğitmen, katılımcıları ikili gruplara ayırır ve her gruba bir görev kartı verir. Kartların, egzersiz sırasında nelere dikkat edilmesi gerektiğine dair talimatlar içerdiğini, örneğin bir banka veya alışveriş web sitesindeki güvenlik özelliklerini tanımayı içerdiğini bildirir. Egzersiz başladıktan sonra, eğitmen odada dolaşarak katılımcıları gözlemler, ipuçları verir ve soruları yanıtlar. Eğitmen ayrıca, katılımcıların güvenlik özelliklerini nasıl tanıyacaklarını anlamalarını sağlamak için, asma kilit simgeleri, 2FA ayarları, "https" adresleri veya güvenli ödeme sembolleri gibi temel güvenlik unsurlarına odaklanmalarına yardımcı olur. Alıştırma bittikten sonra, eğitmen her çifte araştırmaları sırasında keşfettiklerini kısaca paylaşmalarını ister. Eğitmen, "Bu görevde kolay olan ve zor olan neydi?" ve "Bir web sitesini veya uygulamayı güvenli veya güvenli olmayan olarak değerlendirmenize neden olan nedir?" gibi sorular sorarak kısa bir tartışma başlatır. Bu, katılımcıların deneyimlerini düşünmelerine ve bir çevrimiçi platformu güvenli kılan unsurları daha iyi anlamalarına yardımcı olur.
- ❖ Son olarak, eğitmen çevrimiçi platform güvenliği ile ilgili kısa makaleler veya videoların bağlantılarını paylaşarak ek kaynaklar sağlar. Web sitelerinin/uygulamaların güvenli ve güvenli olmayan unsurlarına ilişkin örnekler içeren basılı materyaller de referans materyali olarak dağıtılacak ve egzersiz sırasında edinilen bilgileri pekiştirecektir.

Materyal

- ❖ Katılımcılara basılı görev kılavuzları.
- ❖ Tabletler, dizüstü bilgisayarlar veya bankacılık veya alışveriş platformlarının demo sürümlerini içeren büyük basılı ekran görüntüleri.

Ara | Süre *5 dakika*

- ❖ **Katılımcıların dinlenip düşünmeleri için zaman tanıyın.**
- ❖ **Dinlenmek için kısa bir ara.**

4. Oturum

Ders 2: Güvenli Çevrimiçi Bankacılık Uygulamaları
Süre 30

Öğrenim Hedefleri

- ❖ Katılımcılara güçlü şifreler oluşturma ve hesapları izleme konusunda yardımcı olmak.

İçerik/Yöntem

- Eğitmen, çevrimiçi bankacılıkta temel güvenlik uygulamalarını ele alan bir sunumla başlar. Tartışılacak konular arasında güçlü şifreler oluşturma, iki faktörlü kimlik doğrulama (2FA) etkinleştirme ve hesap uyarıları ayarlama yer alır. Eğitmen, ders sırasında çevrimiçi bankacılık dolandırıcılığına ilişkin gerçek hayattan örnekler veya kısa hikayeler verecektir. Eğitmen, gerçek hayattan dolandırıcılık vakalarını kullanarak yaygın tehditleri vurgular ve pratik güvenlik ipuçları paylaşır. Bu tür vakalardan biri, dolandırıcılığın pratikte nasıl işlediğini gösteren, İrlanda'da bildirilen "Güvenli Hesap" dolandırıcılığıdır. Katılımcılar, bu adımları kendi cihazlarında uygulamaya teşvik edilir, böylece oturum pratik, yararlı ve hemen uygulanabilir hale gelir.
- Eğitmen, katılımcılara güvenli çevrimiçi bankacılığın neden önemli olduğunu ve güvenlik ihlallerinin ne sıklıkla meydana geldiğini açıklar. Potansiyel riskleri vurgular ve basit önlemlerin katılımcıları dolandırıcılıktan nasıl koruyabileceğini gösterir. Eğitmen, şifre gücü kontrol aracını kullanarak zayıf ve güçlü şifreler arasındaki farkı gerçek zamanlı olarak gösterir. Eğitmen, katılımcılardan örnek şifreler önermelerini ister ve bunları canlı olarak test ederek güçlü, benzersiz şifreler oluşturmanın önemini vurgular. Ardından, ekran görüntüleri veya canlı simülasyonlar kullanarak 2FA'yı nasıl etkinleştirebileceklerini gösterir. Eğitmen, yetkisiz erişimi önlemede 2FA'nın rolünü açıklar ve katılımcılara bunu etkinleştirme sürecinde rehberlik eder. Ardından, eğitmen bankacılık faaliyetlerini nasıl izleyeceğinizi ve şüpheli işlemler için uyarılar nasıl ayarlayacağınızı açıklayacaktır. Ekran görüntüleri veya örnek bir bankacılık uygulaması kullanarak, eğitmen katılımcılara bu uyarıları ayarlamak için gerekli adımları gösterir ve hesap faaliyetleri konusunda uyanık olmanın önemini vurgular. Soru-cevap oturumu sırasında, eğitmen katılımcılardan çevrimiçi bankacılık güvenliği ile ilgili deneyimlerini veya endişelerini paylaşmalarını ister. Son olarak, eğitmen, katılımcılar için yararlı bir kaynak olacak, güvenli çevrimiçi bankacılık alışkanlıklarını özetleyen basılı kontrol listeleri dağıtır.

Materyal

- Sunum, şifre gücü demo aracı.
- Basılı kontrol listesi.

Etkinlik 2: Çevrimiçi Bankacılığınızı Güvenli Hale Getirin
Süre 20

Öğrenim Hedefleri

- Katılımcılar, simüle edilmiş bir bankacılık ortamında 2FA'yı kurmayı ve işlemleri izlemeyi uygular.

İçerik/Yöntem

- Eğitmen, katılımcıları ikili gruplara veya küçük gruplara ayırır. Her grup, Revolut veya Monzo gibi demo uygulamaları veya bankacılık platformlarının yüklü olduğu dizüstü bilgisayarlar veya akıllı telefonlar üzerinde çalışır. Eğitmen, katılımcılara 2FA'yı etkinleştirme sürecinde rehberlik eder: Adım adım kılavuzu kullanarak, katılımcıların demo platformunda 2FA kurulum sürecini tamamlamalarına yardımcı olur. Odayı dolaşarak yardım sunar ve herkesin adımları doğru bir şekilde uyguladığından emin olur. Eğitmen daha sonra katılımcılardan yetkisiz işlem olup

olmadığını kontrol etmelerini ister ve şüpheli faaliyetler için uyarılar ayarlamalarına yardımcı olur. Katılımcıların süreci anladığından ve bu adımları demo platformlarında uyguladığından emin olur.

- Alıştırmadan sonra, her gruptan deneyimlerini paylaşmalarını isteyin: "2FA'yı kurarken hangi zorluklarla karşılaştınız?" "İşlem uyarılarını bulup ayarlayabildiniz mi? Hangi adımlar yardımcı oldu, hangileri zordu?" Geri bildirim sağlar: Çevrimiçi bankacılık güvenliği için 2FA'yı etkinleştirmenin ve işlemleri izlemenin önemini vurgular.

Malzeme

- Dizüstü bilgisayarlar veya akıllı telefonlar.
- Demo bankacılık uygulaması.
- 2FA'yı kurma ve işlemleri görüntüleme konusunda adım adım kılavuz.

Ara | Süre *5 dakika*

- **Dinlenmek ve hazırlanmak için zaman tanıyın**
- **Dinlenmek için kısa bir ara.**

5. Oturum

Ders 3: Güvenli Çevrimiçi Alışveriş
Süre 30

Öğrenim Hedefleri

- Yaşlıların web sitelerini değerlendirmeyi, güvenli ödeme seçeneklerini belirlemeyi ve dolandırıcı satıcıları tanımayı öğrenmelerine yardımcı olmak.

İçerik/ Yöntem

- Ders sırasında eğitmen, çevrimiçi alışveriş için güvenli web sitelerini nasıl tanıyacaklarını ve satıcıların gerçekliğini nasıl doğrulayacaklarını açıklar. Eğitmen, HTTPS protokolü, asma kilit simgeleri ve diğer güvenlik sembollerine odaklanarak güvenli web sitelerini nasıl tanıyacaklarını açıklar. Güvenilirliklerini nasıl değerlendireceklerini göstermek için iyi ve kötü web sitelerinin örneklerini sunar. Eğitmen ayrıca yorumları nasıl okuyacaklarını ve satıcıların gerçek olup olmadığını nasıl kontrol edeceklerini gösterir. Dersin sonunda eğitmen, katılımcılara "HTTPS protokolü web sitesi güvenliği hakkında ne diyor?" ve "Çevrimiçi bir satıcının güvenilir olup olmadığını nasıl kontrol edebilirsiniz?" gibi sorular sorarak temel kavramları pekiştirir ve katılımcıları derse dahil eder.
- Sonunda eğitmen, katılımcıları çevrimiçi alışveriş deneyimlerini veya güvenli çevrimiçi alışverişle ilgili endişelerini paylaşmaya teşvik eder. Katılımcıların çevrimiçi alışveriş yaparken karşılaşmış olabilecekleri tüm zorluklar tartışılır ve eğitmen, katılımcıların sorularını yanıtlar.

Materyal

- Basılı alışveriş örnekleri, web sitesi ekran görüntüleri.

Etkinlik 3: Güvenilir Web Sitelerinden Alışveriş Yapmak
Süre 20

Öğrenim Hedefleri

- Katılımcılar, çevrimiçi mağazaların güvenliğini değerlendirmeyi ve ödeme yöntemlerini doğrulamayı öğrenirler.

İçerik/Yöntem

- Katılımcılar gruplar halinde, önce mağazanın meşru web sitesini tanıyarak temel güvenlik özelliklerini (ör. HTTPS, güven mührü, güvenli ödeme seçenekleri) belirler. Ardından, bir sunum veya önceden kaydedilmiş bir video kullanılarak, sahte web siteleri veya şüpheli çevrimiçi etkinlik örnekleri gösterilir. Alıştırma, katılımcıların yaygın uyarı işaretlerini tanımalarına ve güvenli ve güvenli olmayan web sitelerini karşılaştırmalarına yardımcı olmaya odaklanır.
- Eğitmen, katılımcıları küçük gruplara ayırır ve onlara inceleyecekleri bir web sitesi listesi verir. Her grup, HTTPS protokolü, güvenli ödeme yöntemleri ve güvenilir yorumlar gibi göstergelere odaklanarak web sitelerinin güvenliğini değerlendirir. Eğitmen gruplar arasında dolaşarak gerektiğinde yardım sağlar ve grupların şüpheli yorumlar veya güvenli olmayan web sitesi öğeleri gibi uyarı işaretlerini tanımlamada yardıma ihtiyaç duymaları halinde rehberlik eder. Sonunda, gruplar güvenli olduğu düşünülen web siteleri hakkında bilgi paylaşır ve değerlendirmelerini gerekçelendirir.

Malzeme

- İnternet erişimi olan bilgisayarlar.
- Alışveriş web sitelerinin listesi.

Mola | Süre 5 dakika

- **Dinlenmek ve hazırlanmak için zaman tanıyın.**
- **Dinlenmek için kısa bir ara.**

6. Oturum

Ders 4: Kişisel ve Finansal Bilgilerin Korunması
Süre 30

Öğrenim Hedefleri

- Yaşlılara cihazların güvenliğini sağlama, antivirüs yazılımı kullanma ve Wi-Fi bağlantılarını güvenli hale getirme konusunda bilgi kazandırmak.

İçerik/Yöntem

- Eğitmen, antivirüs yazılımı, VPN'ler ve güvenli web taraması kavramlarını açıklayan bir ders verir. Sunum, her konu için önemli bilgiler ve örnekler içeren slaytlar içerir ve cihaz güvenliği için en iyi uygulamaları vurgular. Eğitmen, güvenliği artırmak için cihazların nasıl güncelleneceğini, antivirüs yazılımının nasıl yükleneceğini ve gizlilik ayarlarının nasıl yönetileceğini gösterir. Güvenli web taraması için VPN'in doğru kullanımını gösteren kısa bir

eğitim videosu gösterir. Sunum boyunca eğitmen, katılımcıları aktif olarak katılmaya teşvik eder ve sorular sorarak ve çevrimiçi güvenliği sağlamaya yönelik gerçek hayattan örnekler vererek oturumu etkileşimli hale getirir. Sunumun ardından katılımcılar, cihaz güvenliği ve çevrimiçi koruma ile ilgili sorularını sorma ve şüphelerini giderme fırsatı bulur.

- Son olarak, eğitmen şüpheli bağlantılardan kaçınmak, web sitelerinde çok fazla bilgi paylaşmamak ve yaygın çevrimiçi tuzakları tanımak gibi kişisel verileri korumak için basit, günlük uygulamaları paylaşır. Bu adımlar, katılımcıların daha güvenli dijital alışkanlıklar geliştirmelerine yardımcı olur.

Materyal

- Sunum slaytları, VPN'ler hakkında video eğitimi.

Etkinlik 4: Cihazlarınızı Güvenli Hale Getirme
Süre 20

Öğrenim Hedefleri

- Katılımcılar antivirüs yazılımı yüklemeyi, VPN kullanmayı ve gizlilik ayarlarını yönetmeyi uygular.

İçerik/Yöntem

- Katılımcılar gruplar halinde çalışarak antivirüs yazılımı yükler, güvenli web taraması için VPN'i etkinleştirir ve uygulamalarda ve sosyal medyada gizlilik ayarlarını kontrol eder. Bu uygulamalı alıştırma, katılımcıların cihazlarını ve kişisel verilerini çevrimiçi olarak korumak için pratik adımlar uygulamalarına yardımcı olur.
- Eğitmen, katılımcıları küçük gruplara veya çiftlere ayırır ve alıştırma sırasında kullanmaları için onlara dizüstü bilgisayarlar, antivirüs yazılımı ve VPN uygulamaları sağlar. Her grup, eğitmen tarafından sağlanan adım adım talimatları izleyerek antivirüs yazılımı yükler, güvenli web taraması için VPN'i etkinleştirir ve uygulamalarda ve sosyal medya hesaplarında gizlilik ayarlarını kontrol eder. Eğitmen gruplar arasında dolaşarak gerektiğinde yardım sunar ve tüm katılımcıların görevleri başarıyla tamamlayabilmesini sağlar. Eğitmen ayrıca gruplara, cihazlarında ve sosyal medya profillerinde güvenliği artıran önemli gizlilik ayarlarını belirleme sürecinde rehberlik eder. Alıştırmanın ardından eğitmen, katılımcılardan cihazlarının güvenliğini sağlama ve gizlilik ayarları konusundaki deneyimlerini paylaşmalarını ister.

Malzeme

- Dizüstü bilgisayarlar, antivirüs yazılımı, VPN uygulaması

7. Oturum

Tartışma | Süre 10 dakika

Öğrenme Hedefleri

- Oturumdan elde edilen önemli bilgileri düşünün ve sorularınızı netleştirin.

İçerik/ Yöntem

- Katılımcıların deneyimlerini ve sonuçlarını paylaştıkları grup tartışması. Eğitmen, kalan soruları yanıtlar. Katılımcıları, oturumda edindikleri becerileri uygulamaya devam etmeleri için teşvik eder.

Özet
Süre 5

Öğrenme Hedefleri

- Oturumu özetler ve katılımcıları güvenli bir şekilde uygulamaya devam etmeye teşvik eder.

İçerik/Yöntem

- Eğitmen, oturumu özetleyerek tartışılan en önemli konuları vurgular. Katılımcılar, kişisel çevrimiçi etkinlikleri aracılığıyla edindikleri becerileri uygulamaya devam etmeye teşvik edilir. Eğitmen, katılımcılara katılımları için teşekkür eder ve edindikleri bilgileri internette güvenliklerini sağlamak için kullanmaya teşvik eder.

Materyal

- Önemli noktalar ve kaynakları içeren el broşürleri.

4.4 Ek Bilgiler

4.4.1 Eğitmenlerin Kendi Kendine Yansıtma

Eğitimin hangi yönleri özellikle iyi gitti?
Oturumun hangi kısımlarını sunmak benim için en zordu?
Katılımcılar etkinlikler boyunca ne kadar ilgili ve duyarlı davrandılar?
Katılımcılar öğrenme hedeflerine ulaşabildiler mi? Ulaşamadılarsa, neden?
Gelecekteki oturumlarda oturumu iyileştirmek için ne gibi düzenlemeler yapılabilir?

4.4.2 Eğitmenlerin Program Değerlendirmesi

- Eğitim içeriği yaşlıların ihtiyaçlarına uygun ve onların bilgi düzeyine ve dijital deneyimlerine uyarlanmış mıydı?
- Katılımcılar çevrimiçi bankacılık, e-ticaret, siber güvenlik ve çevrimiçi gizlilik ile ilgili temel ilkeleri anladılar mı?
- Pratik alıştırmalar, testler ve gösterimler öğrenmeyi pekiştirmek ve dijital güveni artırmak açısından etkili miydi?
- Tartışmalar ve yansıtmalar, katılımcıların güvenli çevrimiçi uygulamalar hakkındaki anlayışlarını derinleştirmelerine olanak sağladı mı?
- Güçlü şifreler oluşturma, sahte web sitelerini tanıma, işlemleri izleme ve güvenlik ayarlarını yapılandırma gibi hedeflenen öğrenme çıktıları elde edildi mi?
- Katılımcılar, çevrimiçi bankacılık ve alışveriş işlemlerini gerçekleştirirken artan bir güven ve bağımsızlık sergilediler mi?
- Eğitimin hangi yönleri en başarılıydı ve gelecekteki oturumlar için hangi alanlar iy?

4.4.3 Materyaller, Ek Kaynaklar

Ek 1 | Güçlü Şifrelerin Özellikleri

Çevrimiçi hesaplarınızın güvenliğini sağlamak için şifreniz aşağıdaki özelliklere sahip olmalıdır:

- En az 8 karakter – ne kadar uzun olursa o kadar iyi
- Büyük ve küçük harflerin karışımı
- Harf ve rakamların birleşimi
- En az bir özel karakter içermeli, örneğin !, @, #, ?,]
- Not: Şifrenizde < veya > karakterlerini kullanmayın, bunlar web tarayıcılarında sorunlara neden olabilir
- Ayrıntılı broşürler aşağıdadır!

Çevrimiçi Bankacılık ve Alışveriş Güvenliği
Güçlü Şifrelerin Özellikleri
Güçlü Şifrelerin Önemi

Güçlü şifreler oluşturmak, kişisel ve profesyonel verilerinizi korumak için önemli bir adımdır. Zayıf şifreler, bilgisayar korsanlarının hesaplarınıza erişmesini kolaylaştırır.

Güvenli şifreler oluşturmak için aşağıdaki yönergeleri kullanın:

<u>Güçlü Şifrelerin Özellikleri</u>

- En az 8 karakter – ne kadar uzun olursa o kadar iyidir.
- Büyük ve küçük harflerin birleşimi.
- Harf ve rakamların karışımı.
- En az bir özel karakter, örneğin: !, @, #, ?,].
- Şifrenizde < veya > karakterlerini kullanmaktan kaçının, çünkü bunlar bazı web tarayıcılarında sorunlara neden olabilir.
- Ek İpuçları
- Kişisel bilgilerinizi (adınız veya doğum tarihiniz gibi) kullanmayın.
- Her hesap için benzersiz bir şifre kullanın.
- Güvenilir bir şifre yöneticisi kullanmayı düşünün.
- Şifrelerinizi düzenli olarak değiştirin ve eski şifreleri tekrar kullanmaktan kaçının.

Uygulama Bölümü (İsteğe Bağlı)
Yukarıdaki ipuçlarını kullanarak güçlü bir örnek şifre oluşturun:

Parolanızın gücünü değerlendirin:

ZAYIF	ORTA	GÜÇLÜ

Ek 2 | 2FA ve Uyarılar için Adım Adım Talimatlar

Bölüm I: *İki Faktörlü Kimlik Doğrulama (2FA) Kurma*

Amaç: *2FA, hem şifrenizi hem de ikinci bir doğrulama yöntemini (örneğin, telefonunuza gönderilen kod) gerektirerek ekstra güvenlik sağlar.*

Adımlar

1. Cihazınızda demo bankacılık uygulamasını veya platformunu açın.

2. Ayarlar → Güvenlik Ayarları'na gidin.

3. İki Aşamalı Kimlik Doğrulamayı Etkinleştir (2FA) seçeneğine dokunun.

4. Doğrulama yönteminizi seçin:

- SMS Kodu

- Doğrulama Uygulaması (ör. Google Authenticator)

5. Talimatları izleyin (aldığınız doğrulama kodunu girin).

6. 2FA'nın etkin ve çalışır durumda olduğunu onaylayın.

Bölüm 2*: İşlemleri İnceleme ve Uyarıları Ayarlama*

Amaç: *İşlemlerinizi izlemek ve uyarılar ayarlamak, şüpheli etkinlikleri erken tespit etmenize yardımcı olur.*

Adımlar:

7. Uygulamada İşlem Geçmişi'ne gidin.

8. Son işlemleri inceleyin.

9. Tanımadığınız işlemleri belirleyin ve işaretleyin.

10. Bildirimler veya Uyarı Ayarları'na gidin.

11. Aşağıdakiler için uyarıları etkinleştirin:

- Büyük veya olağandışı işlemler

- Yeni cihazlardan yapılan oturum açma işlemleri

- Hesap ayarlarınızdaki değişiklikler

Önemli Hatırlatmalar

- *Tüm finansal uygulamalarda 2FA'yı etkinleştirin.*
- *İşlem geçmişinizi düzenli olarak kontrol edin.*
- *Olağandışı etkinlikler hakkında bildirim almak için uyarıları kullanın.*

Ek 3 | Bankacılık ve çevrimiçi alışveriş platformlarında güvenlik unsurlarını tanıma

Görev 1. Hesap bakiyesini bulun

Hesap bakiyesini kontrol edebileceğiniz yeri bulun.

- Nerede bulunur? .....
- Nasıl etiketlenmiştir (örneğin, "Bakiye", "Hesap özeti", "Kullanılabilir fonlar")? .....

Görev 2. Ödeme seçeneğini bulun

Ödeme yapabileceğiniz veya satın alma işlemini tamamlayabileceğiniz yeri bulun.

- Bu seçeneğin adı nedir?
  ☐ Transfer
  ☐ Öde
  ☐ Sepet / Ödeme
  ☐ Diğer: .....
- Bulmak kolay mıydı?
  ☐ Evet
  ☐ Hayır
  Neden? .....

Görev 3. Web sitesinin güvenlik özelliklerini belirleyin

Web sitesini dikkatlice inceleyin ve güvenli olduğunu gösteren öğeleri işaretleyin.

☐ Tarayıcı adres çubuğundaki kilit simgesi

☐ adresin **https** ile başlaması

☐ tanınabilir ödeme sistemi logoları (ör. Visa, Mastercard, PayPal, BLIK)

☐ ek ödeme onayı (SMS kodu, bankacılık uygulaması)

☐ gizlilik politikası bilgileri

Başka bir şey fark ettiniz mi? .....

Görev 4. Olası uyarı işaretlerini arayın

Web sitesinin güvenli olmayabileceğini gösteren herhangi bir şey fark ettiniz mi?

☐ kilit simgesi yok

☐ şüpheli web sitesi adresi

☐ çok fazla açılır pencere

☐ çok fazla kişisel bilgi isteyen

☐ diğer: .....

Görev 5. Ek güvenlik ayarlarını kontrol edin

Ek hesap veya ödeme koruması hakkında bilgi arayın.

Şunları buldunuz mu:

☐ iki faktörlü kimlik doğrulama (2FA)

☐ SMS doğrulama

☐ bankacılık uygulaması aracılığıyla onay

Bu seçenek nerede bulunur? .....

Alıştırma Özeti:
Görevin en kolay kısmı neydi? .....
En zor kısmı neydi? .....
Bir web sitesinin veya uygulamanın güvenli olduğunu anlamanıza ne yardımcı olur?
.....

Sonuç: Çevrimiçi bankacılık ve alışveriş platformlarını güvenli bir şekilde kullanmak için web sitesi güvenlik göstergelerine, web adresine ve ödemelerin onaylanma şekline dikkat etmek gerekir.

Unutmayın: Bir web sitesinde sizi tedirgin eden veya şüphe uyandıran bir şey varsa, **kişisel verilerinizi girmeyin ve işlemi durdurun.**

Ek 4 | Katılımcılar için daha fazla okuma ve öğrenme önerileri

Siber güvenlik web siteleri: Siber güvenlikle ilgilenen Avrupa ve hükümet kuruluşları

1) **Tüm Çevrimiçi Hesaplarınızda İki Aşamalı Kimlik Doğrulamayı Nasıl Ayarlarsınız?**
   Web sitesi: https://www.loginradius.com/blog/identity/how-to-setup-2fa-in-online-accounts/
   Bu kapsamlı kılavuz, iki faktörlü kimlik doğrulamanın (2FA) önemini açıklar ve e-posta, sosyal medya ve bankacılık platformları dahil olmak üzere çeşitli çevrimiçi hesaplarda bunu kurmak için adım adım talimatlar sağlar. Hesap güvenliğini artırmak için SMS kodları, kimlik doğrulama uygulamaları ve donanım güvenlik anahtarları gibi yöntemleri kapsar.
2) **2 Faktörlü Kimlik Doğrulama Ayarlama | Teknoloji Destek Hizmetleri**
   Web sitesi: https://it.nmu.edu/docs/setting-2-factor-authentication
   Northern Michigan Üniversitesi BT departmanının hazırladığı bu kaynak, MyNMU ve MyUser gibi NMU hizmetlerinde iki faktörlü kimlik doğrulamayı (2FA) etkinleştirme sürecini açıklamaktadır. Üniversite sistemlerine güvenli erişim sağlamak için kimlik doğrulama uygulamaları, USB güvenlik anahtarları ve yedek kodlar dahil olmak üzere birden fazla doğrulama seçeneği sunmaktadır.
3) **Bank of Ireland, "Güvenli Hesap" Dolandırıcılığındaki Artışa Karşı Uyardı**
   Makale: https://www.rte.ie/news/business/2025/0606/1517043-spike-in-safe-account-scam-warning-boi/
   Bu haber makalesi, İrlanda'da 'güvenli hesap' dolandırıcılığına ilişkin raporların önemli ölçüde arttığını ve geçen hafta on kat artış gösterdiğini bildiriyor. Bank of Ireland, dolandırıcıların sahte bahanelerle bireyleri 'güvenli' hesaplara para transferi yapmaya ikna ettiği bu tür dolandırıcılık konusunda tüketicileri uyarıyor ve dikkatli olmanın ve güvenli bankacılık uygulamalarının önemini vurguluyor.
4) **Ulusal Siber Güvenlik Merkezi – Güvenli Çevrimiçi Alışveriş**
   Web sitesi: https://www.ncsc.gov.uk/guidance/shopping-online-securely
   Bu resmi Birleşik Krallık hükümeti kılavuzu, tüketicilere çevrimiçi alışverişte güvenlik için pratik ipuçları sunuyor. Çevrimiçi mağazaların meşruiyetini doğrulama, güvenli ödeme yöntemleri kullanma, kişisel bilgileri koruma ve şüpheli faaliyetleri bildirme gibi konuları kapsıyor. Önemli öneriler arasında çevrimiçi alışverişlerde kredi kartı kullanma, iki aşamalı doğrulamayı etkinleştirme ve istenmeyen tekliflere ve bağlantılara karşı dikkatli olma yer alıyor.
5) **Güçlü Bir Şifre Oluşturma**
   Video: https://www.youtube.com/watch?v=_wQTRMBAvzg
   Bu video, güçlü ve hatırlanması kolay şifreler oluşturmak için pratik ipuçları sunar. Harf, rakam ve sembollerin bir kombinasyonunu kullanmanın, yaygın hatalardan kaçınmanın ve şifre cümlelerini güvenli bir alternatif olarak değerlendirmenin önemini vurgular.
6) **TechRadar – Sanal Özel Ağlar (VPN'ler)**
   Web sitesi: https://www.techradar.com/vpn/virtual-private-networks
   TechRadar'ın bu kapsamlı kılavuzu, Sanal Özel Ağlar (VPN) kavramını incelemektedir. VPN'lerin nasıl çalıştığını, çevrimiçi gizlilik ve güvenlik açısından faydalarını açıklamakta ve uzman testlerine dayalı olarak en iyi VPN hizmetleri için öneriler sunmaktadır.

4.5 Modül III – Ön/Son Test

1. Bir web sitesi adresinde "HTTPS" neyi gösterir?

A) Web sitesi başka bir ülkede barındırılıyor
B) Web sitesi güvenlidir ve veriler şifrelenmiştir
C) Web sitesi indirimler sunmaktadır
D) Web sitesi giriş gerektirir

2. Çevrimiçi bankacılık için İki Aşamalı Kimlik Doğrulama (2FA) kullanmak neden önemlidir?

A) Çevrimiçi işlemleri hızlandırır
B) Aynı anda birden fazla cihazdan giriş yapmanızı sağlar
C) İki doğrulama adımı gerektirerek ekstra bir güvenlik katmanı sağlar
D) Şifre ihtiyacını ortadan kaldırır

3. Antivirüs yazılımı kullanmanın temel faydası nedir?

A) Bilgisayarınızı daha hızlı hale getirir
B) Kötü amaçlı yazılımlara ve kimlik avı saldırılarına karşı koruma sağlar
C) Çevrimiçi şifrelerin yönetilmesine yardımcı olur
D) Tüm çevrimiçi alışveriş sitelerine erişimi engeller

4. Aşağıdaki şifrelerden hangisi en güvenli olanıdır?

A) Shopping2024
B) 12345678
C) Mybankpassword
D) H@ppy$hopper92!

5. "Gerçek olamayacak kadar iyi" görünen bir çevrimiçi teklif gördüğünüzde ne yapmalısınız?

A) Hemen arkadaşlarınızla paylaşın
B) Ayrıntıları kontrol etmek için bağlantıya tıklayın
C) Kaçının ve herhangi bir işlem yapmadan önce web sitesini doğrulayın
D) Teklifi hızlı bir şekilde almak için bilgilerinizi girin

6. Çevrimiçi alışveriş için güvenli bir ödeme yöntemi nedir?

A) Güvenli bir web sitesinde kredi kartıyla ödeme yapmak
B) Doğrudan banka havalesi ile para göndermek
C) Kart numaranızı e-posta ile paylaşmak
D) Web sitesi profesyonel görünüyorsa herhangi bir yöntemi kullanmak

7. Finansal işlemler için halka açık Wi-Fi kullanmaktan neden kaçınmalısınız?

A) Çevrimiçi bankacılık için çok yavaştır
B) Şifrelenmemiş olabilir ve bilgisayar korsanlarının verilerinizi çalmasına izin verebilir
C) Güvenli web sitelerini desteklemez
D) Banka uygulamalarına erişimi engeller

8. Tarayıcının adres çubuğundaki asma kilit simgesi ne anlama gelir?

A) Web sitesi bakımda
B) Cihazınız ile web sitesi arasındaki bağlantı güvenlidir
C) Web sitesi çerez gerektiriyor
D) Web sitesi güvenilir değildir

9. Güvenilir bir çevrimiçi alışveriş web sitesini nasıl belirleyebilirsiniz?

A) E-posta ile şifrenizi ister
B) Yazım hataları ve belirsiz iletişim bilgileri içerir
C) HTTPS, asma kilit simgesi ve doğrulanmış müşteri yorumları vardır
D) Ödeme yapmadan ücretsiz ürünler sunar

10. Cihazınızı ve finansal bilgilerinizi korumak için ne yapmalısınız?

A) Bilgisayarınızı daha hızlı hale getirmek için antivirüs yazılımını devre dışı bırakın
B) Yazılımınızı güncel tutun ve halka açık ağlarda VPN kullanın
C) İşlem geçmişinizi kontrol etmekten kaçının
D) Tüm hesaplarınız için aynı şifreyi kullanın

Cevap Anahtarı Özeti

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

MODÜL IV

Yaşlılar İçin Güvenli ve Sorumlu Sosyal Medya Kullanımı

5. Modül IV Yaşlılar için Güvenli ve Sorumlu Sosyal Medya Kullanımı

"Sosyal Medyanın Güvenli Kullanımı" modülü, temel bilgileri pratik rehberlikle birleştirerek yaşlılara sosyal medya platformlarını sorumlu ve güvenli bir şekilde kullanmayı öğretir. Katılımcılar, hesap oluşturma ve yönetme, gizlilik ayarlarını değiştirme, yaygın çevrimiçi dolandırıcılık yöntemlerini tanıma ve güvenli iletişim kurma yöntemlerini öğrenerek dijital sosyal alanlara daha fazla güven ve kontrol ile katılabilirler.
Modül, katılımcıların sosyal medyada sıkça rastlanan şüpheli mesajları, sahte profilleri ve yanıltıcı bağlantıları tanımlamalarına yardımcı olan pratik etkinlikler içerir. Ayrıca, etkili gizlilik yönetimi, sınırlı veri paylaşımı ve güçlü şifreler ve iki faktörlü kimlik doğrulama gibi güvenli hesap uygulamaları yoluyla kişisel bilgilerin ve dijital kimliğin korunmasına odaklanır. Cihaz güvenliği, yazılım güncellemeleri ve güvenli internet bağlantıları hakkında da rehberlik sağlanır.
Bu unsurları bir araya getiren modül, yaşlıların sosyal medya ile ilgili riskleri anlamalarını sağlamakla kalmaz, aynı zamanda bu riskleri etkili bir şekilde yönetmek için pratik beceriler geliştirmelerini de sağlar. Katılımcılar, modülü tamamladıklarında dijital farkındalıkları ve özgüvenleri artmış ve günlük çevrimiçi etkileşimlerinde güvenli sosyal medya uygulamalarını kullanma becerisi kazanmış olurlar.

5.1 Öğrenme Hedefleri

Bu modülün amacı, yaşlıların sosyal medyayı güvenli, sorumlu ve anlamlı bir şekilde kullanma konusundaki anlayış ve becerilerini geliştirmektir. Bu eğitim sayesinde, 65 yaş ve üstü yaşlılar:

- Popüler sosyal medya platformlarında gezinme konusunda güven kazanacaklar.
- Gizlilik ayarlarının önemini anlayacak ve bunları etkili bir şekilde nasıl ayarlayacaklarını öğreneceklerdir.
- Sosyal medyada yaygın çevrimiçi dolandırıcılık ve tehditleri tanımlayıp bunlardan kaçınacaklar.
- Çevrimiçi ortamda kişisel bilgilerin güvenli ve sorumlu bir şekilde paylaşılmasına yönelik alışkanlıklar geliştirecektir.
- Güvenliklerini ve refahlarını sağlarken sosyal medya içeriğiyle sorumlu bir şekilde etkileşim kuracaklardır.

5.2 Yapı, İçerik ve Öğrenim Çıktıları

Bu modülü başarıyla tamamlayan öğrenciler şunları yapabileceklerdir:

- Facebook, Instagram ve LinkedIn gibi popüler platformların temel özelliklerini ve kullanım alanlarını tanımlayın.
- Güçlü şifreler seçmek ve iki faktörlü kimlik doğrulamayı etkinleştirmek gibi güvenli yöntemler kullanarak sosyal medya hesapları oluşturma becerisini göstermek.
- Kişisel bilgilerin ve gönderilerin görünürlüğünü kontrol etmek için gizlilik ayarlarını özelleştirmek.
- İstenmeyen mesajları ve bağlantı isteklerini kısıtlamak için iletişim ayarlarını yönetmek.
- Kimlik avı, sahte profiller ve dolandırıcılık amaçlı bağlantılar gibi dolandırıcılık uyarı işaretlerini tanımlayabilecek.
- Hassas kişisel verileri kötü niyetli kişilerden korumak için stratejiler uygulayın.
- Çevrimiçi güvenlik için en iyi uygulamalara uyum sağlamak amacıyla daha önce paylaşılan içeriği gözden geçirin ve değiştirin.
- Aşırı paylaşımdan veya hassas içerik paylaşımından kaçınmak dahil olmak üzere, bilgileri güvenli bir şekilde paylaşma alışkanlıkları geliştirin.

5.3 Gündem I Ayrıntılı Oturum Planı

MODÜL IV
Yaşlılar için Güvenli ve Sorumlu Sosyal Medya Kullanımı

1. Oturum

Hoş geldiniz
Süre 5

Öğrenim Hedefleri

- Konuyu tanıtın ve samimi bir ortam yaratın.

İçerik/ Yöntem

- Oturuma kısa bir giriş yapın, hedefleri özetleyin ve beklentileri belirleyin.
- Modülü ve önemini özetleyerek eğitim için zemin hazırlamak.

Malzeme

- Oturum hedefleri için beyaz tahta veya flip chart.
- Marker kalemler.
- Oturumu özetleyen basılı gündem veya sunum slaytları.

2. Oturum

Buzkıran Etkinliği: Sosyal Medya Bingo
Süre 5 dakika

Öğrenim Hedefleri

- Katılımcıların etkileşimini teşvik etmek ve dijital alışkanlıkları hakkında düşünmeye başlamalarını sağlamak.

İçerik/ Yöntem

- Katılımcılar kendilerini tanıtırken, aşina oldukları terimleri işaretleyeceklerdir. Bingo kartındaki bir sırayı ilk tamamlayan katılımcı küçük bir ödül kazanacaktır. Bu, katılımcıları sosyal medya deneyimlerini paylaşmaya teşvik edecek ve dijital alışkanlıkları hakkında sohbet başlatacaktır.

Malzeme

- "Facebook", "Instagram", "Beğen", "Hashtag", "Yorum", "Takip Et", "Profil" gibi yaygın sosyal medya terimlerinin yazılı olduğu kartları yazdırın.
- Kalemler, fosforlu kalemler ve/veya çıkartmalar

3. Oturum

Ders 1: Sosyal Medyaya Genel Bakış
Süre *30*

Öğrenim Hedefleri

- Katılımcıların sosyal medya platformlarının temel işlevlerini ve türlerini anlamalarına yardımcı olmak.

İçerik/ Yöntem

- Popüler platformların (Facebook, Instagram, Twitter vb.) genel bir özetini sunarak temel özelliklerini ve işlevlerini açıklamak. Bu platformların özelliklerini, avantajlarını, potansiyel risklerini ve güvenli bir şekilde hesap oluşturma yöntemlerini açıklamak.

Materyal

- Popüler sosyal medya platformlarını, özelliklerini ve güvenlik risklerini içeren sunum slaytları.
- Sunum için projektör ve dizüstü bilgisayar.
- Facebook, Instagram ve Twitter'ın özelliklerini ve güvenlik ipuçlarını özetleyen el broşürleri.
- Platform özelliklerinin canlı gösterimi için internet bağlantısı.

Etkinlik 1: Platforma Aşina Olma
Süre 20 dakika

Öğrenim Hedefleri

- Katılımcıların sosyal medya platformlarında gezinmeyi öğrenmeleri.

İçerik/Yöntem

- Platformların (ör. Facebook, Instagram, Twitter) uygulamalı olarak keşfedilmesi. Katılımcılar, güvenlik önlemlerine (ör. güçlü şifreler seçme, iki aşamalı kimlik doğrulamayı etkinleştirme) önem vererek sosyal medya hesabı oluşturma alıştırması yapacaklar.

Malzeme

- Katılımcıların platformları keşfetmeleri için bilgisayarlar, tabletler veya akıllı telefonlar.
- Hesapları güvenli bir şekilde oluşturmaya ilişkin basılı kılavuzlar, şunları içerir: *Güçlü şifreler oluşturmaya ilişkin talimatlar. İki faktörlü kimlik doğrulamayı etkinleştirme adımları*

Ara | Süre *5 dakika*

- **Katılımcıların dinlenip düşünmeleri için zaman tanıyın.**
- **Dinlenmek için kısa bir ara.**

4. Oturum

Ders 2: Gizlilik Ayarları

Süre *30*

Öğrenim Hedefleri

- Katılımcılara gizlilik ayarlarını düzenleme ve kişisel verileri koruma becerileri kazandırmak.

İçerik/ Yöntem

- Kişisel bilgileri korumak için sosyal medya platformlarında gizlilik ayarlarının nasıl değiştirileceğini öğretmek.

Materyal

- Yaygın platformların gizlilik ayarlarını açıklayan sunum slaytları.
- Facebook, Instagram ve Twitter'da gizlilik ayarlarını değiştirmeye ilişkin adım adım basılı kılavuzlar.
- Gizlilik ayarlarının canlı olarak gösterilmesi için projektör ve dizüstü bilgisayar.

Etkinlik 2: Gizlilik Ayarlarını Yapılandırma

Süre *20 dakika*

Öğrenim Hedefleri

- Katılımcılara sosyal medya platformlarında gizlilik ayarlarının nasıl yapılandırılacağını uygulamalı olarak öğretmek.

İçerik/Yöntem

- Katılımcıların kendi sosyal medya hesaplarında gizlilik ayarlarını düzenledikleri etkileşimli alıştırma.

Malzeme

- Uygulamalı alıştırma için bilgisayarlar, tabletler veya akıllı telefonlar.
- Kişisel hesabı olmayan katılımcılar için önceden oluşturulmuş sahte hesaplar (isteğe bağlı).
- Yapılan gizlilik ayarlamalarını not etmek için boşluk bulunan basılı çalışma kağıtları.

Ara | Süre *5 dakika*

- **Dinlenmek ve bir sonraki oturuma hazırlanmak için zaman tanıyın.**
- **Dinlenmek için kısa bir ara.**

5. Oturum

Ders 3: Sosyal Medyada Dolandırıcılık ve Çevrimiçi Tehditleri Tanıma
Süre *30 dakika*

Öğrenim Hedefleri

- Katılımcıların sosyal medyaya özgü dolandırıcılıkları ve tehditleri tanımalarına yardımcı olmak.

İçerik/ Yöntem

- Kimlik avı, sahte reklamlar, sahte profiller ve kimlik hırsızlığı dahil olmak üzere yaygın sosyal medya dolandırıcılıklarını tartışmak.

Materyal

- Kimlik avı e-postaları ve sahte arkadaşlık istekleri gibi dolandırıcılık örneklerini gösteren sunum slaytları.
- Yaygın dolandırıcılık yöntemlerini ve dikkat edilmesi gereken uyarı işaretlerini ayrıntılı olarak açıklayan basılı el broşürleri.
- Sosyal medya dolandırıcılıklarının örneklerini veya videolarını göstermek için projektör ve dizüstü bilgisayar.

Etkinlik 3: Dolandırıcılık Tanıma Alıştırması
Süre 20 dakika

Öğrenim Hedefleri

- Sosyal medya dolandırıcılıklarını tespit etme becerisini geliştirmek ve dolandırıcılık planlarına kanmamayı öğrenmek.

İçerik/Yöntem

- Katılımcıların sahte arkadaşlık istekleri veya kimlik avı mesajları gibi sosyal medya dolandırıcılık örneklerini belirleyip tartıştıkları grup etkinliği.

Materyal

- Grup tartışması için dolandırıcılık örneklerini içeren senaryo kartları.
- Grubun bulgularını not almak için flip chart veya beyaz tahta.
- Katılımcıların yanıtlarını kaydetmek için kalemler.

Ara | Süre 5 dakika

- **Dinlenmek ve hazırlanmak için zaman tanıyın.**
- **Dinlenmek için kısa bir ara.**

6. Oturum

Ders 4: Sosyal Medyada Güvenli ve Sorumlu Bir Şekilde Etkileşim Kurmak
Süre *30*

Öğrenim Hedefleri

- Güvenli ve sorumlu sosyal medya kullanımının önemini açıklamak
- Öğrencilere güvenli paylaşım alışkanlıkları geliştirmeyi öğretmek.

İçerik/Yöntem

- *"Çevrimiçi güvenlik bireyler ve profesyoneller için neden önemlidir?"* sunumu**.** Güvenli olmayan paylaşım uygulamalarının potansiyel risklerine örnekler (ör. kimlik hırsızlığı, itibar kaybı). Öğrencilere varsayımsal senaryolar sunun (ör. tatil planlarını veya profesyonel başarılarını paylaşmak). Şu soruları sorun: *"Neyi paylaşırdınız? Bunu nasıl güvenli bir şekilde paylaşırdınız?".* Yanıtlar üzerine grup tartışması.

Materyal

- Çevrimiçi risklere ilişkin istatistiklerin yer aldığı slaytlar.
- Güvenli olmayan uygulamaların temel risklerini ve sonuçlarını özetleyen infografik.

Etkinlik 4: Geçmişteki Paylaşımları ve Bilgileri Gözden Geçirme
Süre *20*

Öğrenme Hedefleri

- Öğrencilerin sosyal medya profillerini ve gönderilerini güvenlik açısından değerlendirip değiştirmelerini sağlamak.

İçerik/Yöntem

- Örnek bir sosyal medya profilinin (kurgusal veya anonimleştirilmiş örnek) rehberli denetimi. Güvenli olmayan veya aşırı kişisel içeriği (ör. telefon numaraları, konumlar, hassas fotoğraflar) belirleme. Gönderileri silme veya değiştirme ve gizlilik ayarlarını düzenlemeyi gösterme.

Materyal

- Örnek sosyal medya profili (basılı veya ekranda).
- Gizlilik ayarlarını değiştirmeye yönelik adım adım kılavuz (PDF veya el broşürü).

7. Oturum

Tartışma | Süre 10 dakika

Öğrenim Hedefleri

- Sosyal medyada şüpheli faaliyetleri fark etme ve bildirme konusunda proaktif bir zihniyetin teşvik edilmesi.

İçerik/ Yöntem

- Dolandırıcılıkları nasıl bildireceğimiz ve sahte hesapları nasıl tanıyacağımız gibi şüpheli sosyal medya faaliyetleriyle nasıl başa çıkılacağına dair grup tartışması.

Malzeme

- Dolandırıcılıkları bildirme ve şüpheli hesaplarla nasıl başa çıkılacağına dair fikir üretmek için beyaz tahta ve kalemler.
- Dolandırıcılıkları bildirmek için iletişim bilgilerinin bulunduğu basılı kaynaklar (ör. platform yardım merkezlerine bağlantılar)

Özet | Süre 5 dakika

Öğrenim Hedefleri

- Eğitimi özetleyin ve katılımcıların sosyal medya tehditlerinden kendilerini nasıl koruyacaklarını anladıklarından emin olun.

İçerik/Yöntem

- Sosyal medya dolandırıcılıkları ve tehditleri ile ilgili önemli noktaları gözden geçirin, kalan soruları yanıtlayın ve sürekli öğrenme için kaynaklar sağlayın.

Materyal

- Oturumda ele alınan önemli noktaları özetleyen el broşürleri: ***Sosyal medya güvenlik kontrol listesi***

5.4 Ek Bilgiler

5.4.1 Eğitmenlerin Kendi Kendine Yansıtma

- Çevrimiçi güvenlik ve sosyal medya etkileşiminin önemini etkili bir şekilde aktardım mı?
- Katılımcıların gizlilik ayarlarının ve dolandırıcılık tanıma tekniklerinin teknik yönlerini anladıklarından emin oldum mu?
- Katılımcıları etkinliklere ve tartışmalara nasıl dahil ettim?
- Kaynaklar ve materyaller katılımcılar için yararlı oldu mu?

5.4.2 Eğitmenlerin Program Değerlendirmesi

- Eğitimin içeriği yaşlılar için uygun ve anlaşılır mı?
- Etkinlikler ve tartışmalar, katılımcıların materyali öğrenmelerine yardımcı olmak açısından etkili miydi?
- Sonuçlar modülün öğrenme hedefleriyle uyumlu mu?

5.4.3 Materyaller, Ek Kaynaklar

Ek 1 | Buz kırıcı etkinlik: Sosyal medya Bingo

Sosyal Medya Bingo Kartı – A

Beğen	**Yorum**	**Facebook**	**Hikaye**	**Hashtag**
Selfie	Mesaj	Instagram	Etiket	Profil
Emoji	Takipçi	ÜCRETSİZ	Tweet	Paylaş
Video	Gizlilik	LinkedIn	Durum	Gönderi
Zaman Çizelgesi	Bildirim	Twitter	Grup	Reels

Sosyal Medya Bingo Kartı – B

Etiket	**Gönderi**	**Instagram**	**Hikaye**	**Gizlilik**
Mesaj	Facebook	Zaman Çizelgesi	Beğen	Grup
Reels	Hashtag	ÜCRETSİZ	Durum	Yorum
Tweet	Paylaş	LinkedIn	Video	Selfie
Takipçi	Bildirim	Profil	Emoji	Engelle

Sosyal Medya Bingo Kartı – C

Durum	**Beğen**	**LinkedIn**	**Selfie**	**Paylaş**
Facebook	Emoji	Instagram	Tweet	Reels
Mesaj	Gizlilik	ÜCRETSİZ	Grup	Hikaye
Zaman Çizelgesi	Etiket	Bildirim	Gönderi	Hashtag
Engelle	Takipçi	Video	Yorum	Profil

Ek 2 I Ders 1: Sosyal medyaya genel bakış

Sunum slaytları:

- **Facebook:** "Arkadaşlarınız ve ailenizle iletişimde kalmak için en yaygın kullanılan platformdur. Fotoğraf paylaşabilir, güncellemelere yorum yapabilir, ilgi gruplarına katılabilir ve daha fazlasını yapabilirsiniz."
- **Instagram:** "Bu platform, resim ve videolara odaklanmaktadır. 24 saat sonra kaybolan 'Hikayeler' gibi özellikleri kullanarak anları görsel olarak paylaşmak için harikadır."
- **LinkedIn:** "Bunu çevrimiçi profesyonel özgeçmişiniz olarak düşünün. İş arama ve ağ oluşturma için kullanışlıdır, ancak hala aktif olarak çalışanlar dışında yaşlılar arasında yaygın olarak kullanılmaz."
- **Twitter:** "Burada kullanıcılar tweet adı verilen kısa metin mesajları yayınlar. Çoğunlukla haberleri ve ünlü kişileri takip etmek için kullanılır."

Sosyal Medya Platformları Karşılaştırması

Kategori	Facebook	Instagram	LinkedIn	Twitter	Twitter (çift sütun)
Amaç	Arkadaşlar ve aileyle bağlantı kurmak	Fotoğraf ve kısa videolar paylaşmak	Profesyonel ağ oluşturma	Kısa güncellemeler paylaşmak	Kısa güncellemeleri paylaşmak
Gönderi türleri	Metin, fotoğraflar, videolar, bağlantılar, hikayeler	Fotoğraflar, videolar, makaralar, hikayeler	İş güncellemeleri, makaleler, özgeçmişler	Tweetler (metin), fotoğraflar, videolar	Herkese açık, takipçiler
Yorumlar ve tepkiler	Arkadaşlar, gruplar, herkese açık	Takipçiler, herkese açık	Profesyonel bağlantılar	Beğeniler, yorumlar	Beğeniler, yorumlar
Mesajlaşma	Mesajlaşma uygulaması	Beğeniler, yorumlar	Beğeniler, yorumlar	Beğeniler, yorumlar, retweetler	Beğeniler, retweetler
Gizlilik Ayarları	Özelleştirilebilir: herkese açık, arkadaşlar, gruplar	Sınırlı, özel olmadığı sürece çoğunlukla herkese açık	Varsayılan olarak daha fazla herkese açık	Çoğunlukla herkese açık, sınırlı kontrol	Varsayılan olarak herkese açık isim ve gönderiler
Profil Görünürlüğü	Ayarlanabilir: isim, fotoğraflar, biyografi	Özel hesap olmadığı sürece sınırlı kontrol	Varsayılan olarak ayarlanmadıkça herkese açık	Varsayılan olarak herkese açık isim ve ayarlanmış	Varsayılan olarak herkese açık isim ve gönderiler
Yaygın Riskler	Sahte hesaplar, aşırı paylaşım, dolandırıcılık	DM'lerde dolandırıcılık, kimlik hırsızlığı	Kimlik hırsızlığı mesajları, kimlik sahtekarlığı	Taciz, sahte bağlantılar, kimlik hırsızlığı	Taciz, sahte bağlantılar, kimlik hırsızlığı
Şunlar için uygun	✓	✓	✓	✓	✓

Ek 3 | Etkinlik 1: Platforma Aşina Olma

Eğitmen gruba adım adım rehberlik eder:

"İnternet tarayıcınızı açın ve www.facebook.com veya www.instagram.com adresine gidin."
"Yeni hesap oluştur" seçeneğine tıklayın ve bilgilerinizi girin — ad, doğum tarihi vb.
"Şifre seçmeniz istendiğinde, şifrenizin güçlü olduğundan emin olun. İyi bir şifre en az 8 karakterden oluşur, harf ve rakamların karışımını kullanır ve bir sembol içerir."

Eğitmen ekler:

"Örneğin, 'maria123' yerine 'Maria!74books' kullanabilirsiniz."
"Şimdi iki faktörlü kimlik doğrulamayı etkinleştirelim — İki Faktörlü Kimlik Doğrulama (2FA) ekstra bir güvenlik katmanı ekler. Şifrenizi girdikten sonra, cep telefonunuza veya e-postanıza gönderilen bir kod istenecektir."

Ek 4 | Hesap Kurulum Kontrol Listesi, Hesap Kurulum Kontrol Listesi

1. Bir platform seçin (Facebook, Instagram vb.)
2. Resmi web sitesine gidin veya resmi uygulamayı indirin.
3. "Yeni hesap oluştur" seçeneğine tıklayın.
4. Gerçek adınızı ve doğum tarihinizi girin.
5. Güçlü ve benzersiz bir şifre kullanın (bkz. El Broşürü 2).
6. Cep telefonu numaranızı veya e-posta adresinizi girin.
7. İki faktörlü kimlik doğrulamayı etkinleştirin.
8. Gereksiz kişisel bilgileri (adresiniz gibi) atlayın.
9. Hesabı oluşturduktan hemen sonra gizlilik ayarlarınızı gözden geçirin.
10. Halka açık veya paylaşılan bir cihaz kullanırken oturumu kapatın.

Hesap Kurulum Kontrol Listesi

Güçlü bir şifre:

- En az 8 karakter uzunluğunda olmalıdır.
- Büyük ve küçük harflerin karışımını içermelidir.
- En az bir rakam ve bir özel karakter (ör. !, @, #, $) içermelidir.
- Yaygın kelimeler veya kolayca tahmin edilebilir bilgiler (adınız veya doğum tarihiniz gibi) kullanmaktan kaçınmalıdır.
- Oluşturduğunuz her hesap için benzersiz olmalıdır.

Zayıf şifre örneği: maria123
Güçlü şifre örneği: M@r!a74Books

Ek 5 | Ders 2: Gizlilik Ayarları

Sosyal Medya Gizlilik Kontrol Listesi

[ ] Profil görünürlük ayarlarınızı gözden geçirdiniz mi?

[ ] Gönderileriniz yalnızca "Arkadaşlar" veya "Takipçiler" ile sınırlı mı?

[ ] Tüm platformlarda iki faktörlü kimlik doğrulamayı etkinleştirdiniz mi?

[ ] Telefon numaranızı, ev adresinizi veya tam doğum tarihinizi paylaşmaktan kaçınıyor musunuz?

[ ] Size mesaj veya arkadaşlık isteği gönderebilecek kişileri kontrol ettiniz mi?

[ ] Etiketlendiğiniz fotoğrafları ve gönderileri profilinizde görünmeden önce inceliyor musunuz?

[ ] Yeni arkadaş veya takipçi isteklerini kabul ederken dikkatli misiniz?

[ ] Hassas bilgiler içeren eski gönderileri sildiniz mi?

[ ] Gizlilik ayarlarınızı düzenli olarak kontrol ediyor musunuz?

[ ] Her platformda dolandırıcılık ve kötüye kullanımı nereye bildireceğinizi biliyor musunuz?

Gizlilik Ayarları Kılavuzu

Popüler platformlarda gizlilik ayarlarınızı değiştirmek için bağlantılar ve adımlar:

1. Facebook:

- Gizlilik Kontrol Aracına gidin: https://www.facebook.com/privacy/checkup
- Gizlilik Merkezi: https://www.facebook.com/privacy/center
- Gönderilerinizi kimlerin görebileceğini, kimlerin size arkadaşlık isteği gönderebileceğini ve kimlerin sizi arayabileceğini ayarlayın.

2. Instagram:

- Güvenlik Merkezi'ne gidin: https://help.instagram.com/196883487377501
- Instagram Hesabınızı Özel Olarak Ayarlamak: https://help.instagram.com/448523408565555
- Hesabınızı özel olarak ayarlayın, yorumları yönetin ve etiketleri kontrol edin.

3. LinkedIn:

- Gizlilik Ayarları Genel Bakış'a gidin: https://www.linkedin.com/help/linkedin/answer/66
- LinkedIn Genel Profil Ayarlarınızı Yönetin: https://www.linkedin.com/help/linkedin/answer/83
- Bağlantılarınızı, profil ayrıntılarınızı ve etkinliklerinizi kimlerin görebileceğini seçin.

4. Twitter (X):

- Güvenlik Ayarları'na gidin: https://help.twitter.com/en/safety-and-security/twitter-privacy-settings
- Güvenlik ve Hesap Erişimi: https://help.twitter.com/en/managing-your-account/accessing-your-twitter-data
- Tweetlerinizi koruyun, size mesaj gönderebilecek veya sizi etiketleyebilecek kişileri sınırlayın ve bulunabilirliğinizi kontrol edin.

Ek 6 | Etkinlik 2: Gizlilik Ayarlarını Düzenleme

Gizlilik Ayarlama Çalışma Sayfası

Bu çalışma sayfasını, sosyal medya gizlilik ayarlarınızda yaptığınız değişiklikleri takip etmek için kullanın. Hesabınızı inceledikten sonra, yaptığınız değişikliklerin ayrıntılarını ve nedenlerini aşağıya yazın.

1.

Ayarlanan Ayar _____

Yeni Değer/Seçenek _____

Değişiklik Nedeni _____

2.

Ayar Değişikliği _____

Yeni Değer/Seçenek _____

Değişiklik Nedeni _____

3.

Ayarlandı _____

Yeni Değer/Seçenek _____

Değişiklik Nedeni _____

4.

Ayarlandı _____

Yeni Değer/Seçenek _____

Değişiklik Nedeni _____

5.

Ayarlandı _____

Yeni Değer/Seçenek _____

Değişiklik Nedeni _____

Ek 7| Ders 3: Sosyal medyada dolandırıcılık ve çevrimiçi tehditleri tanıma

En yaygın dolandırıcılıkların temel özellikleri:

- **Kimlik avı:** *"Bunlar, kişisel bilgilerinizi vermeniz için sizi kandırmaya çalışan sahte mesajlardır. Örneğin, 'Bir ödül kazandınız! Ödülü almak için buraya tıklayın' diyen bir mesaj."*
- **Sahte Arkadaşlık İstekleri:** *"Kuzeniniz veya komşunuz gibi davranan birinden istek alabilirsiniz — her zaman iki kez kontrol edin."*
- **Şüpheli Bağlantılar:** "*Bunlar cihazınıza virüs bulaştırabilir veya şifrelerinizi çalabilir. Bağlantı garip görünüyorsa veya beklemediğiniz bir bağlantıysa, tıklamayın."*
- **Kimlik Sahtekarlığı ve Romantik Dolandırıcılık:** *"Bazı kişiler, daha sonra para istemek için arkadaşlık veya romantik bir sohbet başlatabilir."*
- **Sahte Kimlikler***: "Dolandırıcılar, güven oluşturmak ve kurbanları para veya kişisel bilgilerini vermeye ikna etmek için çevrimiçi sahte profiller oluşturur."*

Ek 8| Dolandırıcılık Tanıma Kılavuzu

Sosyal medyada yaygın dolandırıcılık yöntemlerini nasıl tespit edeceğinizi öğrenin:

1. Kimlik Avı Mesajları:

- "Hesabınız kilitlenecek!" gibi acil talepler arayın.
- Gönderenin e-posta adresini veya kullanıcı adını kontrol edin — şüpheli görünüyor mu?

2. Sahte Arkadaşlık İstekleri:

- Tanımadığınız kişilere karşı dikkatli olun.
- Tanıdığınız biri gibi davranan sahte profillere dikkat edin.

3. Ödül veya Piyango Dolandırıcılığı:

- "Kazandınız!" mesajları neredeyse her zaman dolandırıcılıktır.
- Asla banka bilgilerinizi vermeyin veya ödülü almak için ödeme yapmayın.

4. Romantik veya Arkadaşlık Dolandırıcılığı:

- Dolandırıcılar güveninizi kazanıp sonra para isteyebilir.
- Birisi çok hızlı bir şekilde çok kişisel davranırsa dikkatli olun.

5. Şüpheli Bağlantılar:

- Bilinmeyen bağlantılara, özellikle özel mesajlarla gönderilenlere tıklamayın.
- Şüpheli etkinlikleri her zaman iki kez kontrol edin ve bildirin.

Ek 9| Sosyal Medya Güvenlik İpuçları

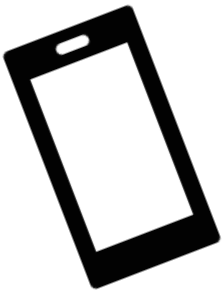
Sosyal medyada güvende kalmak için şu önemli ipuçlarını izleyin:

- Profilinizi özel olarak ayarlayın ve gönderilerinizi kimlerin görebileceğini kontrol edin.
- Her hesap için güçlü ve benzersiz şifreler kullanın.
- Ekstra güvenlik için iki faktörlü kimlik doğrulamayı etkinleştirin.
- Yabancılardan gelen arkadaşlık isteklerini kabul etmeyin.
- Paylaştıklarınıza dikkat edin – seyahat planlarınızı veya kişisel bilgilerinizi paylaşmaktan kaçının.
- Halka açık veya paylaşılan cihazları kullanırken oturumu kapatın.
- Dolandırıcılık ve sahte hesaplar dahil olmak üzere şüpheli her şeyi bildirin.
- Yeni tehditlerden korunmak için uygulamalarınızı güncel tutun.
- Bağlantılara tıklamadan veya dosya indirmeden önce düşünün.
- Şüpheniz varsa, güvendiğiniz birine danışın veya sorunu bildirin.

Bilgi sahibi olun. Güvende kalın.

Ek 10 | Etkinlik 3: Dolandırıcılık Tanıma Alıştırması

Senaryo 1: Kazandınız!



Bilinmeyen bir hesaptan şu mesajı aldınız:
"Tebrikler! Yeni bir akıllı telefon kazandınız! Ödülünüzü almak için aşağıdaki linke tıklayın."
Mesajda bir bağlantı bulunmakta ve kişisel bilgilerinizi girmeniz istenmektedir.

Senaryo 2: Başı Dertte Olan Arkadaş

Facebook Messenger'da uzun süredir konuşmadığınız bir arkadaşınızdan bir mesaj alırsınız. Yurtdışında mahsur kaldıklarını ve hemen 500 EUR göndermenizi istediklerini söylerler. Telefon numaranızı ve banka bilgilerinizi istiyor.

Senaryo 3: Banka Uyarısı

Bankanız olduğunu iddia eden bir hesap Instagram'da doğrudan mesaj gönderir:
"Hesabınızda şüpheli bir hareket tespit ettik. Lütfen buradan yanıt vererek giriş bilgilerinizi hemen onaylayın."
Hesap profilinde banka logosu resmi var.

Senaryo 4: İş Fırsatı

LinkedIn'de, işe alım uzmanı olduğunu iddia eden birinden bağlantı isteği alırsınız. Size yüksek maaşlı ve esnek çalışma saatleri olan bir uzaktan çalışma işi teklif ederler.
Kabul ettikten sonra, özgeçmişinizi, kimlik fotoğrafınızı ve sosyal güvenlik numaranızı ister.

Senaryo 5: Yerel Topluluk Grubu

Yerel yaşlılar için bir Facebook grubuna katılmaya davet ediliyorsunuz. Grup, sağlık ipuçları, etkinlik güncellemeleri ve topluluk haberlerini paylaşıyor. Üyeler dost canlısı ve kimse kişisel verilerinizi istemiyor.

Ek 11 | Ders 4: Sosyal medyada güvenli ve sorumlu bir şekilde etkileşim kurma

Güvenli Paylaşım Kuralları

Sosyal medyada sorumlu bir şekilde paylaşım yapmak için aşağıdaki kuralları kullanın:

- Paylaşmadan önce düşünün: Bir yabancının bunu görmesi sizin için sorun olur mu?
- Özellikle gerçek zamanlı olarak tam konumunuzu paylaşmaktan kaçının.
- Uzun seyahatlerinizi veya evinizin ne zaman boş kalacağını duyurmayın.
- Kimlik, bilet veya banka bilgileri gibi kişisel belgeleri asla paylaşmayın.
- Çocukların fotoğraflarını paylaşırken dikkatli olun; gerektiğinde izin alın.
- Gizlilik ayarlarını kullanarak paylaşımlarınızı kimlerin görebileceğini kontrol edin.
- Hassas konuları herkese açık paylaşımlarda paylaşmaktan kaçının.
- Duygusal olduğunuzda içerik paylaşmayın – önce durun ve düşünün.
- Kişisel konuşmalar için herkese açık yorumlar yerine özel mesajları kullanın.
- Geçmiş gönderilerinizi düzenli olarak gözden geçirin ve güvensiz olduğunu düşündüğünüz her şeyi silin.

Unutmayın: Bir şey bir kez çevrimiçi hale geldiğinde, geri almak zordur.

Ek 12 | Etkinlik 4: Geçmiş Gönderileri ve Bilgileri Gözden Geçirme

Eğitmen şöyle der:
"Şimdi sosyal medya hesaplarınıza girip geçmiş gönderilerinizi veya fotoğraflarınızı inceleyeceğiz. Buna 'Dijital Temizlik' egzersizi denir."

Eğitmen adımları yönlendirir:

- *"Profilinize veya zaman çizelgenize gidin."*
- *"3-5 eski gönderiyi inceleyin. Kendinize sorun: Bu, bugün paylaşmak isteyeceğim bir şey mi? Özel bilgileri ortaya çıkarıyor mu?"*
- *"Eğer evet ise, silelim veya düzenleyelim. Nasıl yapılacağını göstereceğim."*

Eğitmen ekranda veya projektörde gösterir:

- *Facebook gönderisini silme*
- *Fotoğraflardan kendinizi etiketlemekten nasıl çıkarılır*
- *Görünürlüğü "Herkese Açık"tan "Arkadaşlar"a nasıl değiştirilir*

Ek 13 | Profil Güvenliği Kontrol Listesi

Bu kontrol listesini kullanarak sosyal medya profilinizin güvenliğini gözden geçirin:

[ ] Profil resminiz uygun ve kimliğinizi ifşa etmiyor mu (arka planda ev adresi gibi kişisel bilgiler yok mu)?

[ ] Profilinizden doğum tarihinizi, telefon numaranızı veya ev adresinizi kaldırdınız mı veya gizlediniz mi?

[ ] Gönderileriniz "Herkese Açık" yerine "Sadece Arkadaşlar" veya "Özel" olarak ayarlanmış mı?

[ ] Gönderilerinize kimlerin yorum yapabileceğini veya paylaşabileceğini gözden geçirdiniz mi?

[ ] Size arkadaşlık/takip istekleri gönderebilecek kişileri kontrol ettiniz mi?

[ ] Hesabınız için güçlü ve benzersiz bir şifre kullanıyor musunuz?

[ ] İki faktörlü kimlik doğrulama etkin mi?

[ ] Gönderileri düzenli olarak gözden geçirip, güncel olmayan veya güvenli olmayanları siliyor musunuz?

[ ] Gönderilerinizde konum paylaşımını kapattınız mı?

[ ] Zaman akışında görünmeden önce etiketlendiğiniz gönderileri inceliyor musunuz?

Profilinizin güvenliğini sağlamak için bu kontrol listesini birkaç ayda bir doldurun.

Ek 14 | Sosyal Medya Güvenliği Kontrol Listesi

[ ] Her hesap için güçlü ve benzersiz şifreler kullanın

[ ] İki faktörlü kimlik doğrulamayı etkinleştirin

[ ] Gizlilik ayarlarını düzenli olarak inceleyin ve ayarlayın

[ ] Halka açık olarak paylaştığınız kişisel bilgilere dikkat edin

[ ] Arkadaşlık veya takip isteklerini kabul etmeden önce düşünün

[ ] Dolandırıcılık, kimlik avı ve şüpheli mesajlara karşı dikkatli olun

[ ] Bağlantılara tıklarken veya içerik indirirken dikkatli olun

[ ] Şüpheli veya taciz edici kullanıcıları bildirin ve engelleyin

[ ] Konum paylaşımını ve coğrafi etiketlemeyi sınırlayın

[ ] Uygulamalarınızı ve cihazlarınızı güncel tutun

Ek 15| Katılımcılar için daha fazla okuma ve öğrenme önerileri

Siber güvenlik web siteleri: Siber güvenlikle ilgilenen Avrupa ve hükümet kuruluşları

1) **ENISA (Avrupa Birliği Siber Güvenlik Ajansı)**

   Web sitesi: https://www.enisa.europa.eu/

   ENISA, siber güvenlikten sorumlu AB ajansıdır. Siber tehditler hakkında raporlar, kılavuzlar ve uyarılar yayınlar ve vatandaşlara ve kuruluşlara pratik tavsiyelerde bulunur.

2) **CERT-EU (AB Kurumları için Bilgisayar Acil Durum Müdahale Ekibi)**

   Web sitesi: https://cert.europa.eu/

   CERT-EU, siber tehditleri izler ve Avrupa kurumlarını hedef alan siber saldırılara müdahale eder. Ayrıca, eğitmenler ve son kullanıcılar tarafından uygulanabilecek uyarılar ve en iyi uygulamalar sunar.

3) **EC3 – Europol Siber Suç Merkezi**

   Web sitesi: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

   Europol'un EC3'ü, çevrimiçi dolandırıcılık, sahtekarlık ve diğer siber suç türleri hakkında bilgi sağlar. Sosyal medyada riskleri belirlemeye yönelik farkındalık materyalleri ve vaka çalışmaları yayınlar.

4) **Çevrimiçi Güvenliğinizi Koruyun – Ulusal Siber Güvenlik İttifakı (ABD)**

   Web sitesi: https://staysafeonline.org/

   Gizlilik, şifre güvenliği, kimlik avı ve sosyal medya farkındalığı konusunda basit kontrol listeleri ve kampanyalar içeren bir kaynak merkezi.

5) **AARP Dolandırıcılık İzleme Ağı**

   Web sitesi: https://www.aarp.org/money/scams-fraud/

   Özellikle yaşlıları hedef alan dolandırıcılıklarla ilgili güncel bilgiler içeren, önleme ipuçları ve bildirim tavsiyeleri sunan, erişilebilir bir ABD merkezli girişim.

6) NCSC UK – Sosyal Medya Rehberi

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

7) NCSC UK – Şifre Rehberi

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

8) LinkedIn Yardımı – Gizlilik Ayarları

   Web sitesi: https://www.linkedin.com/help/linkedin/answer/66

5.5 Modül IV – Ön/Son Test

1. "Kişisel veriler" neleri içerir?

A) Yalnızca sosyal medya paylaşımlarınız
B) Adınız veya kimlik numaranız gibi sizi tanımlayabilecek her türlü bilgi
C) Yalnızca banka hesap bilgileriniz
D) Yalnızca çevrimiçi şifreleriniz

2. Gizlilik politikalarını okumak neden önemlidir?

A) Veri güvenliği ile ilgili şakalar içerirler
B) Verilerinizin nasıl toplanacağı ve kullanılacağı açıklanır
C) Cihazınızın daha hızlı çalışmasına yardımcı olurlar
D) Yasal olarak zorunludur ancak önemsizdir

3. Aşağıdakilerden hangisi hassas kişisel verilere bir örnektir?

A) En sevdiğiniz renk
B) Ev adresi
C) Tıbbi geçmiş veya biyometrik veriler
D) Alışveriş tercihleri

4. Çevrimiçi olarak fotoğraf veya bilgi paylaşırken en iyi uygulama nedir?

A) Açık ve sosyal olmak için tüm kişisel bilgileri paylaşmak
B) Yayınlamadan önce bilgileri kimlerin görebileceğini kontrol etmek
C) Görünür kalmak için sık sık paylaşım yapın
D) Her zaman konumunuzu ekleyin

5. "Veri şifreleme" ne anlama gelir?

A) Dosyaları gizli bir klasörde saklamak
B) Bilgileri yetkisiz erişimden korumak için bir koda dönüştürmek
C) Dosyalarınızı bir flash sürücüye kaydetmek
D) Tüm eski verileri silmek

6. Sosyal medyada paylaşılan bilgi miktarını neden sınırlamalısınız?

A) İnternet verilerini korur
B) Kimlik hırsızlığı ve dolandırıcılık riskini azaltır
C) Takipçi sayısını artırır
D) Başkalarının yorum yapmasını engeller

7. Bir uygulamaya kişisel bilgilerinize erişim izni vermeden önce ne yapmalısınız?

A) Uygulamayı daha hızlı kullanmak için hemen kabul edin
B) İzinleri dikkatlice okuyun ve sadece gerekli olanlara izin verin
C) Uygulama hatalarını önlemek için tüm izinleri verin
D) Uygulamayı hemen kaldırın

8. Genel Veri Koruma Yönetmeliği'nin (GDPR) amacı nedir?

A) Şirketlerin daha fazla veri toplamasına yardımcı olmak
B) Bireylerin kişisel verilerini ve gizlilik haklarını korumak
C) İnsanların sosyal medyayı kullanmasını engellemek
D) Çevrimiçi alışveriş faaliyetlerini kontrol etmek

9. Aşağıdaki eylemlerden hangisi, paylaşılan bir bilgisayarda verilerinizin korunmasına yardımcı olur?

A) Kolaylık olması için oturum açık kalmak
B) Kullanımdan sonra oturumu kapatmak ve tarayıcı geçmişini temizlemek
C) Tarayıcıların şifrelerinizi kaydetmesine izin vermek
D) Oturum açma bilgilerinizi aile üyelerinizle paylaşmak

10. Kişisel verilerinizin çalındığından şüpheleniyorsanız ne yapmalısınız?

A) Görmezden gelin ve kendiliğinden çözülmesini umun
B) Sosyal medyada paylaşmak
C) İlgili makamlara bildirin ve şifrelerinizi hemen değiştirin
D) Para çalınmadıkça hiçbir şey yapmayın

Cevap Anahtarı Özeti

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

MODÜL V

Yaşlıların Güvenli Dijitalleşmesi

6. Modül V - Yaşlıların Güvenli Dijitalleşmesi

Modül 5, eğitimcilere yaşlıların dijital teknolojileri güvenli bir şekilde kullanmalarını etkili bir şekilde desteklemek için gerekli bilgi, araç ve çalışma yöntemlerini kazandırmaya odaklanmaktadır. Modül, katılımcılara yaşlıların özellikle internet uygulamaları, e-posta hizmetleri, sosyal medya platformları ve çevrimiçi bankacılık araçlarının kullanımıyla ilgili özel özelliklerini ve öğrenme ihtiyaçlarını tanıtmaktadır.

Siber güvenliğe büyük önem verilmekte ve dolandırıcılık, sahtekarlık ve dezenformasyon risklerinin en aza indirilmesine özel dikkat gösterilmektedir. Katılımcılar, yaşlıların karşılaştığı yaygın çevrimiçi tehditleri inceler ve bu riskleri önleyici stratejiler, açık iletişim ve bu yaş grubuna özel pratik rehberlik yoluyla nasıl ele alacaklarını öğrenirler.

Ayrıca, Modül 5, öğretim araçlarını uygulamalı alıştırmalarla birleştirerek yaşlıların dijitalleşmesi için kapsamlı eğitim desteği sağlar. Katılımcılar, bilgileri etkili ve empatik bir şekilde aktarma, siber güvenlikle ilgili zorluklara yanıt verme ve hem bireysel koçluk seansları hem de grup temelli eğitim faaliyetleri için erişilebilir ve destekleyici öğrenme ortamları tasarlama becerilerini geliştirirler.

6.1 Öğrenim Hedefleri

Bu modülün amacı, katılımcıların yaşlılara dijital teknolojileri güvenli bir şekilde kullanmayı etkili bir şekilde öğretmek ve siber güvenlikle ilgili zorluklarla başa çıkmalarında onlara destek olmak için gerekli eğitim ve pratik becerileri edinmelerini sağlamaktır.

- Dijitalleşme konusunda yaşlıların özel ihtiyaçlarını anlamak.
- Yaşlılara özel öğretim yöntemlerini öğrenmek.
- Yaşlıları hedef alan tipik siber tehditleri belirleme ve bunlara yanıt verme becerilerini kazanmak.

6.2 Yapı, İçerik ve Öğrenim Çıktıları

Bu modülü başarıyla tamamlayan öğrenciler şunları yapabileceklerdir:

- Yaşlıların teknoloji öğrenimindeki engelleri (psikolojik, bilişsel ve teknik) anlamak, tekrar, küçük adımlarla alıştırmalar ve basit açıklamalar gibi pratik ve erişilebilir öğretim yöntemlerini kullanmak.
- Güvenli oturum açma kurallarını iletme, güvenli siteleri tanıma ve kişisel verileri koruma yöntemlerini öğrenmek, yaşlıların çevrimiçi hizmetleri bağımsız ve güvenli bir şekilde kullanmalarını desteklemek.
- Yaşlıların özellikle maruz kaldığı en yaygın tehditleri öğrenin ve bu bilgileri basit bir şekilde aktararak yaşlıların dikkatini artırmayı öğrenin.
- Egzersizler ve durum senaryoları aracılığıyla yaşlıların çevrimiçi tehditleri tanımalarını ve güvenli alışkanlıklar geliştirmelerini nasıl destekleyeceğinizi öğrenin.
- Tehdit durumunda ne gibi önlemler alınması gerektiğini öğrenin, örneğin şifreleri hemen değiştirmek veya cihazı ağ bağlantısını kesmek gibi, tehdit durumunda hangi verilerin korunmasının önemli olduğunu anlayın.
- Siber tehdit olaylarını bildirme prosedürlerini öğrenin, örneğin bankanızla, polisle veya uzman kuruluşlarla iletişime geçme, siber suç mağdurları için hangi destek kaynaklarının mevcut olduğu.

- ❖ Anlık mesajlaşma, e-posta ve görüntülü görüşme uygulamalarında güvenlik kurallarının yöntemlerini ve çevrimiçi tehditleri fark etme alıştırmalarının nasıl yapılacağını açıklayın.
- ❖ Cihazları virüslerden koruma konusunda bilgi sağlamak ve sistemleri erişilebilir ve anlaşılır bir şekilde güncellemek için adım adım öğrenme.

6.3 Gündem I Ayrıntılı Oturum Planı

MODÜL V
Yaşlıların güvenli dijitalleşmesi

1. Oturum

Hoş geldiniz
Süre 5

Öğrenim Hedefleri

- ❖ Aktif katılımı teşvik eden açık ve ilgi çekici bir atmosfer yaratmak.

İçerik/ Yöntem

- ❖ Katılımcıların karşılanması, eğitmenin kısa tanıtımı. Eğitmen, eğitim planını ve çalışma kurallarını sunar.

Malzeme
Ek materyal gerekmez.

Yorum
Atölyenin amacını basit bir dille açıklamak faydalı olabilir.

2. Oturum

Buz kırıcı etkinlik
Süre 15

Öğrenme Hedefleri

- ❖ Katılımcılar arasında dostane bir ilişki kurmak, birbirlerini tanımak ve asıl bölüm başlamadan önce grubu harekete geçirmek.

İçerik/ Yöntem

- ❖ Tartışmayı başlatacak kısa bir harekete geçirme egzersizi: "Yaşlılara yeni teknolojileri öğretirken hangi zorluklarla karşılaşıyorlar? Bunlarla nasıl başa çıkıyorlar?" Eğitmen, tartışmanın gidişatını etkileyecek destekleyici sorular ekleyebilir: Sizi şaşırtan ne oldu? En etkili yöntemler hangileri oldu? Derslerin hızı veya şekli katılımcıların bireysel ihtiyaçlarına göre nasıl ayarlanabilir? Her katılımcı bir zorluk sunabilir.

Malzeme
Ek materyal gerekmez.

Yorum
En yaygın zorlukları belirlemek için katılımcıların cevaplarını beyaz tahtaya veya flipchart'a yazmak yararlıdır.

3. Oturum

Ders 1: Yaşlılara siber güvenlik ve yeni teknolojiler hakkında eğitim vermeye yönelik pratik ipuçları
Süre *25*

Öğrenim Hedefleri

- Eğitimcilerin, yaşlıların yeni teknolojileri öğrenirken karşılaştıkları engeller konusunda farkındalıklarını artırmak ve öğrenme sürecini desteklemek için etkili öğretim araçlarıyla donatmak.
- Eğitimcilere, yaşlılara internet uygulamalarının güvenli kullanım ilkelerini öğretmek, güvenlik duygularını ve dijital yetkinliklerini güçlendirmek için bilgi ve yöntemler sağlamak.

İçerik/Yöntem

- Ders iki tematik alana ayrılmıştır:

Konu 1: Siber güvenlik ve yeni teknolojiler alanında yaşlılara etkili öğretim yöntemleri
<u>İçerik/Yöntemler:</u>

- Psikolojik engellerin (ör. teknolojiden korkma, düşük özgüven), bilişsel engellerin (ör. bilginin daha yavaş işlenmesi, konsantre olma zorluğu) ve teknik engellerin (cihazlarla ilgili deneyim eksikliği) belirlenmesi.
- Yaşlılarla dostane iletişim ilkelerinin tartışılması.

<u>Materyal:</u>
Eğitimciler için öğretim yardımı: Yaşlılara öğretim için pratik yöntemler – eğitimciler için alıştırma materyali (Ek 1)

Konu 2: Eğitimcileri, yaşlılara internet uygulamalarının (bankacılık, alışveriş, sosyal ağ siteleri) güvenli kullanım ilkelerini öğretmeye hazırlamak
<u>İçerik / Yöntemler:</u>

- Yaşlılar tarafından kullanılan popüler internet uygulamalarının gözden geçirilmesi.
- Güvenli web sitelerini ve uygulamaları tanıma (sertifikalar, URL'ler, giriş formlarının görünümü).
- Güvenli şifreler oluşturma ve giriş verilerini saklama ilkelerinin tartışılması.
- Hayali hesaplar üzerinde pratik alıştırmalar: oturum açma, sitenin güvenliğini kontrol etme, simüle edilmiş çevrimiçi alışveriş.

Materyal:
Eğitimciler için öğretim yardımı: Pratik alıştırmalar – eğitimcilere yaşlılar için siber güvenlik ilkelerini öğretme (Ek 2)

Yorum
En yaygın zorlukları belirlemek için katılımcıların cevaplarını beyaz tahtaya veya flipchart'a yazmak yararlıdır.

Etkinlik 1: Yaşlıların öğrenme engellerini belirleme
Süre 15

Öğrenme Hedefleri

- Yaşlıların öğrenme süreci hakkında farkındalığı artırmak.
- Yaşlıların öğrenme engellerini tanımak.

İçerik/Yöntem

- Alıştırma, katılımcıların tercihlerine bağlı olarak bireysel olarak veya çiftler halinde yapılır.
- Katılımcılara, yaşlıların öğrenme sürecinde karşılaşabilecekleri olası engelleri düşünmelerini içeren bir görev içeren çalışma kağıtları (Ek 3) verilir.
- Katılımcılar, yaşlıların öğrenme sürecinde ortaya çıkabilecek psikolojik, bilişsel ve teknik engellerin örneklerini belirlemelidir.
- Ardından, bu engellerin her birini aşmak için yöntemler önerir ve bunların yaşlıların öğrenme sürecini nasıl etkileyebileceğini açıklarlar.
- Alıştırma, liderin moderatörlüğünde yapılan ve katılımcıların sonuçlarını ve deneyimlerini paylaştıkları bir tartışma ile sona erer.

Materyal

- Çalışma kağıdı – Yaşlıların Öğreniminde Engelleri Belirleme (Ek 3)

Yorum
Katılımcıları tartışmaya aktif olarak katılmaya teşvik etmek faydalı olacaktır.

Ara | Süre *5 dakika*

- **Katılımcıların enerji toplamaları ve düşünmeleri için zaman tanıyın.**
- **Dinlenmek için kısa bir ara.**

4. Oturum

Ders 2: Yaşlılar için siber güvenliğe giriş

Süre *35*

Öğrenim Hedefleri

- ❖ Yaşlıların özellikle maruz kaldığı en yaygın tehditleri tanımak ve bu bilgileri yaşlıların dikkatini çekecek ve internet güvenliğini artıracak şekilde erişilebilir ve etkili bir şekilde aktarmayı öğrenmek.
- ❖ Yaşlıların çevrimiçi tehditleri fark etmelerine nasıl destek olunacağı ve onlara güvenli internet kullanımı alışkanlıkları nasıl kazandırılacağı konusunda bilgi edinmek, böylece dijital farkındalıklarını artırmak.

İçerik/Yöntem

- ❖ Ders iki tematik alana ayrılmıştır:

Konu 1: Yaygın dijital tehditler ve yaşlıların ihtiyaçları

İçerik/Yöntemler:

- Phishing, çevrimiçi dolandırıcılık, veri hırsızlığı, sahte haberler gibi yaygın çevrimiçi tehditlerin tartışılması.
- Yaşlıların daha fazla maruz kaldığı belirli risklerin belirlenmesi.
- Yaşlıları gereksiz korkuya sevk etmeden bu tehditler hakkında etkili bir şekilde bilgilendirmek için ipuçları.
- Yaşlıların karşılaşabileceği çevrimiçi dolandırıcılık örnekleri ve bunları nasıl tanıyabilecekleri.

Materyal:

Eğitimciler için öğretim yardımı: Yaşlılar için güvenli internet kullanımı (Ek 4)

Konu 2: Yaşlılar arasında dijital farkındalık oluşturmak

İçerik/Yöntemler:

- Yaşlıların internette şüpheli durumları fark etmeyi öğrenmelerini destekleyecek yöntemlerin tartışılması.
- Yaşlıların siber güvenlik ilkelerini hatırlamalarına yardımcı olacak alıştırma örnekleri.
- Yaşlıların hata yapabileceği çevrimiçi durumların simülasyonları ve bu hataları önlemeyi öğrenmelerine etkili bir şekilde yardımcı olma yöntemleri.

Materyal:

Eğitimciler için öğretim yardımı: İnternetteki tehditleri tanımak (Ek 5)

Yorum

Katılımcıları, yaşlılarla çalışırken edindikleri deneyimleri ve zor konuları açıklamak için etkili yöntem örneklerini paylaşmaya teşvik edin.

Etkinlik 2: Simülasyon alıştırması: Bir yaşlıyla siber güvenlik hakkında konuşmak
Süre *15*

Öğrenme Hedefleri

- ❖ Eğitimcinin yaşlılarla konuşmasına olanak tanıyarak, çevrimiçi tehditlerden nasıl kaçınacaklarını anlamalarına yardımcı olun.

İçerik/Yöntem

- Görev, katılımcıların eğitimci ve yaşlı rollerini dönüşümlü olarak üstlendikleri ikili gruplar halinde gerçekleştirilir. Alıştırmanın amacı, yaşlıların karşılaşabileceği gerçek durumları dikkate alarak, internetteki tehditler hakkında simüle edilmiş bir eğitim konuşması yapmaktır. Her ikili gruba, belirli bir tehdidi açıklayan bir metin verilir (Ek 6).
- Eğitimcinin rolü, belirli bir tehdidin ne olduğunu, nasıl tanınacağını ve nasıl tepki verileceğini sakin ve anlaşılır bir şekilde açıklamaktır. Yaşlı vatandaşın rolü, dijital bilgisi sınırlı olan ve açık, dostane talimatlara ihtiyaç duyan bir kişinin rolünü üstlenmenizi sağlar. Alıştırma, liderin moderatörlüğünde yapılan ortak bir tartışma ile sona erer. Bu tartışma sırasında katılımcılar, yaşlılarla etkili eğitim iletişimi konusunda duygularını, sonuçlarını ve düşüncelerini paylaşırlar.

Materyal

- ❖ Simülasyon Alıştırması: Bir Yaşlıyla Siber Güvenlik Hakkında Konuşmak (Ek 6)

Yorum
Dilin netliğine dikkat etmek ve teknik jargondan kaçınmak önemlidir.

Ara | Süre *5 dakika*

- ❖ **Dinlenmek ve bir sonraki oturuma hazırlanmak için zaman tanıyın.**
- ❖ **Dinlenmek için kısa bir ara.**

5. Oturum

Ders 3: Siber tehditlere yanıt verme
Süre *30*

Öğrenim Hedefleri

- ❖ Eğitimcileri, yaşlılara dijital tehditler ve bunlardan kaçınma yolları hakkında etkili bir şekilde bilgi verebilecek şekilde hazırlamak.
- ❖ Eğitimcilerin yaşlılara siber tehditlere yanıt verme konusunda ders verme becerilerini geliştirmek.
- ❖ Aktivasyon yöntemleri ve yaşlıların ihtiyaçlarına göre uyarlanmış yöntemlerin kullanımında eğitimcilerin yetkinliklerini güçlendirmek.

İçerik/Yöntem

- Ders iki tematik alana ayrılmıştır:

Konu 1: Siber saldırı şüphesi durumunda atılması gereken adımlar
İçerik/Yöntemler:
Eğitmen şunları tartışır:

- potansiyel bir siber saldırının en yaygın belirtileri (ör. cihazın garip davranışları, şüpheli e-postalar, hata mesajları, ani oturum kapatmalar);
- temel güvenlik kuralları - saldırı şüphesi durumunda nasıl tepki verilmesi gerektiği: ağ bağlantısının derhal kesilmesi, şifrelerin değiştirilmesi, şüpheli eklerin veya bağlantıların açılmaması;
- sakin kalmanın ve aceleci davranışlarda bulunmamanın önemi (ör. bilinmeyen numaraları geri aramamak, kimlik avı uyarılarına tıklamamak);
- güvenli şifreler oluşturma ve bunları güncelleme yöntemleri - doğum günlerini ve basit kombinasyonları kullanmaktan kaçınmak dahil.

Konu 2: Dijital tehditleri nasıl bildirebilirsiniz ve nereden yardım alabilirsiniz?
İçerik/Yöntemler:
Eğitmen şunları tartışır:

- siber tehditleri bildirebileceğiniz kurumlar ve yerler (örneğin CERT Polska, banka yardım hatları, yerel polis, yaşlıları destekleyen kuruluşlar);
- bankayla ne zaman ve nasıl iletişime geçilmesi gerektiği - ör. hesap ele geçirildiğinden veya yetkisiz bir işlem yapıldığından şüphelenildiğinde;
- Bildirim için nasıl hazırlanmalı - tarih, saat, mesajın içeriği yazılmalı, ekran görüntüsü alınmalı, şüpheli mesajlar kaydedilmeli;
- duygusal ve bilgilendirici desteğin rolü - bu desteği nasıl ve nerede arayacağınız (yardım hatları, danışma noktaları, sevdikleriniz);
- kayıp olmasa bile dolandırıcılık girişimini bildirmenin önemi - diğer kullanıcıların iyiliği için.

Materyal

- ❖ Eğitimciler için öğretim yardımı: Senaryo simülasyonları (Ek 7)

Yorum
Katılımcıları tartışmaya katılmaya teşvik etmek faydalı olacaktır.

Etkinlik 3: Dolandırıcılık Tanıma Alıştırması
Süre 20

Öğrenim Hedefleri

- ❖ Yaşlıların çevrimiçi tehdit durumlarında (örneğin dolandırıcılık girişimleri, şüpheli e-postalar, bilinmeyen telefon aramaları) sakin ve soğukkanlı kalmalarına nasıl yardımcı olunacağı konusunda bilgi edinmek.
- ❖ Rasyonel kararlar alma, aceleci davranışlardan kaçınma ve doğru kişi ve kurumlarla iletişime geçme becerisini geliştirmek.

İçerik/Yöntem

- Alıştırma, bir yaşlı ve bir eğitimci arasındaki konuşmanın simülasyonunu gerçekleştirmekten oluşur.
- Katılımcılar çiftler halinde çalışır ve kendilerine verilen rolleri oynarlar: eğitimci ve yaşlı. Katılımcılar, siber tehditler hakkında gerçekçi bir konuşma yapmalarına yardımcı olacak ipuçlarına ve simülasyon konularına (Ek 8) erişebilirler. Simülasyon bittikten sonra, lider tartışmayı yönetir. Her çift, karşılaştıkları zorlukları, duygularını ve etkili iletişim stratejilerini tartışarak düşüncelerini grupla paylaşır. Tartışma, yaşlıların tehditleri fark etmelerine ve bunlara uygun şekilde nasıl tepki vereceklerini öğrenmelerine destek olma yöntemlerini daha iyi anlamaya yardımcı olur.

Materyal

- Simülasyon Alıştırması: Örnek Siber Tehdit Raporları (Ek 8)

Yorum

Eğitimcilerin, yaşlıları dahil etmek ve günlük yaşamlarından örnekler kullanarak onları öğrenmeye aktif olarak katılmaya motive etmek için iyi hazırlanmış olmaları önemlidir.

Ara | Süre 5 dakika

- **Dinlenmek ve hazırlanmak için zaman tanıyın.**
- **Dinlenmek için kısa bir ara.**
- **Dinlenmek ve rahatlamak için kısa bir mola.**

6. Oturum

Ders 4: Yaşlılara elektronik cihazların ve internet uygulamalarının kullanımı konusunda eğitim vermek – eğitimciler için rehber
Süre *20 dakika*

Öğrenim Hedefleri

- Eğitimcilere, yaşlılara e-posta, anlık mesajlaşma (ör. Messenger, WhatsApp) ve görüntülü görüşme uygulamaları (ör. Zoom) gibi iletişim uygulamalarının güvenli kullanım ilkelerini etkili bir şekilde öğretmelerini sağlayacak araçlar ve yöntemler sunmak.
- Eğitimcileri, antivirüs programlarının temel kullanımından işletim sistemi ve uygulamaların güncellenmesini öğrenmeye kadar, yaşlıların dijital cihazlarının korunması konusunda dersler vermeye hazırlamak.

İçerik/Yöntem

- Ders iki tematik alana ayrılmıştır:

Konu 1: Yaşlılara iletişim uygulamalarını güvenli bir şekilde kullanmayı öğretme
<u>İçerik/yöntemler:</u>

- İletişim uygulamalarının temel işlevlerini basit, günlük dilde açıklama yolları.
- Tehlikeli mesajların (spam, phishing) tanınmasını destekleyen alıştırma örnekleri, örneğin gerçek ve sahte e-postaların analizi.

- Uygulamalardaki gizlilik ve güvenlik ayarlarının pratik gösterimleri - bilinmeyen kişileri engelleme, şifreleri değiştirme, gizlilik ayarları.
- Etkinleştirme yöntemleri: kontrol listesi ile çalışma, tehlikeli durumların simülasyonu, sahnelerin ortak çözümü.

Materyal:
Eğitimciler için öğretim yardımı: Yaşlılara iletişim uygulamalarını güvenli bir şekilde kullanmayı öğretme (Ek 9)

Konu 2: Yaşlılara antivirüs ve sistem güncellemelerini kullanmayı öğretme
İçerik / yöntemler:

- Yaşlılara bilgisayar virüsü, güncelleme, sistem taraması kavramlarını anlaşılır bir şekilde nasıl açıklayabiliriz?
- Ücretsiz antivirüs programlarının (ör. Avast, AVG) kurulumu ve kullanımı ile ilgili grup çalışmaları.
- Adım adım: Yaşlılara sistem ve uygulama güncellemelerini nasıl yapacaklarını gösterme.

Materyal:
Eğitimciler için öğretim yardımı: Yaşlılara antivirüs ve sistem güncellemelerini kullanmayı öğretme (Ek 10)

Yorum
Tartışma sırasında, katılımcılar arasında fikir alışverişinin sağlanması önemlidir.

Etkinlik 4: Yaşlılar için pratik tavsiyeler ve teknikler
Süre *30*

Öğrenme Hedefleri

- Yaşlılara interneti güvenli bir şekilde kullanma konusunda basit ve etkili tavsiyelerde bulunma becerisini geliştirmek.
- Yaşlılar için anlaşılır ve erişilebilir öğretim tekniklerini tanıma ve uygulama becerisini geliştirmek.
- Diğer eğitimcilere ilham kaynağı olabilecek, yaşlılarla çalışırken edinilen iyi uygulamaları ve gerçek deneyimleri paylaşmak.

İçerik/Yöntem

- Alıştırma iki aşamadan oluşur: bireysel ve grup çalışması. İlk aşamada, katılımcılar çalışma kağıdını (Ek 11) bağımsız olarak doldururlar ve yaşlılara siber güvenlik konusunda etkili öğretim yöntemleri ile ilgili kendi düşüncelerini, gözlemlerini ve fikirlerini yazarlar. İkinci aşamada, katılımcılar tüm grubun forumunda düşüncelerini paylaşırlar, bu da deneyimlerin paylaşılmasını ve ilham verici çözümler ile kanıtlanmış uygulamaların aranmasını kolaylaştırır. Ortak bir sohbet, bilginin tamamlanmasına, bakış açılarının zenginleştirilmesine ve yaşlılarla eğitim çalışmasının farklı tarzlarının fark edilmesine olanak tanır. Alıştırmanın sonunda, lider konuyu derinleştirmek amacıyla bir tartışma başlatır.

Materyal

- ❖ Çalışma kağıdı: Güvenli İnternet Kullanımı: Yaşlılar için Pratik İpuçları ve Teknikler (Ek 11)

Yorum

Katılımcıları alıştırmayı yaparken soru sormaya teşvik etmek faydalı olacaktır.

7. Oturum

Tartışma | Süre 10 dakika

Öğrenme Hedefleri

- ❖ Katılımcıların oturumdan sonra deneyimlerini ve gözlemlerini paylaşmalarına olanak sağlamak.
- ❖ Yaşlılara eğitim verirken karşılaşılan zorlukları belirlemek.
- ❖ Yaşlı gruplarla çalışmayı iyileştirmek için toplu bir beyin fırtınası oturumu başlatmak.

İçerik/Yöntem

- ❖ Eğitmen, "En zor kısım neydi?", "Hangi alanların daha fazla geliştirilmesi gerekiyor?", "Yaşlılara öğretim nasıl basitleştirilebilir?" gibi sorularla açık bir tartışma başlatır. Katılımcılar, oturumdan edindikleri düşüncelerini, uygulamalarını ve sonuçlarını paylaşır. Sonuçlar, özetlemeyi ve gelecekte kullanmayı kolaylaştırmak için flipchart veya beyaz tahtaya yazılır.

Malzeme

- ❖ Flipchart veya beyaz tahta
- ❖ Marker

Özet | Süre 5 dakika

Öğrenim Hedefleri

- ❖ Önemli bilgileri özetlemek, katılımcıların son sorularını yanıtlamak ve daha fazla öğrenme için kaynakları belirtmek.

İçerik/Yöntem

- ❖ Eğitim sırasında ele alınan en önemli konuların kısa bir özeti.
- ❖ Ek bilgi kaynaklarının belirtilmesi (ör. eğitim web siteleri, video materyalleri).
- ❖ Katılımcılara katılımları için teşekkür etmek ve oturumu kapatmak.

Materyal

- ❖ Eğitimciler için öğretim yardımı: Teknolojinin güvenli kullanımı ile ilgili web siteleri (Ek 12).

Yorum

Sonunda, kısa bir değerlendirme anketi yapmak iyi bir fikirdir.

6.4 Ek Bilgiler

6.4.1 Eğitmenlerin Kendi Kendine Yansıtma

- Katılımcılar için siber güvenlik konusunda anlaması en zor olan şey neydi?
- Eğitim sırasında en etkili yöntemler hangileriydi?
- Alıştırma sırasında katılımcıların deneyimini iyileştirebilecek değişiklikler nelerdir?
- Katılımcılar, yaşlıların öğrenmesiyle ilgili deneyimlerini ve endişelerini rahatça paylaşabildiler mi?

6.4.2 Eğitmenlerin Program Değerlendirmesi

- Eğitim hedeflerine ulaşıldı mı?
- Gelecekte hangi konuların genişletilmesi veya değiştirilmesi gerekiyor?
- Bu katılımcı grubu için en etkili didaktik teknikler hangileriydi?

6.4.3 Materyaller, Ek Kaynaklar

Ek 1 | Yaşlılara Öğretimde Pratik Yöntemler – Eğitimciler için Egzersiz Materyali

Her yöntem için Eğitimci Egzersizlerini tamamlayın (örneğin, kılavuzlar oluşturun, benzetmeler önerin, görseller tasarlayın veya yanıtları açıklayın).

Tekrar ve Adım Adım Egzersizler

- **Yöntem Açıklaması:** Kısa, tekrarlayan talimatlar, her aktivite basit adımlara bölünmüştür.
- **Eğitimci Egzersizi:** Bir sosyal medya platformuna veya çevrimiçi bankacılık sistemine giriş yapmak için adım adım talimat kılavuzu geliştirin (basit ve açık bir dil kullanarak).
- **Amaç:** Görevleri mantıklı ve takip etmesi kolay bir yapı içinde formüle etme becerisini geliştirmek.

Görselleştirme ve Gerçek Hayat Örneklerinin Kullanımı

- **Yöntem Açıklaması:** Soyut teknolojik kavramları yaşlıların günlük deneyimleriyle ilişkilendirmek (örneğin, şifreyi ev anahtarıyla karşılaştırmak).
- **Eğitimci Egzersizi:** Yaşlılara şifre, güvenli web sitesi ve kimlik avı kavramlarını açıklamak için 3 benzetme önerin.
- **Amaç:** Yaşlıların tanıdık durumlara atıfta bulunarak karmaşık kavramları anlamalarına yardımcı olmak.

Büyük Baskı Materyallerinin Kullanımı

- **Yöntem Açıklaması:** Büyütülmüş baskı, yüksek kontrastlı renkler, piktogramlar ve diyagramların kullanılması.
- **Eğitimcinin Alıştırması:** Yaşlılar için güvenli şifre oluşturma ilkelerini içeren görsel yardımcı kart örneği hazırlayın.
- **Amaç:** Yaşlıların görsel ve bilişsel ihtiyaçlarına uygun materyaller oluşturma becerilerini geliştirmek.

Gruba Uygun Hızda Öğretim

- **Yöntem Açıklaması:** Katılımcıların tepkilerini gözlemlemek, kontrol soruları sormak ve derslerin hızında esnekliği korumak.
- **Eğitimcinin Alıştırması:** Grubun yarısı tartışılan bir uygulamanın işlevini anlamazsa nasıl tepki vereceğinizi açıklayın – hangi adımları atarsınız?
- **Amaç:** Farklı öğrenme hızlarına sahip bir grupla çalışırken yansıtıcı bir öğretim yaklaşımı ve esneklik geliştirmek.

  Ek'in Kullanımı:

  Ek, eğitimci atölyeleri sırasında bireysel ve grup alıştırmaları, simüle edilmiş yaşlılar için eğitim oturumları için materyal ve özelleştirilmiş ders planları oluşturmak için bir başlangıç noktası olarak kullanılabilir.

Ek 2 | Pratik alıştırmalar – Eğitimcilere 'daki yaşlılar için siber güvenlik ilkelerini öğretmek

Her konu için pratik görevleri tamamlayın (ör. uygulamaları inceleyin, web sitesi güvenliğini kontrol edin, güvenli şifreler oluşturun ve test hesaplarıyla pratik yapın).

Eğitimcilerle Çalışmak için İçerik ve Yöntemler:

1. Yaşlılar Tarafından Kullanılan Popüler Çevrimiçi Uygulamalara Genel Bakış
   - **Eğitimcinin Görevi:** Allegro gibi alışveriş siteleri, Facebook gibi sosyal medya platformları ve mobil bankacılık gibi uygulamaların arayüzlerini tanıyın.
   - **Yöntem:** Ekran görüntülerinin analizi, mobil cihazlarda ve bilgisayarlarda arayüz incelemesi.
   - **Amaç:** Yaşlıların karşılaştığı ortak unsurları ve potansiyel zorlukları tanımak.

2. Güvenli Web Sitelerini ve Uygulamaları Tanımayı Öğrenme
   - **Pratik Görev:** 5 web sitesi örneğini inceleyin – hangilerinin güvenli olduğunu belirleyin. SSL sertifikasını, URL değerlendirmesini, şüpheli giriş formlarını belirtin.
   - **Yöntem:** Karşılaştırmalı analiz (güvenli ve güvenli olmayan siteler), etkileşimli test.
   - **Amaç:** Web sitesi güvenliğinin eleştirel analizini öğretmek.

3. Güvenli Şifre Oluşturma ve Giriş Verilerini Saklama İlkeleri
   - **Alıştırma:** 3C kuralını (Karmaşıklık, Değiştirilebilirlik, Hatırlanabilirlik) kullanarak 3 güvenli şifre oluşturun. Giriş bilgilerini saklamak için güvenli bir yol önerin (ör. şifre yöneticileri, çevrimdışı not defteri).
   - **Yöntem:** Beyin fırtınası, tartışma + şifre oluşturma konusunda mini atölye çalışması.
   - **Amaç:** Güvenlik ilkelerini basit ve ikna edici bir şekilde anlamak ve aktarmak.

4. Kurgusal Hesapları Kullanarak Pratik Alıştırmalar
   - **Görev:** Test amaçlı bir banka veya çevrimiçi mağaza hesabına (simülasyon) giriş yapın, güvenli bir "satın alma" işlemi gerçekleştirin ve sitedeki güvenlik öğelerini kontrol edin.
   - **Yöntem:** Bilgisayar/tabletlerle çiftler halinde çalışma, durum senaryoları.
   - **Amaç:** Teorik bilgileri, eğitimcilerin yaşlılara aktarabilecekleri pratik becerilere dönüştürmek.

Ek 3 | Çalışma Sayfası: Yaşlıların Öğreniminde Engelleri Belirleme

Engelleri (psikolojik, bilişsel, teknik) belirleyerek çalışma kağıdını doldurun.

Psikolojik Engeller	Örnek	Çözüm	Öğrenmeye Etkisi
Başarısızlık korkusu			
Özgüven eksikliği			
Sınırlı motivasyon			
Bilişsel Engeller	Örnek	Nasıl Çözülür	Öğrenme Üzerindeki Etkisi
Daha yavaş ezberleme			
Konsantrasyon güçlükleri			
Kısa süreli hafıza sorunları			
Teknik engeller	Örnek	Nasıl Çözülür	Öğrenme üzerindeki etkisi
Teknolojiyi kullanmada zorluklar			
İnternet kullanımında deneyim eksikliği			
Yeni eğitim platformlarını kullanma sorunları			

Ek 4 | Yaşlılar için İnternetin Güvenli Kullanımı

Örnekler sunun, gerçek hayattaki tehditleri tartışın ve yaşlılara çevrimiçi güvenliği öğretmek için etkileşimli alıştırmalar yapın.

1. Çevrimiçi Dolandırıcılık Örnekleri İçeren Sunumlar

- **Açıklama:** Sunumlar, yaşlıları hedef alan yaygın çevrimiçi dolandırıcılık örneklerini (örneğin, kimlik avı, sahte açık artırmalar veya dolandırıcılık amaçlı e-postalar) içermelidir. Eğitimciler, belirli vakaları gösteren ve tehlikeli unsurları nasıl tanıyacaklarını gösteren slaytlar veya görsel materyaller hazırlayabilirler.
- **Amaç:** Yaşlıların en yaygın çevrimiçi tehditler konusunda farkındalıklarını artırmak. Yaşlıların özellikle maruz kalabileceği dolandırıcılık ve diğer çevrimiçi istismar türlerini tanımayı öğretmek.
- **Tartışılacak Dolandırıcılık Örnekleri:**
  Kimlik avı: Giriş bilgilerini çalmak için kullanılan sahte e-postalar veya web siteleri.
  Çevrimiçi açık artırma dolandırıcılığı: sahte ürün satış teklifleri.
  Sahte SMS ve e-postalar: Bankalar gibi kurumlardan geliyormuş gibi görünen mesajlar.

2. Yaşlıların Günlük Yaşamlarında Karşılaştıkları Gerçek Tehditler Hakkında Tartışma

- **Açıklama:** Dolandırıcılık örneklerini sunduktan sonra, eğitimcinin katılımcıların yaşlıların karşılaştığı çevrimiçi tehditler hakkındaki deneyimlerini ve bilgilerini paylaşabilecekleri bir tartışma yürütmesi önemlidir. Eğitimciler, yaşlıları teknolojiyi kullanırken karşılaştıkları kendi deneyimleri ve zorlukları hakkında konuşmaya teşvik etmelidir.
- **Amaç**: Yaşlıların günlük yaşamlarında karşılaştıkları gerçek tehlikeleri anlamak. Dijital beceri eksikliği veya güvenlikle ilgili korkular gibi yaşlıların internet kullanımının önündeki engelleri belirlemek.
- **Örnek Tartışma Soruları**
  - Ne tür çevrimiçi dolandırıcılıklarla karşılaştınız veya duydunuz?
  - Yaşlıların çevrimiçi güvenlikle ilgili başlıca endişeleri nelerdir?
  - Yaşlılar interneti kullanmayı öğrenirken karşılaştıkları en büyük zorluk nedir?

3. Çevrimiçi Tehditleri Belirlemek için Etkileşimli Alıştırmalar ve Simülasyonlar

- **Açıklama:** Alıştırmalar ve simülasyonlar, çevrimiçi güvenlik bilgilerinin pratikte uygulanmasına yardımcı olur. Yaşlılar, hangi web sitelerinin veya mesajların güvenli, hangilerinin tehlikeli olabileceğini belirlemeleri gereken etkinliklere katılabilirler. Eğitimciler, şüpheli unsurları nasıl tanıyacaklarını gerçek zamanlı olarak göstermek için kurgusal bir banka hesabı, çevrimiçi mağaza veya sosyal medya profili gibi örnekler kullanabilirler.
- **Amaç:** Uygulamalı alıştırmalarla internet tehditlerini tanıma becerisini geliştirmek. Yaşlıların çevrimiçi güvenlikleri hakkında bilinçli kararlar alma becerilerini geliştirmek.
- **Örnek Alıştırmalar**
  - *Oltalama tanıma alıştırması:* Katılımcılara örnek e-postalar gönderilir ve hangilerinin oltalama girişimi olabileceğini belirtmeleri istenir.
  - *Çevrimiçi alışveriş simülasyonu:* Bir e-ticaret sitesinin grup analizi, sahte teklifleri nasıl tanıyacaklarını ve bir web sitesinin güvenli olduğunu gösteren unsurları kontrol etme.
  - *Web sitesi güvenlik değerlendirmesi:* Web sitelerini inceleyerek, eksik SSL sertifikaları veya şüpheli giriş formları gibi şüpheli unsurları belirlemek.

Ek 5 | İnternetteki tehditleri tanıma

Yaşlılara çevrimiçi tehditleri tanımayı öğretin ve e-postalar, bağlantılar ve şifreler ile alıştırma yapın.

1. Yaşlıların şüpheli çevrimiçi durumları tanımalarına yardımcı olacak yöntemlere genel bakış

❖ **Açıklama**

Eğitimciler, yaşlıların internetteki şüpheli durumları tanımalarını sağlayan çeşitli yöntemler kullanmalıdır. Ana hedef, güvenilir görünen her şeyin aslında güvenilir olmadığı konusunda farkındalık yaratmaktır. Açık ve basit kılavuzlar, yaşlıların belirli bir durumun güvenli olup olmadığını bağımsız olarak değerlendirmelerine yardımcı olabilir.

❖ **Yöntem**

- **Şüpheli durumları belirlemenin temel ilkeleri:** Yaşlılara şüpheli e-postaları, SMS mesajlarını veya sahte web sitelerini nasıl tespit edeceklerini öğretin. Örnekler: SSL sertifikasının olmaması, mesajlardaki yazım hataları, tutarsız URL'ler.
- **"Bilinmeyene güvenme" kuralı:** Yaşlıların şüpheli teklifler alabileceği durumlar (ör. sahte yatırım fırsatları, yarışma kazançları veya bilinmeyen kişisel veri talepleri) hakkında ortak bir tartışma.
- **Analojilerle eğitim:** Çevrimiçi durumları, pazarda şüpheli bir satıcıyı tanımak gibi gerçek hayattaki senaryolarla karşılaştırmak.

2. Yaşlıların siber güvenlik kurallarını hatırlamalarına yardımcı olan alıştırma örnekleri

❖ **Açıklama**

Yaşlıları dahil eden pratik alıştırmalar, siber güvenlik ilkelerini ve çevrimiçi ortamda dikkatli davranışları pekiştirmeye yardımcı olur. Yaşlılar, bu kuralları güvenli ve kontrollü bir ortamda uygulama fırsatı bulduklarında bu kuralları daha kolay hatırlarlar.

❖ **Alıştırmalar**

- **Sahte e-postaları tanıma:** Katılımcılara çeşitli e-posta örnekleri (gerçek ve sahte) verilir. Görevleri, hangi e-postaların dolandırıcılık olabileceğini ve hangilerinin güvenli olduğunu belirlemektir.
- **Tehlikeli bağlantıları tespit etme:** Yaşlılar, e-postalarda veya SMS mesajlarında şüpheli bağlantıları tespit etme alıştırması yapar ve bir URL'nin güvenilir olup olmadığını nasıl doğrulayacaklarını öğrenir.
- **Şifre güvenliği alıştırması:** Katılımcılar, güçlü ve zayıf şifre örnekleri oluştururlar. Güvenli şifreler oluşturmanın ilkelerini ve bunları güvenli bir şekilde saklamayı öğrenirler.

3. Yaşlıların hata yapabileceği çevrimiçi durumların simülasyonları ve bu hataları önlemelerini öğrenmelerine nasıl yardımcı olunabileceği

❖ **Açıklama**

Çevrimiçi simülasyonlar, yaşlıların deneyim yoluyla hataları nasıl tanıyacaklarını ve önleyeceklerini öğrenmelerini sağlayan pratik alıştırmalardır. Simülasyonlar, katılımcıların interneti kullanırken daha güvenli ve bilinçli hissetmelerine yardımcı olur.

❖ **Yöntem**

- **Oltalama simülasyonu:** Eğitimci, yaşlıların bankadan gelen gerçek bir mesaj gibi görünen ve giriş bilgilerini isteyen bir e-posta aldıkları bir senaryo sunar. Yaşlılar, nasıl aldatılmamaları gerektiğini ve e-postadaki hangi unsurların şüphe uyandırması gerektiğini öğrenirler.
- **Çevrimiçi alışveriş simülasyonu:** Yaşlılar, çevrimiçi mağazaları taklit eden web sitelerini ziyaret eder. Görevleri, çok düşük fiyatlar, SSL sertifikasının olmaması veya garip ödeme yöntemleri gibi şüpheli unsurları tespit etmektir.
- **Sahte ödül duyurusu simülasyonu:** Eğitimciler, bir yaşlının aslında bir dolandırıcılık olan bir yarışmayı kazandığına dair bir mesaj aldığı bir durum sunar. Yaşlılar bu tür dolandırıcılıkları tanımayı ve nasıl tepki vereceklerini öğrenir.

Ek 6 | Simülasyon Alıştırması: Bir Yaşlıyla Siber Güvenlik Hakkında Konuşmak

Eğitimcinin rehberliğinde ve yaşlıların uygulamasıyla, kimlik avı, dolandırıcılık, hesap güvenliği ve sosyal medya konularında rol yapma oyunu gerçekleştirin.

Görev Senaryosu

Eğitimci ve yaşlı, çevrimiçi tehditler hakkında bir konuşma yapar ve riskli durumları nasıl tanıyacaklarını ve önleyeceklerini öğrenir. Her senaryo, yaşlıların internette karşılaşabilecekleri farklı yaygın tehditleri sunar.

Alıştırma sırasında tartışılacak örnek konular

- Kimlik avı (sahte e-postalar, mesajlar)
  E-postalarda, SMS mesajlarında ve web sitelerinde kimlik avı nasıl tanınabilir?
  Sahte mesaj ve bağlantıların tipik belirtileri nelerdir?

- Sahte ödüller ve yarışma dolandırıcılığı
  Ödül ve yarışma kazançlarıyla ilgili yaygın dolandırıcılık türleri nelerdir?
  Ön ödeme gerektiren tekliflere nasıl yanıt verilmelidir?

- Çevrimiçi hesap güvenliği
  Bankalar, çevrimiçi mağazalar ve sosyal medyada hesap güvenliğini sağlamak için iyi uygulamalar nelerdir?
  Bir şifreyi güvenli kılan nedir ve iki faktörlü kimlik doğrulama neden önemlidir?

- Sosyal medyanın güvenli kullanımı
  Sosyal medyadaki sahte profiller ve dolandırıcılar nasıl tanınabilir?
  Hangi bilgiler korunmalı ve hangi bilgiler çevrimiçi olarak paylaşılmamalıdır?

Alıştırmada rol dağılımı (çiftler halinde)

- **Eğitmenin rolü (simülasyon eğitmeni):**
  Eğitmenin görevi, konuşmayı yönlendirmek, yaşlıların çevrimiçi tehditleri anlamalarına yardımcı olmak ve bunları nasıl tanıyacaklarını öğretmektir.
  Eğitimci, basit ve anlaşılır bir dil kullanmalı, tehditleri sabırla açıklamalı ve yaşlıların sohbete aktif olarak katılmalarını teşvik etmek için sorular sormalıdır.
  Eğitimci ayrıca yaşlılara internet güvenliği kurallarını hatırlatmak ve konuyu anladıklarından emin olmakla da sorumludur.

- **Yaşlıların rolü**
  Yaşlılar, internet kullanımıyla ilgili deneyimlerini paylaşarak sohbete aktif olarak katılırlar.
  Çevrimiçi güvenlikle ilgili şüphelerini veya endişelerini dile getirebilirler.
  Yaşlılar, eğitimcinin sorularını yanıtlar, kendi bakış açılarını paylaşır ve çevrimiçi tehditlerle ilgili sunulan sorunları çözmeye çalışır.

- **Kimlik avı (sahte e-postalar, mesajlar)**

E-postalarda, SMS mesajlarında ve web sitelerinde kimlik avı nasıl fark edilir?

Sahte mesaj ve bağlantıların tipik belirtileri nelerdir?

- **Sahte ödüller ve yarışma dolandırıcılığı**

Ödül ve yarışma kazançlarıyla ilgili yaygın dolandırıcılık türleri nelerdir?

Ön ödeme gerektiren tekliflere nasıl yanıt verilmelidir?

- **Çevrimiçi hesap güvenliği**

Bankalar, çevrimiçi mağazalar ve sosyal medyada hesap güvenliğini sağlamak için iyi uygulamalar nelerdir?

Bir şifreyi güvenli kılan nedir ve iki faktörlü kimlik doğrulama neden önemlidir?

- **Sosyal medyanın güvenli kullanımı**

Sosyal medyadaki sahte profiller ve dolandırıcılar nasıl tanınabilir?

Hangi bilgiler korunmalı ve çevrimiçi ortamda paylaşılmamalıdır?

Ek 7 | Senaryo Simülasyonları

Yaşlıların dolandırıcılık amaçlı aramalar, e-postalar veya SMS'lerle karşılaştığı senaryo simülasyonları yapın. Nasıl tepki vereceklerini sorun, duygularını ve güvenli tepkileri tartışın ve nefes alma gibi sakinleştirme tekniklerini uygulayın.

Alıştırma İçeriği

Alıştırma için hazırlık

Oturumu, zor durumlarda sakin kalmanın önemi hakkında kısa bir tartışma ile başlatın. Dolandırıcıların genellikle yaşlıları hızlı ve düşüncesiz kararlar almaya zorlamak için panik veya aciliyet hissi yaratmaya çalıştıklarını vurgulayın.

Tehdit senaryosu simülasyonları

- **Senaryo 1**
  Bir yaşlı, hesabının bloke edildiğini iddia eden ve bir uygulama yüklemesini isteyen bir "banka çalışanı"ndan telefon alır. Yaşlı ne yapar?
- **Senaryo 2**
  Yaşlı bir kişi, bir yarışmayı kazandığına dair bir e-posta alır ve kişisel bilgilerini girip bir bağlantıya tıklaması istenir. Yaşlı kişi ne yapar?
- **Senaryo 3**
  Bir yaşlı, bir paket için ekstra ödeme yapması gerektiğine dair şüpheli bir SMS alır. Yaşlı ne yapar?

Her senaryodan sonra:

- Yaşlılardan, böyle bir durumda nasıl tepki vereceklerini kısaca paylaşmalarını isteyin.
- Aşağıdaki gibi yansıtıcı sorular sorun
  Bu tür mesajlar aldığınızda ne hissedersiniz?
  Hangi duygular uyanır?
  Kararlarınızı etkileyen düşünceler nelerdir?

Ardından, sakin kalmak için atılması gereken adımları grup olarak tartışın:
panik yapmayın, dürtüsel davranmayın, durun ve yakınınızdaki biriyle konuşun, bilgileri doğrulayın.

Duygusal farkındalık egzersizi:
Yaşlılardan gözlerini kapatmalarını ve çevrimiçi ortamda kendilerini tehdit altında hissettikleri bir durumu (örneğin, şüpheli bir e-posta aldıkları) hatırlamalarını isteyin.
Şu soruları sorun: *O anda hangi duyguları hissettiniz? Vücudunuz hangi fiziksel sinyalleri verdi (örneğin, kalp atış hızınızın artması, tedirginlik hissi)?*
Onları, daha önce tartışılan nefes alma tekniklerini kullanmak gibi, tehditkar bir durumda bu duyguları kontrol etmenin yollarını bulmaya teşvik edin.

Alıştırma özeti:
Potansiyel bir tehditle karşı karşıya kaldıklarında karar vermeden önce bir duraklama yapmanın ne kadar önemli olduğunu vurgulayın.
Her zaman hemen harekete geçmenin gerekli olmadığını belirtin. Herhangi bir adım atmadan önce yardım istemek veya sevdiklerinize veya profesyonellere danışmak akıllıca olacaktır.

Eğitimciye yönelik ipuçları:

- **Sabırlı olun:** Yaşlılar tehditleri anlamak ve uygun şekilde tepki vermek için daha fazla zamana ihtiyaç duyabilir. Her tehdidi sabırla açıklayın ve olası çözümleri sunun.
- **Hızı ayarlayın:** Tüm katılımcıların her egzersizi anladığından ve soru sorma fırsatı bulduğundan emin olun.
- **Duygulara dikkat edin:** Duyguların karar vermeyi nasıl etkilediğini anlamak çok önemlidir. Bu nedenle gevşeme egzersizleri ve duyguları tanıma önemlidir.

Düzenli olarak pratik yapın

Yaşlıların kendilerini daha güvende hissetmeleri ve tehditlerle karşılaştıklarında nasıl tepki vereceklerini bilmeleri için bu oturumlar düzenli olarak tekrarlanmalıdır.

Ek 8 | Simülasyon Egzersizi: Örnek Siber Tehdit Raporları

Örnek siber tehditlerle rol oyunları yapın; riskleri açıklayın, belirleyin ve güvenli tepkileri uygulayın.

Görev Senaryosu

Katılımcılar ikili gruplar halinde çalışarak eğitimci ve kıdemli çalışan rollerini üstlenirler.
Her ikili, dört örnek siber tehdit raporundan birinin açıklamasını alır.
Eğitimcinin görevi, yaşlılarla sakin ve net bir eğitim sohbeti yürütmektir. Bu sohbet sırasında eğitimciler şunları yapar:

- tehdidin niteliğini açıklamak,
- yaşlı kişinin tehlike işaretlerini nasıl tanıyacağını anlamasına yardımcı olmak,
- yaşlı ile birlikte çalışarak duruma çözümler ve güvenli yanıtlar bulmak.

Katılımcılar rollerini değiştirebilir ve yeni bir raporla çalışabilirler.

Yaşlıları ilgilendirebilecek dört siber tehdit raporu örneği

Rapor 1: Paket için ek ödeme talep eden SMS

Durum açıklaması: Yaşlı kişi, bir paketin teslimat için beklediğini, ancak 2 EUR ek ödeme yapılması gerektiğini bildiren bir SMS aldı. Mesajda, bilinmeyen bir web sitesine yönlendiren şüpheli bir bağlantı vardı.

Rapor 2: Bankadan gelen sahte telefon görüşmesi

Durum açıklaması: Yaşlı kişi, banka çalışanı olduğunu iddia eden birinden telefon almıştır. Dolandırıcı, hesabın bloke edildiğini iddia etmiş ve hesabı korumak için bir uygulama yüklemesini önermiştir.

Rapor 3: Sözde ödül hakkında e-posta

Durum açıklaması: Yaşlı kişi, bir yarışma kazandığını iddia eden bir e-posta aldı. E-posta, kişisel verileri talep etti ve yaşlı kişiden şüpheli bir web sitesine yönlendiren bir bağlantıya tıklamasını istedi.

Rapor 4: Facebook hesabının ele geçirilmesi

Durum açıklaması: Yaşlı kişinin arkadaşları, onun hesabından bağlantılar veya kredi talepleri içeren garip mesajlar aldı. Yaşlı kişi bu mesajları göndermedi, bu da hesabının bir dolandırıcı tarafından ele geçirildiğini gösteriyor.

Eğitimcilere tehditler hakkında nasıl konuşacakları konusunda öneriler:

- **Durumu anlamak:** Tehditleri açıklamak için basit bir dil ve benzetmeler kullanın. Yaşlılar, durumlar günlük yaşam bağlamında sunulduğunda genellikle daha iyi anlarlar (örneğin, siber dolandırıcılığı geleneksel telefon dolandırıcılığıyla karşılaştırmak).
- **Örnekler ve simülasyonlar:** Simüle edilmiş telefon görüşmeleri kullanarak veya şüpheli e-postaların örneklerini analiz ederek düzenli olarak alıştırmalar yapın. Bu, yaşlıların gerçek tehditlere daha etkili bir şekilde yanıt vermelerine yardımcı olur.
- **Olayları bildirme konusunda yardım:** Yaşlıların siber tehditleri CERT Poland, bankalar veya polis gibi uygun kurumlara bildirmelerine yardımcı olun. Bu, eğitim oturumu sırasında güvenlerini artırmak için uygulanabilir.
- **İki faktörlü kimlik doğrulamanın önemi:** Yaşlıların çevrimiçi hesaplarının güvenliğini sağlamasına yardımcı olabilecek iki faktörlü kimlik doğrulamanın etkinleştirilmesi konusunda rehberlik sağlayın, özellikle sosyal medya kullanırken.
- **Sakin kalmak:** Eğitimciler, yaşlılara tehditkar durumlarda sakin kalmayı ve bilinmeyen uygulamaları yüklemek veya kişisel bilgileri paylaşmak gibi dürtüsel eylemlerden kaçınmayı öğretmelidir.
- **Güvenlik araçları hakkında eğitim:** Antivirüs yazılımı kullanımı, çevrimiçi hesapların güvenliğini sağlama ve bilgi kaynaklarının güvenilirliğini doğrulama (örneğin, resmi banka telefon numaralarını kontrol etme) konularını tanıtmak faydalı olacaktır.

Ek 9 | Yaşlılara İletişim Uygulamalarını Güvenli Bir Şekilde Kullanmayı Öğretme

Basit bir dil kullanarak uygulamaların güvenli kullanımını öğretin, simgelerle pratik yapın ve spam veya kimlik avı mesajlarını tanımlayın.

İçerik Kapsamı ve Öğretim Yöntemleri

1. İletişim uygulamalarının temel işlevlerini günlük dilde açıklama

Eğitimciye Öneriler

- Teknik terimler kullanmaktan kaçının – "hesabınıza giriş yapın" demek yerine "adınızı ve şifrenizi yazarak posta kutunuzu açın" deyin.
- "Gizlilik ayarları" yerine "sizi kimlerin görebileceğini ve kimlerin size mesaj gönderebileceğini seçebileceğiniz yer" deyin.
- Benzetmeler kullanın, örneğin "mesajlaşma uygulaması, mesaj ve resimlerin olduğu bir telefon gibidir".

Örnek Alıştırma

- Popüler uygulamaların simgelerinin bulunduğu kartları dağıtın (örneğin, e-posta, WhatsApp, Messenger, Zoom).
- Katılımcılardan bunları kendi kelimeleriyle tanımlamalarını isteyin.
- Birlikte, her biri için basit bir tanım oluşturun.

Destekleyici Materyaller

- Basit terimlerin (ör. "mesaj", "video görüşmesi", "ek") bulunduğu basılı bir sözlük hazırlayın.

2. Tehlikeli mesajları (Spam, Phishing) tanımlama alıştırmaları
Eğitimciye Öneriler

- Güvenli ve sahte mesajları göstermek için daima gerçek örnekler kullanın.
- Şüpheli bir e-posta adresinin neye benzediğini, "bu bağlantıya tıklayın" ifadesinin ne anlama geldiğini, "yurtdışındaki torun" dolandırıcılığını nasıl tespit edebileceğinizi tartışın.

Örnek Alıştırma

- Katılımcıları gruplara ayırın ve onlara üç adet basılı e-posta verin:
  - Gerçek bir sohbet daveti
  - "Fatura" bağlantısı içeren sahte bir e-posta
  - Dilbilgisi hataları içeren ve kişisel veri talebinde bulunan bir mesaj
- Görev: Hangi mesajların şüpheli olduğunu ve nedenini belirleyin.

Destekleyici Materyaller

- Analiz için örnek e-postalar içeren çalışma kağıtları oluşturun
- Her mesaj için 5 temel soru ekleyin:
  - Göndereni tanıyor muyum?
  - Mesaj mantıklı mı?
  - Herhangi bir hata var mı?
  - E-posta adresi doğru görünüyor mu?
  - Bağlantı şüpheli görünüyor mu?

3. Gizlilik ve güvenlik ayarlarını gösterme
Eğitimciler için öneriler

- Her görevi büyük bir ekranda veya projektörde adım adım gösterin.
- Unutmayın: yaşlılar genellikle tekrar yoluyla öğrenir – her adımı birlikte tamamlamayı planlayın.

Örnek Alıştırma
Katılımcılarla birlikte tamamlamak için:

- WhatsApp ayarlarına gidin → "Gizlilik" → "Profil Fotoğrafı" → "Kişilerim" seçeneğini seçin
- Messenger'da: bir yabancıyı nasıl engelleyeceğinizi gösterin

Destekleyici Materyaller

- Resimli adım adım talimat kartları oluşturun, örneğin:
  - "Şifrenizi nasıl değiştirebilirsiniz"
  - "Gizlilik ayarları nasıl yapılır"
  - "Bir kullanıcıyı nasıl engelleyebilirsiniz"

4. Etkileşimli yöntemler – Bilgileri pekiştirme ve tehditlere yanıt verme
Eğitimciler için öneriler:

- Simülasyonlar etkilidir – yaşlılar gerçekçi senaryolar aracılığıyla en iyi şekilde öğrenirler.
- Güven ve takım çalışması oluşturmak için ikili gruplar veya küçük gruplar kullanın.

Örnek Alıştırmalar:

- Simülasyon 1: "Bankadan garip bir mesaj aldım" – ne yapmalı?
- Simülasyon 2: "Zoom'da kızımla bağlantı kuramıyorum" – ayarları nasıl kontrol edebilirim?
- Rol oyunu: eğitimci dolandırıcı rolünü, katılımcı yaşlı rolünü oynar – sonra roller değiştirilir.

Destekleyici Materyaller:

- Simülasyon senaryoları oluşturun
- Rol kartları: eğitimci/katılımcı/dolandırıcılık yapan kişi
- Güvenlik ipuçları içeren eve götürülebilir hatırlatma kartları (örneğin, buzdolabına yapıştırmak için)

Ek 10 | Yaşlılara Antivirüs ve Sistem Güncellemelerini Kullanmayı Öğretme

Yaşlılara virüslerin ve güncellemelerin ne olduğunu öğretin, antivirüs kullanımını gösterin ve tarama yapma ve sistem güncellemelerini yüklemeyi adım adım uygulayın.

İçerik kapsamı ve öğretim yöntemleri

1. Giriş – Virüsler, güncellemeler ve güvenlik özellikleri nedir?

Eğitimciye öneriler:

- Karmaşık konuları açıklarken benzetmeler kullanmayı unutmayın.
- "Bilgisayar virüsleri"nin ne olduğunu açıklayın – bilgisayara saldırabilen soğuk algınlığı veya enfeksiyonla karşılaştırmalar yapın.
- Güncellemelerin bilgisayar için "ilaç" gibi olduğunu açıklayın – arızaları ve saldırıları önlemeye yardımcı olurlar.

Örnek alıştırma

- Katılımcılara şu soruları sorun:
  - "Bilgisayar virüsü"nü hiç duydunuz mu?
  - "Güncelleme" kelimesini duyduğunuzda aklınıza ne geliyor?

2. Antivirüs yazılımının tanıtımı

Eğitimciye öneriler:

- Güvenli ve sezgisel bir program kullanın (örneğin, Windows Defender, Avast'ın ücretsiz sürümü).
- Süreci adım adım izleyin: programı açma, güncellemeleri kontrol etme, hızlı tarama yapma. Prosedürü bir projektör kullanarak gösterebilirsiniz.

Örnek Alıştırma:

- Katılımcılardan kendi cihazlarında (veya paylaşılan bir dizüstü bilgisayarda) antivirüs yazılımını açmalarını isteyin.
- Birlikte bir tarama gerçekleştirin. Sonuçların ne anlama geldiğini tartışın: "tehdit bulunamadı" ve "tehditler tespit edildi".

3. İşletim sistemini güncellemeyi öğrenme

Eğitimciye öneriler:

- Güncelleme ayarlarının nasıl bulunacağını gösterin (örneğin, Windows'ta: Ayarlar → Güncelleme ve Güvenlik).
- Güncellemelerin genellikle otomatik olarak göründüğünü vurgulayın – kullanıcının sadece "Şimdi yükle" seçeneğine tıklaması yeterlidir.

Örnek alıştırma:

- **Her katılımcıya bir kontrol listesi verilir:**
  - "Ayarlar"ı açın
  - "Windows Güncelleme"yi bulun
  - Mevcut güncellemeleri kontrol edin
  - Varsa güncellemeyi yükleyin
- **Not: Paylaşılan bir bilgisayar kullanılıyorsa, alıştırma yorumlu bir sunum olarak gerçekleştirilebilir.**

4. Pekiştirme yöntemleri – kontrol listeleri, rol oyunları, tartışmalar

Eğitimciye öneriler:

- Materyali oyun veya test şeklinde özetleyin.
- Katılımcıları soru sormaya ve kendi deneyimlerini paylaşmaya teşvik edin.

Örnek alıştırmalar:

- Güvenlik kontrol listesi: Katılımcı, bilgisayarının/akıllı telefonunun korunup korunmadığını adım adım kontrol eder (şifreler, güncellemeler, taramalar).
- Telefon görüşmesi simülasyonu: Eğitimci, "Bilgisayarınız risk altında – programımızı indirin" diyen bir dolandırıcı rolünü oynar. Yaşlıların görevi, tehdidi fark edip "Önce antivirüs ayarlarımı kontrol edeceğim" şeklinde yanıt vermektir.

Destek materyalleri:

- Kullanıma hazır kontrol listeleri: "Güvenli Bilgisayar – İhtiyacım Olan Her Şeye Sahip miyim?"

Ek 11 | Çalışma kağıdı: Güvenli İnternet Kullanımı: Yaşlılar için Pratik İpuçları ve Teknikler

Güvenli alışveriş, cihaz güvenliği, çevrimiçi gizlilik ve teknolojiden korkmayı yenme ile ilgili soruları yanıtlayarak çalışma sayfasını doldurun.

Güvenli Çevrimiçi Alışveriş	
Çevrimiçi tekliflerin hangi unsurları yaşlılara potansiyel olarak tehlikeli veya şüpheli olarak vurgulanmalıdır?	
Yaşlıları çevrimiçi alışveriş sürecinde nasıl yönlendirebilirsiniz – nasıl konuşmalı, ne göstermeli ve neye dikkat etmelisiniz ki kendilerini güvende hissetsinler?	
Cihaz Güvenliği	
Yaşlıların cihazlarını güvenli bir şekilde nasıl kuracaklarını anlamalarına yardımcı olacak teknikler nelerdir?	
Yaşlıların cihazlarını korumak için hangi uygulamalar ve ayarlar gereklidir?	
Çevrimiçi Gizlilik Koruması	
Yaşlıların, özellikle WhatsApp gibi iletişim uygulamalarını kullanırken çevrimiçi gizlilik koruması kavramını daha iyi anlamalarına yardımcı olmak için hangi yöntemleri kullanacaksınız?	
Teknoloji Korkusunu Aşmak	
Yaşlıların teknoloji korkusunu yenmelerine ve interneti kullanırken kendilerine güvenlerini güçlendirmelerine yardımcı olacak eğitim unsurları nelerdir?	
Yaşlıların yeni teknolojiler dünyasında kendilerini rahat hissetmeleri için hangi özgüven geliştirme yöntemleri kullanılmalıdır?	

Ek 12 | Katılımcılar için daha fazla okuma ve öğrenme önerileri

Siber güvenlik web siteleri: Siber güvenlikle ilgilenen Avrupa ve hükümet kuruluşları

1) **ENISA – Avrupa Birliği Siber Güvenlik Ajansı**
   Web sitesi: https://www.enisa.europa.eu
   ENISA, siber güvenlik konusunda kılavuzlar, raporlar ve eğitim kampanyaları sunmaktadır. Yaşlılar da dahil olmak üzere bireysel kullanıcılar için e-postaları, şifreleri, akıllı telefonları ve çevrimiçi bankacılığı güvenli bir şekilde kullanmaya yönelik eğitim materyalleri içermektedir.
2) **Avrupa Komisyonu – Daha Güvenli İnternet**
   Web sitesi: https://digital-strategy.ec.europa.eu/en/policies/safer-internet
   Avrupa Komisyonu'nun yaşlılar dahil tüm yaş grupları için güvenli internet kullanımını teşvik eden programı. Web sitesi, bilgilendirme kampanyaları ve ulusal girişimlere bağlantılar içermektedir.
3) **Avrupa Tüketici Merkezi Ağı (ECC-Net)**
   Web sitesi: https://www.eccnet.eu
   AB'deki tüketici merkezlerinden oluşan bir ağ olup, güvenli çevrimiçi alışveriş, kişisel verilerin korunması ve internet dolandırıcılığından kaçınma konusunda tavsiyeler sunar; bu bilgiler özellikle yaşlılar için yararlı olabilir.
4) **Cyberprofilaktyka – Dijital Önleme Programı**
   Web sitesi: https://cyberprofilaktyka.pl/
   Yaşlılara çevrimiçi tehditlerden kaçınmak için tavsiyeler içeren bir bölümün yer aldığı dijital önleme programı. Ayrıca, dijital riskleri daha iyi anlamaya yardımcı olmak için eğitim materyalleri, infografikler ve gerçek hayattan dolandırıcılık örnekleri de içerir.

6.5 Modül V – Ön/Son Test

1. Modül 5'in ana hedefi nedir?

A) Yaşlılara sosyal medyayı eğlence amaçlı kullanmayı öğretmek
B) Eğitimcileri, yaşlıları güvenli dijitalleşmede etkili bir şekilde desteklemek için eğitmek
C) Yaşlıların yapay zeka konusundaki bilgilerini geliştirmek
D) Yaşlıların programlama becerilerini geliştirmek

2. Aşağıdakilerden hangisi yaşlıların dijital becerileri öğrenirken karşılaştıkları yaygın bir engeldir?

A) Yeni teknolojilere karşı merak
B) Başarısızlık korkusu veya özgüven eksikliği
C) Sosyal medyanın aşırı kullanımı
D) Güçlü teknik bilgi

3. Yaşlılar için etkili bir öğretim yöntemi nedir?

A) Profesyonel görünmek için karmaşık jargon kullanmak
B) Dersleri hızlı bir tempoda yürütmek
C) Talimatları küçük, basit adımlara bölmek
D) Yalnızca teorik bilgiye odaklanmak

4. Eğitimciler, çevrimiçi bankacılık ve alışveriş hakkında ders verirken nelere vurgu yapmalıdır?

A) Parayı daha hızlı harcamak
B) Güvenli web sitelerini nasıl tanıyacakları ve kişisel verilerini nasıl koruyacakları
C) Çevrimiçi görünürlüğü nasıl artırabiliriz
D) Antivirüs yazılımını nasıl devre dışı bırakılacağı

5. Aşağıdakilerden hangisi kimlik avı girişiminin iyi bir örneğidir?

A) Bir arkadaşınızın size tanıdık bir bağlantı göndermesi
B) Bankanızdan gelen, kullanıcı adınızı ve şifrenizi isteyen bir e-posta
C) Güvenilir bir yazılım programından gelen bir güncelleme
D) Takvim uygulamanızdan gelen bir hatırlatma

6. Bir yaşlı, "banka çalışanı"ndan şüpheli bir telefon aldığında ilk olarak ne yapmalıdır?

A) Önerilen uygulamayı hemen yüklemeli
B) Telefonu kapatıp resmi numaradan bankasını aramalı
C) Kimlik ve hesap bilgilerini vermek
D) Aramayı tamamen görmezden gelmek

7. Eğitimcilerin yaşlıların antivirüs programlarını anlamalarına yardımcı olmanın en iyi yolu nedir?

A) Virüsleri hastalıklara benzetmek gibi benzetmeler kullanarak açıklamak
B) Teknik açıklamalardan tamamen kaçınmak
C) Antivirüs konuları çok ileri düzeyde olduğu için atlamak
D) Yalnızca metin tabanlı açıklamalar göstermek

8. Yaşlılar için "dijital farkındalık" ne anlama gelir?

A) Çevrimiçi alışverişi daha hızlı yapmayı bilmek
B) Çevrimiçi tehditleri anlamak ve tanımak
C) Teknolojiyi hiç kullanmamak
D) Web sitesi tasarlamayı öğrenmek

9. Bir yaşlı, ders sırasında bir uygulamayı anlamazsa eğitimci ne yapmalıdır?

A) Bir sonraki konuya geçmek
B) Sabırla açıklamayı tekrarlamak ve basitleştirmek
C) Başka bir yaşlıdan öğretmesini istemek
D) Sorunu görmezden gelmek

10. Yaşlılar, hesaplarına siber saldırı yapıldığından şüphelenirlerse ne yapmalıdır?

A) Sorunun kendiliğinden çözülüp çözülmediğini beklemelidirler.
B) Banka veya yetkililere bildirmeli ve şifrelerini hemen değiştirmelidir
C) Bu haberi sosyal medyada paylaşmak
D) Tüm hesaplarını silmelidirler

Cevap Anahtarı Özeti

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

7. Değerlendirme Anketi

Bu ankette verdiğiniz bilgiler, katıldığınız eğitimlerin düzeyini ve bir sonraki eğitim programlarınızın etkinliğini ve çekiciliğini artırmak için bir kılavuz görevi görecektir.

Anketi kendiniz yanıtlayarak veya aşağıdaki derecelendirme ölçeğine göre doldurun. 1 en düşük, 5 en yüksek derecelendirmedir.

I. **Atölye değerlendirmesi:**

- Eğitim programı ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Derslerin yürütülme yöntemleri ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Dersler sırasındaki atmosfer ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Eğitimin yararlılığı ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Eğitmenin hazırlığı ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Eğitim içeriğinin seçimi ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Eğitimin hedefleri açıkça belirtilmişti ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1

1. **Hangi konular sizin için yararlı oldu ve kesinlikle kullanacaksınız?**
   .....
   .....

2. **Hangi konular sizin için daha az yararlı oldu?**
   .....
   .....

3. **Derste işlenmeyen ancak programa dahil edilmesi gerektiğini düşündüğünüz konular hangileridir ve neden?**
   .....
   .....

4. **Eğitim programına eklenmesi veya çıkarılması gereken konular olduğunu düşünüyor musunuz? Nedenini açıklayın.**
   .....
   .....

II. **Eğitim materyallerinin değerlendirilmesi:**

- İçerik 54321 ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Bilginin erişilebilirliği ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Okunabilirlik ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1
- Materyallerin kullanışlılığı ☐ 5 ☐ 4 ☐ 3 ☐2 ☐1

III. **Ek bilgi:**

1. **Eğitimin genel değerlendirmesi** ☐ **OLUMLU** ☐ **OLUMSUZ**

2. **Eğitim beklentilerinizi ve gereksinimlerinizi karşıladı mı - amaçlanan hedefler, çıktılar ve sonuçlar elde edildi mi?** ☐ **EVET** ☐ **HAYIR**

3. **Böyle bir eğitimin düzenlenmesinin faydalı olduğunu düşünüyor musunuz (ve neden)?**
   .....
   .....

4. **Ek yorum ve gözlemleriniz:**
   .....
   .....

5. **Eğitimden nasıl haberdar oldunuz?**
   .....
   .....

www.cybersafesenior.eu

Cyber-Safe-Senior

Funded by
the European Union

CYBER SAFE
SENIOR

Instytut
Nowych Technologii

iED

ILKSENOL
DERNEĞİ

SIMBIOZA
MED GENERACIJAMI

“Avrupa Birliği tarafından finanse edilmiştir. Burada ifade edilen görüş ve düşünceler yalnızca yazar(lar)a aittir ve Avrupa Birliği’nin veya Erasmus+ Ulusal Ajansı’nın görüşlerini mutlaka yansıtmaz. Avrupa Birliği ve hibe sağlayan kurum bunlardan sorumlu tutulamaz.”