ERASMEDIAH – EDUCATIONAL REINFORCEMENT AGAINST THE SOCIAL MEDIA HYPERCONNECTIVITY
PROJE NUMARASI: 2023-1-HU01-KA220-YOU-000161173

MODÜL 5
SİBER GÜVENLİK VE ÇEVRİMİÇİ GÜVENLİK

ERASMEDIAH
Educational Reinforcement Against the Social Media Hyperconnectivity

erasmediah.eu

Co-funded by the European Union

Avrupa Birliği Tarafından Finanse Edilmektedir. Bununla birlikte, ifade edilen görüş ve görüşler yalnızca yazar(lar)ın görüşleridir ve Avrupa Birliği veya Avrupa Araştırma Yürütme Ajansı'nın görüşlerini yansıtması gerekmez. Ne Avrupa Birliği ne de EACEA bunlardan sorumlu tutulamaz.

Ders 5.4

Siber Tehditlerin Tanınması ve Uygunsuz İçeriğe Maruz Kalmayı Önlemeye Yönelik Stratejiler

ERASMEDIAH
Educational Reinforcement Against the Social Media Hyperconnectivity

Co-funded by the European Union

Avrupa Birliği Tarafından Finanse Edilmektedir. Bununla birlikte, ifade edilen görüş ve görüşler yalnızca yazar(lar)ın görüşleridir ve Avrupa Birliği veya Avrupa Araştırma Yürütme Ajansı'nın görüşlerini yansıtması gerekmez. Ne Avrupa Birliği ne de EACEA bunlardan sorumlu tutulamaz.

Süre: 40 Dakika

Ders 5.4

Siber Tehditlerin Tanınması ve Uygunsuz İçeriğe Maruz Kalmayı Önlemeye Yönelik Stratejiler

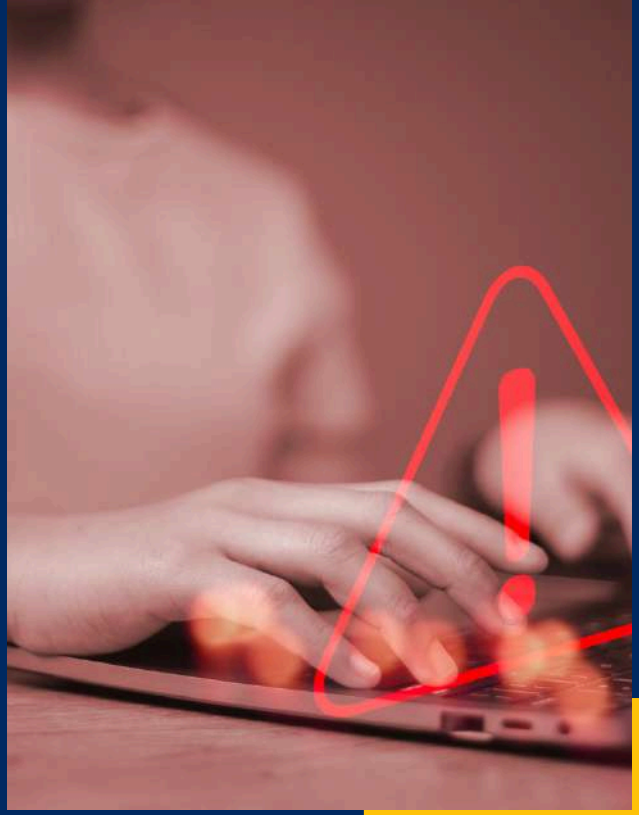
Hedefler:

- Özellikle çocuklar ve gençler gibi savunmasız kullanıcıları hedef alan, uygunsuz içerik, siber zorbalık ve çevrim içi taciz (grooming) gibi yaygın çevrim içi riskler konusunda farkındalık geliştirmek.
- Şüpheli bağlantılar, yırtıcı çevrim içi davranışlar ve manipülatif içerik gibi siber tehditlerin uyarı işaretlerini tanıma konusunda katılımcıları eleştirel becerilerle donatmak.
- Eleştirel düşünmeyi teşvik ederek, güvenli dijital alanları tanımlayarak ve çevrim içi deneyimler hakkında açık iletişimi sürdürerek çevrim içi etkileşimleri bilinçli şekilde yönetmeye yönelik proaktif alışkanlıkları desteklemek.

Temel Mesaj(lar):

- Çevrim içi tehditler çoğu zaman masum görünen platformlar veya etkileşimler arkasına saklanır. İşaretleri tanımak, güvende kalmanın anahtarıdır.
- İçerik filtreleri kullanmak ve güçlü bir iletişim kurmak gibi basit uygulamalar, zararlı içeriklere ve siber tehditlere karşı korunmaya yardımcı olabilir.

DERSİN TÜRÜ:



Derse Genel Bakış

Günümüzün aşırı bağlantılı dijital ortamında, uygunsuz içeriklere ve siber tehditlere maruz kalmak sürekli bir risk haline gelmiştir. Bu ders, bu tehditlerin doğasını ve risklerini kapsamlı bir şekilde anlamanızı sağlamak, bunları azaltmak için pratik araçlar sunmak ve daha güvenli çevrim içi etkileşimleri destekleyecek stratejileri öğretmek amacıyla hazırlanmıştır. Etkileşimli alıştırmalar ve uygulanabilir öneriler aracılığıyla, bu oturum sonunda dijital dünyada daha güvenli ve sorumlu bir şekilde gezinmeye hazır olacaksınız.

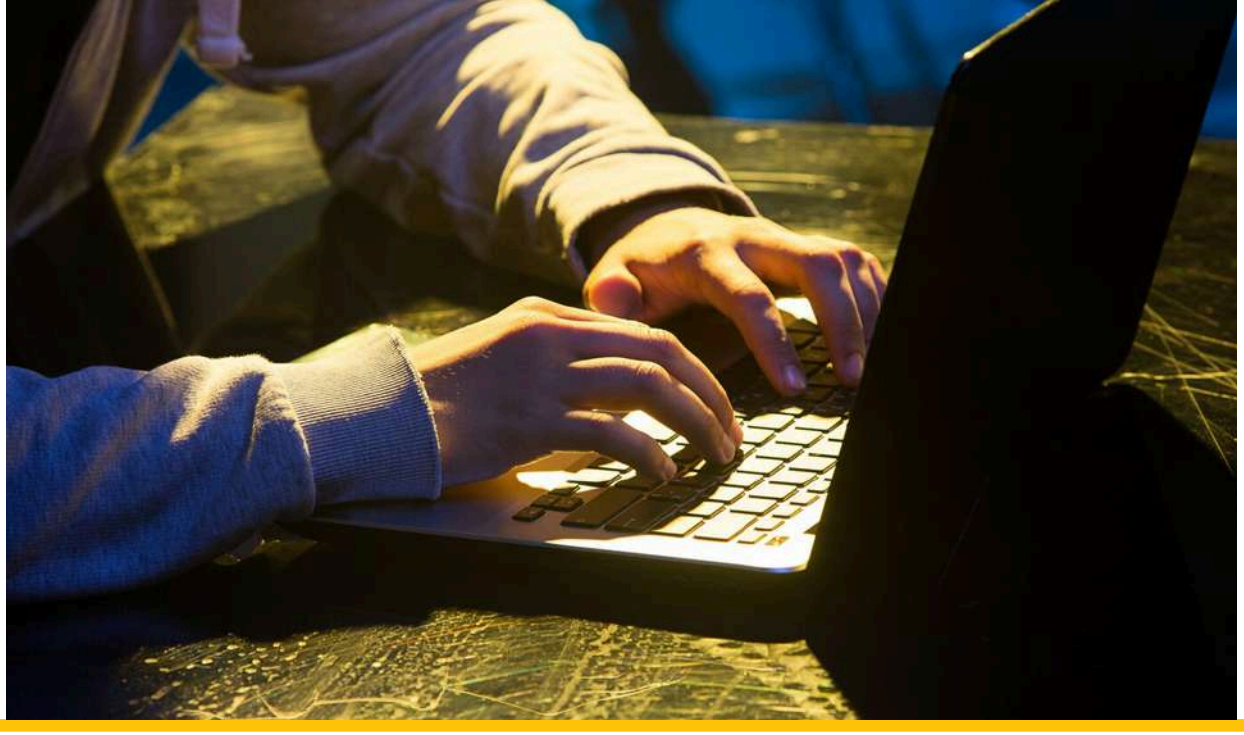
Atölye 4 adımda düzenlenmiştir:

1: Siber tehditlerin ve uygunsuz içeriklerin temelleri (10 dakika)

2: Uyarı işaretlerini ve riskleri tanıma (15 dakika)

3: Önleme ve risk azaltma yaklaşımları (10 dakika)

4: Yansıtma ve uygulama (5 dakika)



1 Adım

Siber tehditler ve uygunsuz içerikle ilgili temel bilgiler

Hiç çevrim içi ortamda sizi rahatsız eden veya güvende hissettirmeyen bir şeyle karşılaştınız mı?
Siber tehditler, bireyleri veya sistemleri hedef alarak bilgi çalmak, zarar vermek ya da güvenlik açıklarından faydalanmak amacıyla gerçekleştirilen zararlı çevrim içi faaliyetlerdir. Örnekler şunları içerir:

- Siber zorbalık: Çevrim içi platformlar kullanılarak bir kişiye taciz ya da baskı uygulanması.
- Oltalama: Kişisel bilgileri elde etmek amacıyla insanları kandırmaya yönelik aldatıcı mesajlar gönderilmesi.
- Taciz amaçlı yakınlık kurma: Genellikle uygunsuz amaçlarla, biriyle çevrim içi ortamda ilişki kurarak zamanla onu sömürmeye çalışma.

Uygunsuz içerik nedir? Bazı yaş grupları için zararlı, açık ya da uygun olmayan içeriklerdir. Örneğin:

- Müstehcen görüntüler veya videolar
- Manipülatif ya da istismar edici mesajlar
- Şiddet içeren veya nefret söylemi barındıran materyaller

1 Adım

Siber tehditler ve uygunsuz içerikle ilgili temel bilgiler

Bu tür içeriklere maruz kalmak duygusal sıkıntılara, ilişkilerin zarar görmesine ve kimlik hırsızlığı ya da istismar gibi uzun vadeli sonuçlara yol açabilir.

Etkinlik

Şimdi küçük gruplara ayrılacağız. Her gruba analiz etmesi için bir senaryo verilecek:

- Senaryo 1: Tanımadığınız bir kişiden, kişisel bilgilerinizi isteyen bir e-posta alıyorsunuz.
- Senaryo 2: Bir e-postada şüpheli bir bağlantıyla karşılaşıyorsunuz.
- Senaryo 3: Sosyal medyada uygunsuz bir yorum görüyorsunuz.

Göreviniz, grubunuzla birlikte şu soruları yanıtlamaktır:

- Bu durumun riskli tarafı nedir?
- Bu duruma güvenli şekilde nasıl yanıt verebilirsiniz?

Gruplar çalışmalarını tamamladıktan sonra, hep birlikte sonuçları paylaşacağız.

2 Adım

Uyarı işaretlerini ve riskleri tanımak

Aşağıdaki örneklere göz atın ve internette buna benzer bir şeyle karşılaşıp karşılaşmadığınızı düşünün. Beyin fırtınası yaparken grup olarak tartışın: Bu uyarı işaretlerinden hangileri en yaygın olanlardır ve bunlara nasıl yanıt verebilirsiniz?

1. Bilinmeyen veya şüpheli gönderici

Tanımadığınız bir kişiden, sizden kişisel bilgi isteyen ya da sizi bir bağlantıya tıklamaya yönlendiren bir mesaj alırsınız. E-posta adresi alışılmadık görünür, örneğin "bank123rastgele@mail.com" gibi, resmi bir adres değildir.

Tartışma sorusu: “Tanımadığınız bir kişiden mesaj aldığınızda ne yaparsınız?”

2. Yazım veya dil bilgisi hataları

Mesaj yazım hatalarıyla doludur ya da cümle yapısı gariptir.

Örnek: “Hesabınız bloke edildi! Yeniden etkinleştirmek için buraya tıklayın.”

Tartışma sorusu: “Bir mesajdaki yazım hataları sizi şüphelendirir mi? Neden veya neden değil?”

2 Adım

Uyarı işaretlerini ve riskleri tanımak

3. Acil talepler veya tehditler

- Şu tür mesajlar: "24 saat içinde ödeme yapmazsanız hesabınız devre dışı bırakılacak!"
- İçerik sizi korkutarak ya da baskı altına alarak hızlı harekete geçmenizi sağlamaya çalışır.
- **Tartışma sorusu:** “Gerçek bir uyarıyla dolandırıcılığı nasıl ayırt edebilirsiniz?”

4. Gerçek olamayacak kadar iyi teklifler

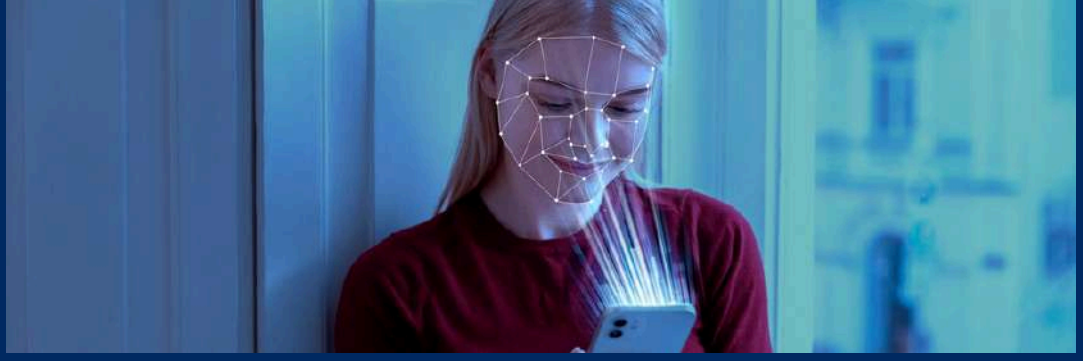
- İnanılmaz ödüller vaat eden reklamlar: "Yeni bir iPhone kazandınız! Ödülünüzü almak için buraya tıklayın"
- Çok az çabayla büyük kazançlar sunduğunu iddia eden internet siteleri.
- **Tartışma sorusu:** “Bu tür teklifleri neden tehlikeli bulmalıyız?”

2 Adım Uyarı işaretlerini ve riskleri tanımak

5. Bilinmeyen bağlantılar veya ekler

- Güvenilir görünmeyen bir bağlantı alırsınız, örneğin: "www.ucretsizhediye.simdi"
- Bilinmeyen gönderenlerden gelen ve virüs içerebilecek ekler.
- Tartışma sorusu: “Bir bağlantının veya ekin güvenli olup olmadığını nasıl kontrol edebilirsiniz?”

Grubunuzla birlikte bu uyarı işaretlerinden birini seçin ve bu durumu nasıl yöneteceğinizi tartışın. Etkinliğin sonunda, her grup günlük çevrim içi etkinliklerde bu risklerden nasıl kaçınılacağına dair fikirlerini ve çıkarımlarını paylaşacaktır.



3 Adım

Önlemeye ve hafifletmeye yönelik yaklaşımlar

İnternette güvende kalmanın en iyi yolu, verilerinizi koruyan ve riskler gerçekleşmeden önce önlem alan proaktif adımlar atmaktır. Haydi, hemen uygulamaya başlayabileceğiniz basit stratejileri birlikte inceleyelim.

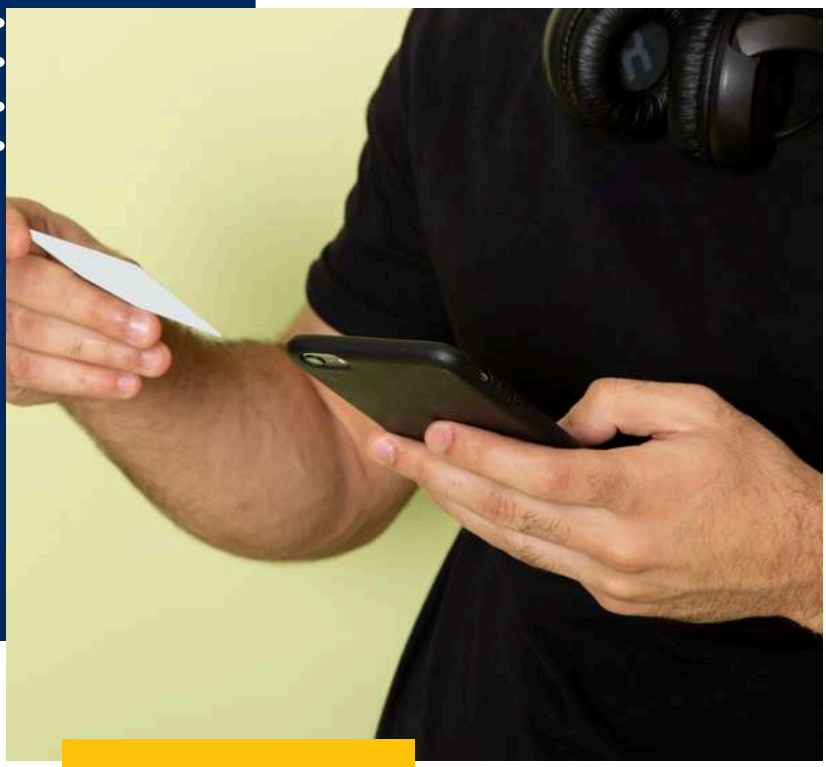
Aynı gruplarda kalalım. Aşağıdaki listeyi okuyun çevrim içi riskleri azaltmak için atabileceğiniz basit adımlardan bazıları:

- **Güçlü, benzersiz parolalar kullanın** ve düzenli olarak güncelleyin.
- **Önemli hesaplarınız için** çok faktörlü kimlik doğrulamayı (MFA) etkinleştirin.
- **Şüpheli bağlantı ve eklerden** kaçının her zaman kaynağın güvenilirliğini doğrulayın.
- **Sosyal medya ve uygulamalardaki** gizlilik ayarlarınızı gözden geçirerek bilgilerinizi kimlerin görebileceğini kontrol edin.
- Güvenlik açıklarını kapatmak için yazılımlarınızı güncel tutun.

Grubunuzla birlikte, bu adımlardan hangilerini zaten uyguladığınızı ve hangilerini uygulamakta zorlanabileceğinizi tartışın.

Bu soruları birlikte yanıtlayın:

- “Sizce internette güvende kalmak için en etkili strateji hangisidir?”



3 Adım

Önlemeye ve hafifletmeye yönelik yaklaşımlar

“Kendinize daha iyi alışkanlıklar edinmeyi örneğin gizlilik ayarlarını kontrol etmeyi ya da riskli bağlantılardan kaçınmayı nasıl hatırlatabilirsiniz?”

Beyin fırtınası yaptıktan sonra, her grup **hangi yeni stratejiyi** benimsemeyi planladığını ve bunun neden önemli olduğunu kısaca açıklayarak paylaşır.

Son bir yansıma olarak, çevrim içi güvenliğinizi artırmak için hemen uygulamaya başlayacağınız belirli bir alışkanlık ya da aracı düşünün. Bunu bir post-it notuna yazın ve aynı alışkanlıkları başkalarına nasıl kazandırabileceğinizi düşünün. Bilginizi paylaşarak yalnızca kendiniz için değil, arkadaşlarınız, aileniz ve topluluğunuz için de daha güvenli bir dijital ortam oluşturabilirsiniz.

4 Adım

Yansıma ve uygulama

Artık çevrim içi riskleri ve bu risklere karşı alınabilecek önlemleri incelediğimize göre, şimdi öğrendiklerinizi düşünme ve bunları günlük dijital yaşamınızda nasıl uygulayabileceğinizi planlama zamanı.

Sessizce şu soruyu yanıtlayın:

- “Şu anda çevrim içi ortamda sizi riske atabilecek bir alışkanlığınız nedir?”

Cevabınızı bir post-it kâğıdına yazın.

Sonraki adımda, bir eşle eşleşin ve düşüncelerinizi paylaşın:

- Tanımladığınız riskli alışkanlığı ve neden sorun olabileceğini açıklayın.
- Bu riski azaltmak için benimsemeyi planladığınız eylemi veya aracı paylaşın.
- Birbirinize geri bildirim verin veya planınızı güçlendirecek ek fikirler sunun.
- Bu stratejilerin farklı durumlarda örneğin halka açık Wi-Fi kullanırken, kişisel bilgi paylaşırken ya da oltalama ve çevrim içi yönlendirme risklerinden kaçınırken nasıl uygulanabileceğini tartışın.

Temel Çıkarım Özeti

- **Farkındalık, korunmanın ilk adımıdır.**
- **Uyarı işaretleri her yerde olabilir; ancak bunları tanımayı ve doğru şekilde tepki vermeyi öğrendiğinizde, çevrim içi güvenliğinizi büyük ölçüde artırabilirsiniz!**
- **Siber tehditleri ve uygunsuz içerikleri anlamak, olası riskleri tanımanızı ve kendinize güvenle yanıt vermenizi sağlar.**
- **Günlük çevrim içi durumlarda riskleri fark etmek, hızlı hareket etmenizi ve tehlikelerden kaçınmanızı sağlar.**
- **Farkındalık yaydığınızda, herkes için daha güvenli bir dijital topluluk oluşturulmasına katkı sağlarsınız.**

Gençlik çalışanları, eğitimciler ve öğretmenlere yönelik yönergeler

Hedef:

Bu ders, çevrim içi tehditler ve uygunsuz içerikler dâhil olmak üzere dijital ortamdaki riskler konusunda farkındalık oluşturmak ve katılımcılara daha güvenli çevrim içi etkileşimler kurmalarına yardımcı olacak pratik stratejiler kazandırmak amacıyla hazırlanmıştır. Katılımcılar, gerçek yaşamdan alınan senaryoları analiz ederek riskleri tanımayı, uyarı işaretlerini fark etmeyi ve önleyici tedbirler almayı öğreneceklerdir.

Gerekli Materyaller:

- Temel kavramların sunumu için flipchart veya dijital sunum aracı
- Kalem ve renkli keçeli kalemler
- Not almak veya etkinlikleri tamamlamak için boş A4 kâğıtları
- Katılımcılara tanıtmak amacıyla *CyberWise* veya *Malwarebytes Browser Guard* gibi araçlara erişim
- Beyin fırtınası çalışmaları için renkli post-it notlar

1 Adım: Siber tehditlerin ve uygunsuz içeriğin temelleri (10 dakika)

1. Katılımcılara şu soruyla başlayın: “Çevrim içi ortamda sizi güvensiz veya şüpheli hissettiren bir şeyle karşılaştınız mı?”. Bazı katılımcıların deneyimlerini paylaşmasını teşvik edin ya da şüpheli bir e-posta almak veya rahatsız edici bir yorum görmek gibi kısa bir örnek verin. Bu soruyu, çevrim içi riskleri anlamanın ve bunlara karşı önlem almanın önemini vurgulamak için kullanın.
2. Mini ders – temel siber tehditleri açıklayın: kimlik avı, istismar amaçlı çevrim içi yakınlaşma vb. Uygunsuz içeriği tanımlayın, örnek olarak şunları verin:

- Açık materyaller – Zararlı veya grafik içerikli görseller ve videolar.
- Yırtıcı mesajlar – Kandırıcı ya da zararlı iletişim.
- Yaşa uygun olmayan içerikler – Belirli yaş grupları için uygun olmayan materyaller.

3. Etkinlik: Katılımcıları 3-5 kişilik gruplara ayırın ve her gruba üç farklı senaryodan birini verin.

Gruplar için talimatlar:

1. Riski analiz edin: Senaryoda riski oluşturan unsurları tartışın (örneğin: bilinmeyen gönderici, acil tonlama ya da şüpheli bağlantı).
2. Güvenli eylemler önerin: Pratik yanıtlar üzerine beyin fırtınası yapın:

- E-postalar için: Bağlantılara tıklamaktan kaçının, göndereni resmi kanallardan doğrulayın veya spam olarak işaretleyin.
- Uygunsuz yorumlar için: Kullanıcıyı engelleyin, yorumu bildirin ve yanıt vermekten kaçının.
- Şüpheli bağlantılar için: Üzerine gelerek URL’yi kontrol edin, emin değilseniz tıklamayın ve güvendiğiniz birine danışın.

3. Bulguları paylaşın: Gruplar analizlerini özetleyerek sınıfla paylaşsın. Ortak stratejiler vurgulansın ve bunların ne kadar etkili olduğuna dair sınıfça tartışma yürütülsün.
4. Temel noktaları vurgulayarak etkinliği tamamlayın, bu etkinliği ilerleyen adımlarda işlenecek çevrim içi güvenlik stratejilerine bağlayın.

2 Adım: Uyarı işaretlerini ve riskleri tanıma (15 dakika)

1. Katılımcılara, siber tehditlerin yaygın uyarı işaretlerini net örneklerle tanıtın:

- Şüpheli bağlantılar veya bilinmeyen göndericiler: Tanımadığınız kişilerden gelen, bağlantı veya ek içeren mesajlar (örnek: "www.freeprizes.xyz").
- Yazım hataları veya acil talepler: “Hesabınız bloke edildi! Şimdi yeniden etkinleştirin” gibi acele ettiren, genellikle kötü yazılmış mesajlar.
- Gerçek olamayacak kadar iyi teklifler: “Ücretsiz iPhone kazandınız!” gibi ödül veya fırsat vaadi içeren mesajlar.
- Bu örnekleri daha etkili hale getirmek için kimlik avı girişimlerinden ekran görüntüleri gibi görseller kullanabilirsiniz. Katılımcıların kendi karşılaştıkları örnekleri paylaşmalarını teşvik edin.

2. Bir grup çalışması gerçekleştirin. Katılımcıları küçük gruplara ayırın ve her gruba belirli bir uyarı işaretini analiz etmeleri için atayın (örneğin: acil mesajlar veya şüpheli bağlantılar). Aşağıdaki adımları uygulamalarını isteyin:

- Uyarıyı analiz edin: Tehdidi inandırıcı kılan unsurları tartışın (örneğin: aciliyet duygusu veya aldatıcılık).
- Çözüm önerin: Kaynağı doğrulamak, şüpheli bağlantılardan kaçınmak veya dolandırıcılığı bildirmek gibi yanıtlar üzerine beyin fırtınası yapın.
- Bulguları özetleyin:Atanan tehdide karşı nasıl önlem alınabileceğine dair pratik ipuçları hazırlayın.

3. Etkinliğin sonunda her grup bulgularını ve stratejilerini sunar. Tüm grupların önerileri beyaz tahta veya flipchart üzerine yazılarak ortak bir "en iyi uygulamalar" listesi oluşturulur. Oturumu, çevrim içi ortamda güvende kalmak için dikkatli olmanın, doğrulamanın ve eleştirel düşünmenin önemini vurgulayarak sonlandırın.

3 Adım: Önleme ve zarar azaltma yaklaşımları (10 dakika)

1. Kişisel verilerin korunması ve çevrim içi risklerin azaltılması için proaktif adımların önemini vurgulayarak başlayın. Katılımcıların hemen uygulayabileceği basit eylemlerden oluşan bir liste sunun, örneğin:

- Güçlü, benzersiz şifreler kullanmak ve bunları düzenli olarak güncellemek.
- Kritik hesaplar için çok faktörlü kimlik doğrulama (MFA) etkinleştirmek.
- Şüpheli bağlantı ve eklerden kaçınmak için kaynaklarını doğrulamak.
- Sosyal medya ve uygulamalardaki gizlilik ayarlarını gözden geçirmek.
- Güvenlik açıklarını gidermek için yazılımları güncel tutmak.

Bu adımların çevrim içi ortamlardaki yaygın riskleri nasıl etkili şekilde azaltabileceğini açıklayın.

2. Katılımcılar mevcut gruplarında kalır. Aksiyon listesini verin ve aşağıdaki görevleri tamamlamalarını isteyin:

1. Grup tartışması:

- Halihazırda uyguladıkları adımları ve zorlandıkları adımları belirleyin.
- Bazı stratejilerin neden daha zor uygulanabildiğini tartışın ve bu zorlukları aşmak için yollar üretin.

2. Anahtar sorulara yanıt verin:

- “Çevrim içi ortamda güvende kalmak için en etkili strateji sizce hangisi?”
- “Gizlilik ayarlarını düzenli olarak kontrol etmek ya da riskli bağlantılardan kaçınmak gibi alışkanlıkları sürdürmek için kendinize nasıl hatırlatmalar yapabilirsiniz?”

3. Yeni stratejiler paylaşımı:

Her grup, benimsemeyi planladıkları yeni bir strateji seçer, bunun neden önemli olduğunu açıklar ve diğer gruplarla paylaşır.

3 Adım: Önleme ve zarar azaltma yaklaşımları (10 dakika)

3. Etkinliği şu şekilde sonlandırın: Her katılımcıdan çevrim içi güvenliğini artırmak için hemen uygulamaya başlayacağı bir alışkanlık ya da aracı bireysel olarak düşünmesini isteyin. Bunu bir post-it kâğıdına yazsınlar. Katılımcılara, bu alışkanlığı arkadaşlarıyla, aile üyeleriyle veya iş arkadaşlarıyla nasıl paylaşabileceklerini düşünmelerini söyleyin. Böylece toplu olarak daha güvenli bir çevrim içi ortam oluşturulabilir.

4 Adım : Yansıtma ve uygulama (5 dakika)

1.Bireysel yansıtma:

- Öğrencilere şu soruyu sorun: “Güvenliğinizi artırmak için çevrim içi davranışlarınızda değiştirebileceğiniz bir alışkanlık nedir?”
- Katılımcılar yanıtlarını post-it kâğıtlarına yazarlar.

2. Eşli tartışma:

- Katılımcılar ikili gruplar oluşturarak hedeflerini birbirleriyle paylaşır ve uygulanabilir adımlar önerirler.

3. Kapanış:

- Motivasyon verici bir mesajla oturumu tamamlayın. Örneğin:
- “Çevrim içi davranışlarınızda yapacağınız küçük değişiklikler, hem sizin hem de çevrenizin güvenliği için büyük bir fark yaratabilir.”

Temel Çıkarımlar:

- Katılımcılar, oturumdan; oltalama girişimleri, manipülatif mesajlar veya şüpheli bağlantılar gibi siber tehditleri ve uygunsuz içerikleri tanıma konusunda net bir farkındalıkla ayrılmalıdır. Kişisel bilgileri korumak için güçlü parolalar kullanma, çok faktörlü kimlik doğrulamayı etkinleştirme ve gizlilik ayarlarını özelleştirme gibi pratik güvenlik stratejilerinin önemi vurgulanmalıdır.
- Katılımcıların eleştirel düşünmeyi geliştirmeleri ve çevrim içi riskler hakkında açık iletişimi sürdürmeleri teşvik edilmelidir. Bu ilkelerin düzenli uygulamalarla ve başkalarıyla bilgi paylaşarak pekiştirilmesi, topluluk içinde daha güvenli dijital alışkanlıkları yaygınlaştıracak bir etki yaratacaktır.

İzleme ve Evde Uygulama Etkinlikleri:

Katılımcılardan şunları yapmaları istenir:

- Kendi sosyal medya gizlilik ayarlarını gözden geçirsinler.
- Malwarebytes Browser Guard veya içerik filtreleri gibi araçları denesinler.
- Öğrendikleri bir stratejiyi bir arkadaşları ya da aile bireyleriyle paylaşsınlar.

Eğiticilere Yönelik İpuçları:

- Çevrim içi riskleri ve pratik güvenlik stratejilerini açıklarken gerçek hayat örnekleri ve görsellerle dersleri ilgi çekici hale getirin. Katılımcıların içerikle bağlantı kurmasını sağlamak için etkileşimli tartışmaları teşvik edin. Güvenlik rehberi hazırlamak gibi uygulamalı etkinlikler, kavramların pekişmesini sağlar.
- Soruların memnuniyetle karşılandığı destekleyici ve açık bir ortam oluşturun; güvenli çevrim içi alışkanlıkların uzun vadeli faydalarını vurgulayın. Anahtar derslerin kalıcılığını sağlamak için takip görevleri ya da grup yansımalarıyla içeriği yeniden gözden geçirin.

İzleme ve Evde Uygulama Etkinlikleri:

Katılımcılardan şunları yapmaları istenir:

- Kendi kişisel sosyal medya gizlilik ayarlarını gözden geçirsinler.
- Malwarebytes Browser Guard gibi araçları veya içerik filtrelerini test etsinler.
- Öğrendikleri bir stratejiyi bir arkadaşları ya da aile bireyleriyle paylaşsınlar.

Eğiticiler için İpuçları:

- Dersleri ilgi çekici hale getirmek için çevrim içi riskleri ve pratik güvenlik stratejilerini açıklarken gerçek hayat örnekleri ve net görseller kullanın.
- Katılımcıların içeriğe bağlanmasını sağlamak için etkileşimli tartışmaları teşvik edin.
- Güvenlik rehberi hazırlamak gibi uygulamalı etkinlikler, kavramların pekişmesini sağlar.
- Soruların memnuniyetle karşılandığı destekleyici ve açık bir ortam oluşturun; güvenli dijital alışkanlıkların uzun vadeli faydalarını vurgulayın.
- Anahtar derslerin pekişmesini sağlamak için takip görevleri veya grup değerlendirmeleri yoluyla konuları düzenli olarak gözden geçirin.

Araçlar

CyberWise

CyberWise, bireylerin, özellikle ebeveynlerin, eğitimcilerin ve öğrencilerin çevrimiçi güvenliği anlamalarına yardımcı olmak için araçlar, kaynaklar ve kılavuzlar sunan bir eğitim platformudur. Kimlik avı, siber zorbalık ve uygunsuz içerik gibi siber tehditlerin tanınmasına ilişkin modüllerin yanı sıra riskleri azaltmaya yönelik stratejiler sağlar.

www.cyberwise.org

Malwarebytes Browser Guard

Bu, kullanıcıları kimlik avından, dolandırıcılıktan, kötü amaçlı yazılımlardan ve uygunsuz içerikten koruyan ücretsiz bir tarayıcı uzantısıdır. Zararlı web sitelerini ve reklamları aktif olarak engelleyerek yalnızca çocuklar için değil tüm kullanıcılar için daha güvenli gezinme sağlar.

www.malwarebytes.com

Kaynakça

- CyberWise. (n.d.). Retrieved from https://www.cyberwise.org
- Dalby, J. (2021, January 15). How to Avoid Inappropriate Content. Gabb Now. Retrieved from https://gabb.com/blog/how-to-avoid-inappropriate-content
- Fadziso, T., Thaduri, U., Ballamudi, V., Desamsetti, H. (2023, September 25). Evolution of the Cyber Security Threat: An Overview of the Scale of Cyber Threat. Retrieved from https://figshare.com/ndownloader/files/42443952
- Lynch, M. (2024, April 5). 19 simple ways to block inappropriate content. The Tech Edvocate. Retrieved from https://www.thetechedvocate.org/19-simple-ways-to-block-inappropriate-content
- Mallick, R. (2024, February 21). Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. Retrieved from https://www.researchgate.net/publication/378343830
- Malwarebytes Browser Guard. (n.d.). Retrieved from https://www.malwarebytes.com/browserguard
- Roy, R. (2021, August 23). What Is a Cyber Threat? Definition, Types, Hunting, Best Practices, and Examples. Retrieved from https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-cyber-threat
- Singh, J. (n.d.). 10 Types of Cyber Security Threats and Solutions. Retrieved from https://cybersecuritykings.com/10-types-of-cyber-security-threats-and-solutions

SINAV

1. Kimlik avı girişiminin temel bir işareti nedir?
A. Daha önce bilinmeyen ancak doğrulanmış bir hesaptan gelen bir mesaj almak
B. Bağlantı, görsel veya ek içermeyen bir e-posta
C. Hemen harekete geçmenizi isteyen, genellikle dil bilgisi hataları içeren bir e-posta
D. Tanıdık bir göndericiden gelen ve rutin bilgi isteyen bir mesaj

2. Aşağıdaki davranışlardan hangisi siber tehdit riskini artırabilir?
A. Cihazlarınızı ve uygulamalarınızı düzenli olarak güncellemek
B. Göndereni doğrulamadan e-postalardaki bağlantılara tıklamak
C. Çevrim içi hesaplarınızda iki faktörlü kimlik doğrulama kullanmak
D. Sosyal medyada gizlilik ayarlarını ayda bir gözden geçirmek

3. Siber tehditlere karşı kurban olma riskini azaltan alışkanlık hangisidir?
A. Güçlü ve benzersiz parolalar oluşturmak ve saklamak için bir parola yöneticisi kullanmak
B. Kolaylık olması adına uygulamaları yüklerken tüm izinleri kabul etmek
C. Parolanızı unutmamak için güvenilir arkadaşlarınız veya aile üyelerinizle paylaşmak
D. Tarayıcınızdan gelen güvenlik uyarılarını dikkate almamak

SINAV

4. Bir bağlantıyı şüpheli ve potansiyel olarak zararlı yapan nedir?
A. HTTPS şifreleme kullanması
B. Başka bir web sitesine yönlendirmesi
C. Alışılmadık karakterler veya alan adları içermesi
D. Bir arkadaş tarafından doğrudan mesajla paylaşılması

5. Uygunsuz içeriklere maruz kalmayı önlemede en etkili strateji hangisidir?
A. Tüm çevrim içi etkileşimleri en aza indirmek
B. Cihazlardaki tüm bildirimleri kapatmak
C. Yalnızca antivirüs yazılımına güvenmek
D. İçerik filtreleri kullanmak ve gizlilik ayarlarını düzenlemek

Cevaplar

Soru 1: C

Soru 2: B

Soru 3: A

Soru 4: C

Soru 5: D

ERASMEDIAH

Educational Reinforcement Against the Social Media Hyperconnectivity

Lélekben Otthon Közhasznú Alapítvány

AdM Archivio della Memoria

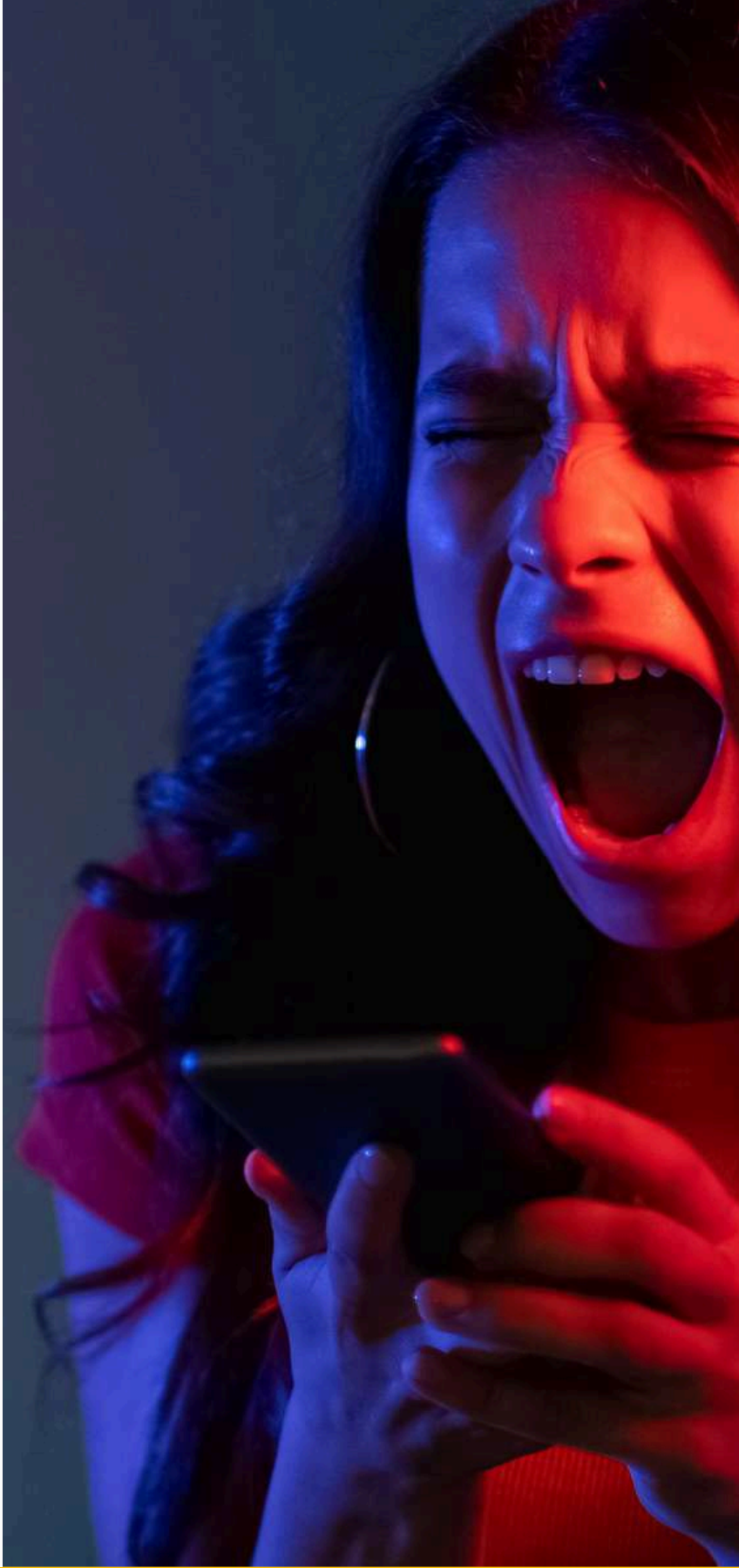
LABC

CWEP Centrum Wspierania Edukacji i Przedsiębiorczości

EDU yayıncılık

ASSERTED KNOWLEDGE THE ICT EQUALISERS

Inno Hub Valencia



Co-funded by the European Union

Avrupa Birliği Tarafından Finanse Edilmektedir. Bununla birlikte, ifade edilen görüş ve görüşler yalnızca yazar(lar)ın görüşleridir ve Avrupa Birliği veya Avrupa Araştırma Yürütme Ajansı'nın görüşlerini yansıtması gerekmez. Ne Avrupa Birliği ne de EACEA bunlardan sorumlu tutulamaz.