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 5.1

Siber Güvenliğin Esaslarına Giriş

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 5.1

Siber Güvenliğin Esaslarına Giriş

Hedefler:

- Tehditler, açıklar ve riskler gibi temel terimlerle birlikte siber güvenliğin temel kavramlarını net bir şekilde anlamak.
- Kimlik avı, kötü amaçlı yazılım, fidye yazılımı ve sosyal mühendislik saldırıları gibi yaygın çevrim içi tehditleri tanımlamak ve etkilerini kavramak.
- Olası siber güvenlik olaylarını tanımlama ve bu olaylara yanıt verme konusunda proaktif bir bakış açısı geliştirmek.

Temel Mesaj(lar):

- Birey, küçük işletme ya da küresel bir şirket olun; dijital ayak izinizi korumak için temel siber güvenlik uygulamalarını anlamak hayati öneme sahiptir.
- Basit önleyici adımlar atmak, bir siber saldırının ardından oluşacak zaman, para ve stres kaybını önlemek açısından çok daha etkilidir.

DERSİN TÜRÜ:

Derse Genel Bakış

IGünümüz dijital dünyasında, siber güvenliğin temellerini anlamak artık bir seçenek değil, bir zorunluluktur.

Bu ders, sizi siber güvenliğin temel ilkeleri, yaygın tehditler ve çevrim içi güvenliği artırmanın pratik yolları ile tanıştırır. Kişisel ve profesyonel dijital varlıkları nasıl koruyacağımızı birlikte keşfedecek; siber farkındalık ve dayanıklılık kültürünü nasıl geliştirebileceğimizi inceleyeceğiz.

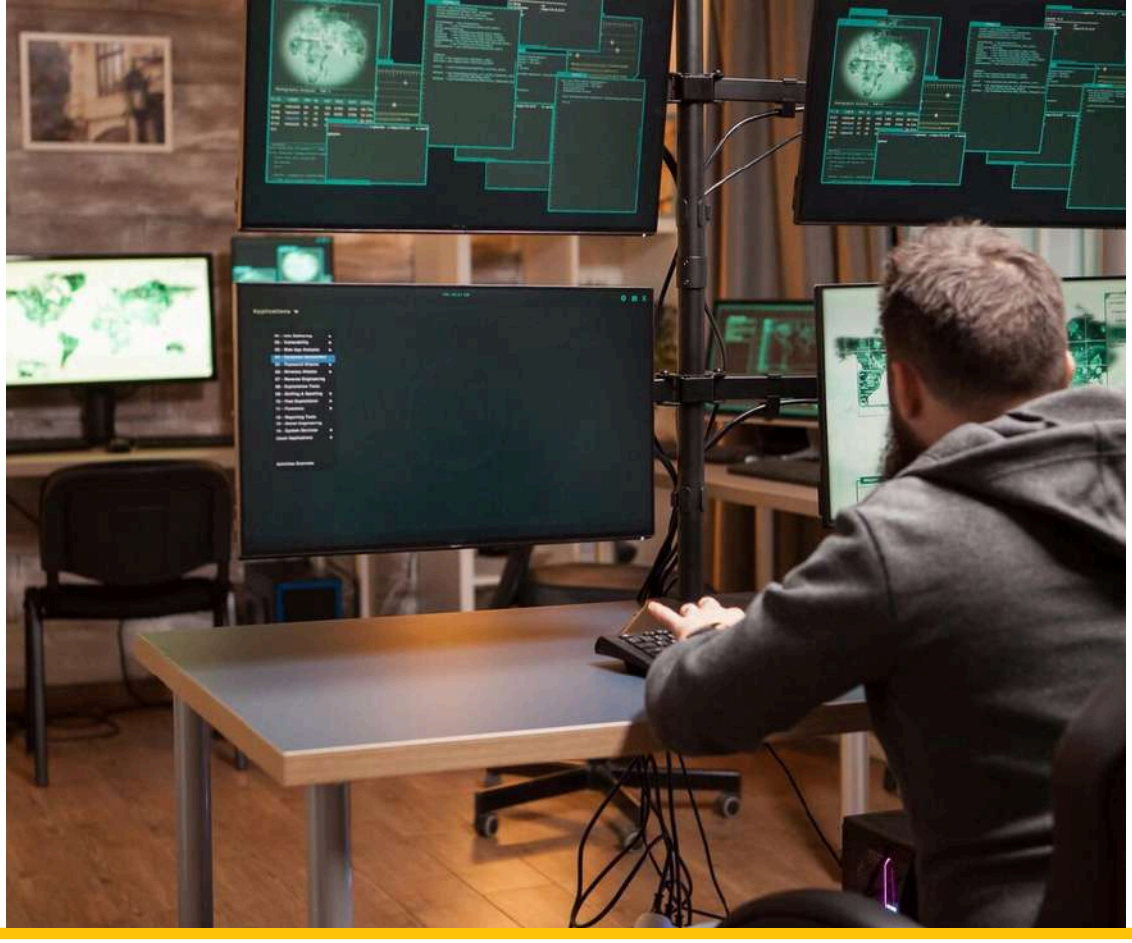
Atölye çalışması 4 adımdan oluşur:

1: Siber güvenlik temellerine giriş (15 dakika)

2: Yaygın siber tehditlerin tanımlanması (10 dakika)

3: Siber güvenlik için en iyi uygulama stratejileri (10 dakika)

4: Kapanış değerlendirmesi ve temel çıkarımlar (5 dakika)



1 Adım

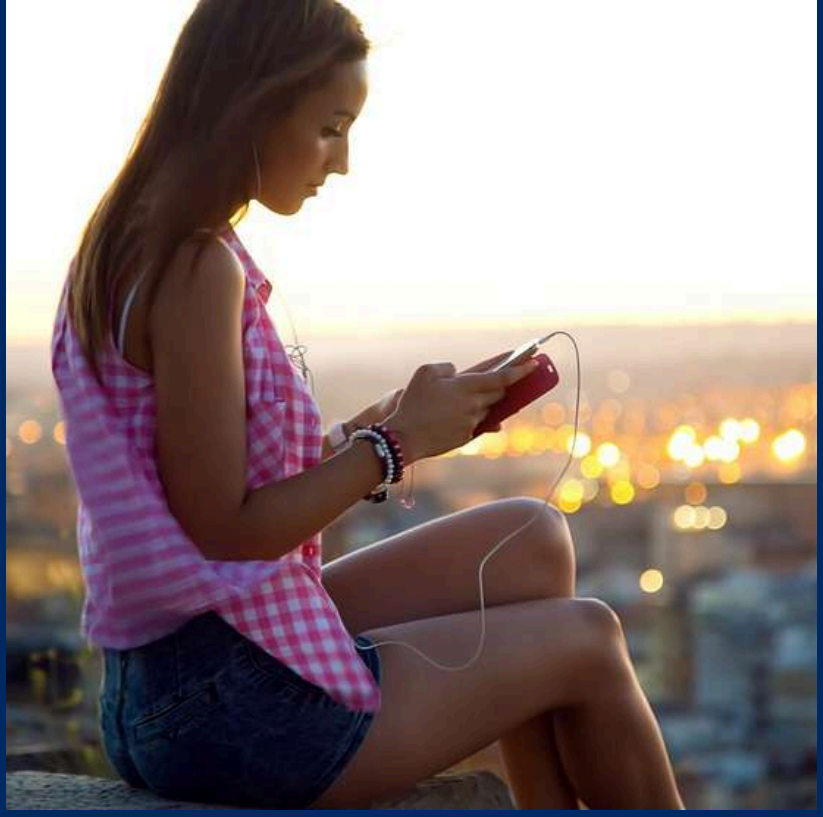
Siber güvenlik temellerine giriş

Siber güvenlik kavramını tanıtan kısa bir video ile başlayalım. Günlük yaşamımızda sürekli dijital araçlar kullanıyoruz, ancak bu araçların güvenliğini ne sıklıkla düşünüyoruz? Siber güvenlik, dijital dünyada kendimizi ve kişisel bilgilerimizi güvende tutmak için hayati öneme sahiptir. Bugün, siber güvenliğin temellerine dalacağız ve neden bu kadar önemli olduğunu keşfedeceğiz.

Haydi birlikte bu videoyu izleyelim:

Şimdi videoyu izlediğimize göre, birlikte tartışalım:

- Videoda siber güvenlikle ilgili olarak dikkatinizi çeken ne oldu?
- Sizce siber güvenlik neden günlük hayatımızda bu kadar önemli?



1 Adım

Siber güvenlik temellerine giriş

Siber güvenlik yalnızca sistemleri korumakla ilgili değildir; aynı zamanda çevrim içi davranışlarımızı anlamakla da ilgilidir. Dijital araçlarla nasıl etkileşim kurduğumuz, güvenliğimizi güçlendirebilir ya da tehditlere karşı savunmasız bırakabilir.

Şimdi dijital yaşamınızı düşünme zamanı.

Aşağıdaki sorulara yanıtlarınızı yazın:

- Çevrim içi faaliyetlerinizin güvenliği hakkında ne sıklıkla düşünüyorsunuz?
- Kişisel bilgilerinizi riske atabilecek herhangi bir alışkanlığınızı tanımlayabilir misiniz?

Düşüncelerinizi paylaşmaya hazır olun!

2 Adım

Yaygın siber tehditlerin belirlenmesi

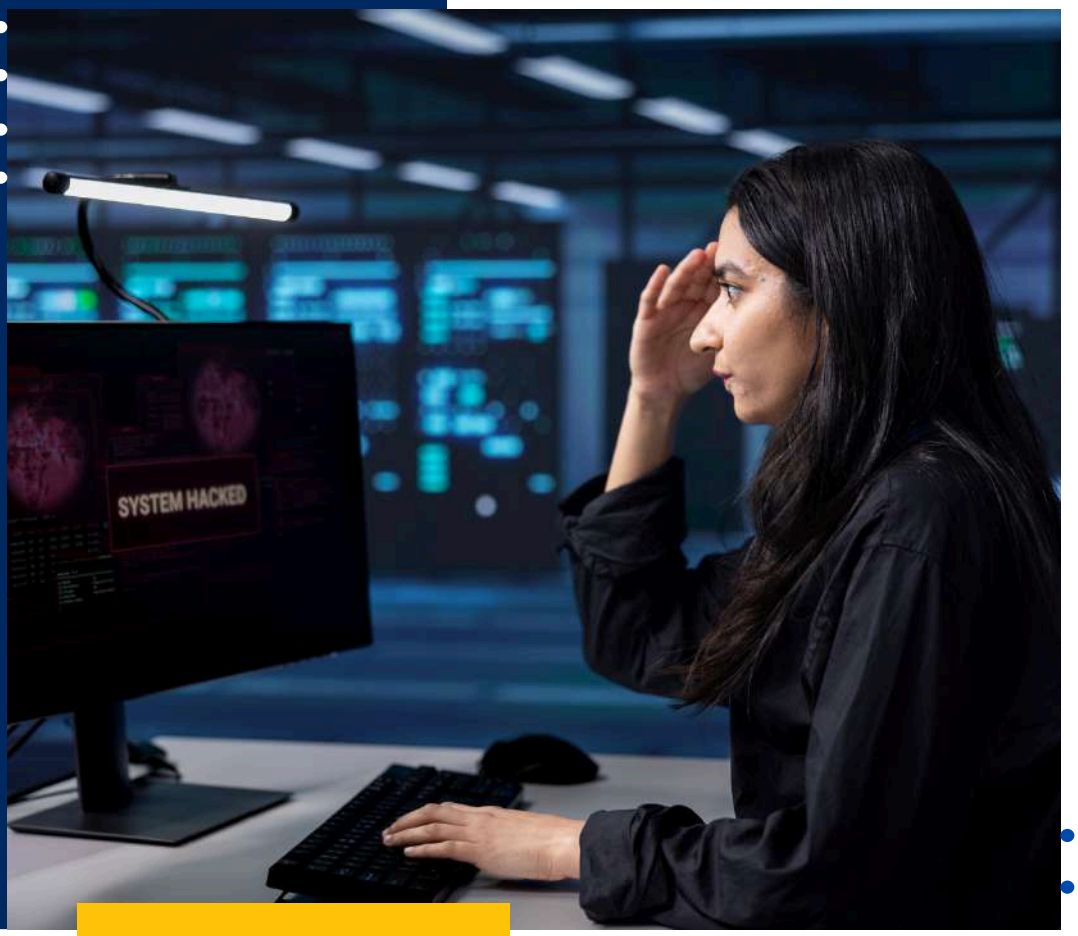
Siber tehdit türlerine daha yakından bakalım.

İnternet, sayısız fırsatla dolu geniş bir alan olsa da, beraberinde riskleri de getirir. Siber tehditler, kim olursak olalım ve nerede bulunursak bulunalım hepimizi hedef alabilir. Bu nedenle, bu tehditlerin doğasını ve etkilerini anlamak son derece önemlidir. Bu adımda, çeşitli siber tehdit türlerini ve üzerimizde nasıl etkili olabileceklerini inceleyeceğiz.

Makaleyi okuyun: IBM – Siber Tehdit Türleri

Makale şu noktaları vurgulamaktadır:

- Kimlik avı (phishing), fidye yazılımı (ransomware) ve kötü amaçlı yazılım (malware) gibi çeşitli siber tehdit türleri.
- Bu tehditlerin nasıl çalıştığı ve kimleri hedef aldığı.
- Bu tehditlerin yol açabileceği zararlarla ilgili örnekler.



2 Adım

Yaygın siber tehditlerin belirlenmesi

Makaleyi okuduktan sonra aşağıdakileri düşünün:

1. Sizi en çok endişelendiren siber tehdit türü hangisiydi ve neden?
2. Siz ya da tanıdığınız biri bu tehditlerden herhangi birini yaşadı mı?
3. Bu tehditleri anlamanın, onları önlemede nasıl yardımcı olabileceğini düşünüyorsunuz?

Ardından, makalede bahsedilen siber tehditlerden birinin gerçekleşebileceği gerçek hayattan bir örnek ya da senaryo yazın.

Örneğinizi paylaşmaya ve grup ile tartışmaya hazır olun!

3 Adım

Siber güvenlik iyi uygulamalarına yönelik stratejiler

Şimdi, çevrim içi ortamda kendimizi korumaya odaklanalım.

Siber tehditler sürekli gelişiyor olsa da, bilgilerimizi korumak ve güvenliği sürdürmek için atabileceğimiz basit ve etkili adımlar vardır. Siber güvenlik en iyi uygulamalarını benimseyerek, riskleri en aza indirebilir ve dijital hayatımızda daha güvende kalabiliriz.

Siber güvenlik, ileri düzey teknik beceriler gerektirmez küçük ama bilinçli eylemler, sizi ve verilerinizi korumada büyük fark yaratabilir.

3 Adım

Siber güvenlik iyi uygulamalarına yönelik stratejiler

Dikkate almanız gereken bazı temel uygulamalar:

- Güçlü, benzersiz parolalar oluşturun ve bunları düzenli olarak değiştirin.
- Ek güvenlik için çok faktörlü kimlik doğrulama (MFA) özelliğini etkinleştirin.
- Özellikle bilinmeyen kaynaklardan gelen bağlantılara ve ek dosyalara karşı dikkatli olun.
- Güvenlik açıklarını kapatmak için yazılım ve cihazlarınızı güncel tutun.
- Güvenli Wi-Fi bağlantıları kullanın; mümkün olduğunca halka açık ağlardan kaçının.

Etkinlik: Siber Güvenlik En İyi Uygulamalar Kontrol Listesi

1. Adım: Mevcut alışkanlıklarınızı değerlendirin

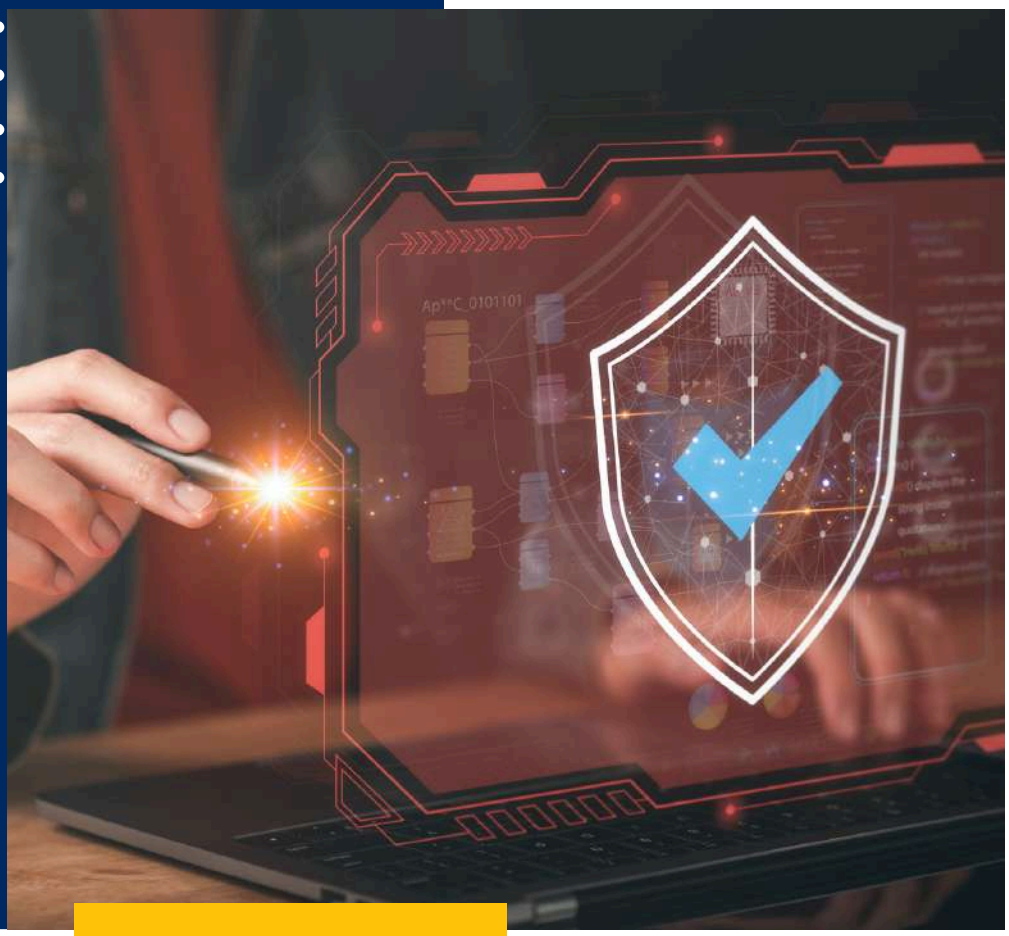
- Mevcut çevrim içi davranışlarınızı ve alışkanlıklarınızı düşünün. Kendinizi riske atabileceğiniz alanlar var mı?

Örnek: “Aynı parolayı birden fazla hesapta kullanıyorum.”

2. Adım: Bir plan oluşturun

- Aşağıda yer alan her bir temel kavram için uygulanabilir bir adım yazın.

Güçlü parolalar: “Güvenli parolalar oluşturmak ve saklamak için bir parola yöneticisi kuracağım.” vb.



3 Adım

Siber güvenlik iyi uygulamalarına yönelik stratejiler

3. Adım: Grup Paylaşımı

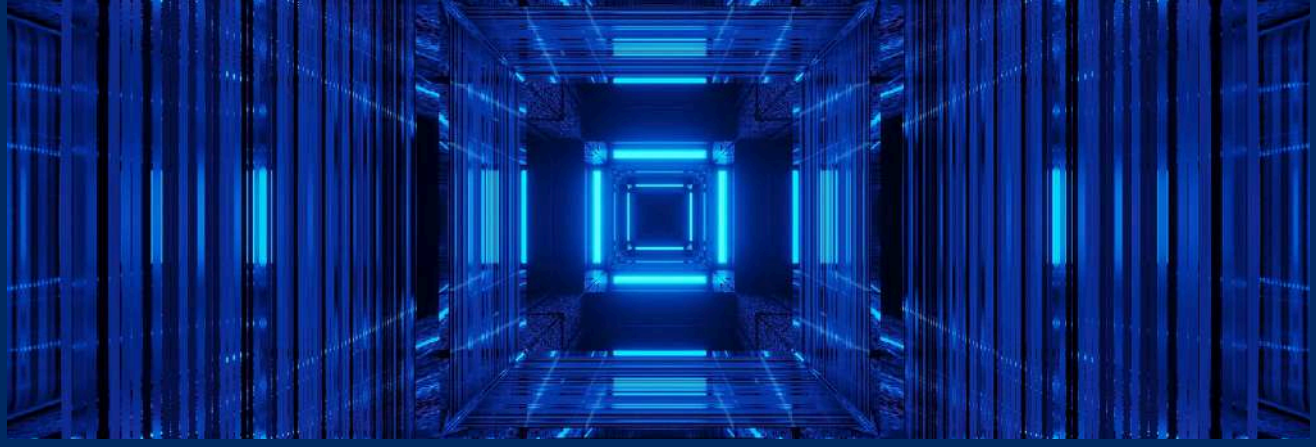
- Hazırladığınız eylem planlarından birini bir arkadaşınızla veya grupla paylaşın.
- Bu adımların dijital güvenliğinizi nasıl geliştirebileceğini tartışın.
- Diğer katılımcıların alabileceği ek önlemler için ipuçları veya öneriler sunun.

En sonunda, aşağıdaki **temel yansıtma** sorusunu zihninizde düşünerek yanıtlayın:

- Bugün çevrim içi güvenliğinizi hemen artırmak için uygulamaya başlayabileceğiniz bir alışkanlık ya da strateji nedir?

4 Adım Kapanış değerlendirmesi ve temel çıkarımlar

Dersimizi tamamlarken, bugün ele aldığımız her şeyi gözden geçirmek ve bu bilgileri ileriye dönük nasıl kullanabileceğimizi düşünmek için kısa bir zaman ayıralım.
Çevrim içi alışkanlıklarınızı düşünün bugünkü tartışmalardan sonra değiştirmek istediğiniz herhangi bir şey var mı?
Varsa, siber güvenliğinizi artırmak için ilk atacağınız adım ne olacak?
Şimdi başkalarına nasıl yardımcı olabileceğimizi düşünelim.
Bu atölyeden öğrendiğiniz ve bir arkadaşınızla ya da meslektaşınızla paylaşabileceğiniz basit bir ipucu ya da alışkanlık nedir?
Bugünkü etkin katılımınız ve değerli katkılarınız için hepinize çok teşekkür ederim!



Temel Çıkarım Özeti

- **Siber güvenlik herkes içindir. Tehditleri anlamak ve en iyi uygulamaları benimsemek, çevrim içi ortamda güvende kalmamıza yardımcı olur.**
- **Küçük adımlar büyük fark yaratır. Parola yöneticileri ve düzenli güncellemeler gibi araçlar, güvenliğinizi önemli ölçüde artırabilir.**
- **Bilgili olun. Siber tehditler sürekli gelişir, bu nedenle en güncel ipuçları ve araçlar hakkında bilgi sahibi olmak, uzun vadeli güvenlik için önemlidir.**
- **Proaktif olun. Güvenli alışkanlıklar edinmek, sizi ve çevrenizdekileri daha güvende tutar.**

Gençlik çalışanları, eğitimciler ve öğretmenlere yönelik yönergeler

Hedef:

Bu ders, gençlik çalışanları, eğitimciler ve öğretmenlerin gençleri temel siber güvenlik bilgileriyle donatmalarına yardımcı olmayı hedefler. Katılımcılar, etkileşimli tartışmalar, etkinlikler ve yansıtma yoluyla yaygın siber tehditleri anlayacak, çevrim içi güvenlik için en iyi uygulamaları öğrenecek ve dijital dünyada kendilerini korumaya yönelik uygulanabilir planlar oluşturacaklardır.

Gerekli Malzemeler:

- Video izleme veya makale okumak için internet bağlantısı
- Projektör ve perde
- Hoparlör
- Önerilen siber güvenlik araçlarına erişim
- Şema kâğıdı veya beyaz tahta ve tahta kalemleri
- Kalemler
- Kâğıt sayfalar

1. Adım: Siber Güvenliğe Giriş (15 dakika)

1. Katılımcıları günlük yaşamdan bir örnekle sürece dahil edin:
2. “En son yeni bir uygulama kullandığınızda ya da bir web sitesine girdiğinizde, verilerinizin ne kadar güvende olduğunu düşündünüz mü?”
3. Siber güvenliğin önemini vurgulayın: Siber güvenliğin sadece bilişim uzmanları için değil, dijital çağda herkes için gerekli bir beceri olduğunu açıklayın. Kişisel, profesyonel ve kurumsal bilgileri korumak için siber güvenliğin temel bir ihtiyaç olduğunu belirtin. Oturumun hedeflerini açıkça paylaşın.
4. **Etkinlik: Video izleme ve tartışma**

- “Siber Güvenlik Nedir?” başlıklı videoyu oynatın.
- İzleme sonrasında tartışmayı yönlendirecek bazı soruları katılımcılarla paylaşın.

5. **Video sonrası tartışma:**
   - “Siber güvenlikle ilgili sizi en çok ne şaşırttı?”
   - “Sizce siber güvenlik herkes için önemli mi? Neden?”
   - “Çevrim içi güvenliğe dikkat etmemek hangi riskleri beraberinde getirir?”

1. Adım: Siber Güvenliğe Giriş (15 dakika)

6. Kişisel düşünme etkinliği:

- Katılımcılardan aşağıdaki sorular üzerinde birkaç dakika düşünmelerini ve cevaplarını yazmalarını isteyin:
- “Çevrim içi faaliyetlerinizin güvenliğini ne sıklıkla düşünüyorsunuz?”
- “Kişisel bilgilerinizin risk altında olmasına neden olabilecek bir veya iki alışkanlığınızı belirleyebilir misiniz?”
- “Çevrim içi güvenliğinizi artırmak için hangi değişiklikleri yapabileceğinizi düşünüyorsunuz?”

7. İkili ya da küçük grup paylaşımları yapmalarını teşvik edin:

- Seçenek 1: Riskli olduğunu düşündüğünüz bir alışkanlığı paylaşın ve grubunuzdan bunu nasıl geliştirebileceğiniz konusunda öneri alın.
- Seçenek 2: Daha önce yaşadığınız veya duyduğunuz bir siber tehdit durumunu ve bu durumun nasıl yönetildiğini tartışın.

8. Grup paylaşımı yapmak istemeyen katılımcılar için:

Çevrim içi güvenliklerini artırmak adına yapmayı taahhüt ettikleri bir değişikliği yazmalarını ve bu notu daha sonra tartışılmak üzere isimsiz olarak kolaylaştırıcıya teslim etmelerini sağlayın.

2. Adım: Yaygın Siber Tehditlerin Belirlenmesi (10 dakika)

1. Katılımcılarla IBM: Siber Tehdit Türleri başlıklı makaleyi ya da önemli noktalarının yazılı bir özetini paylaşın.
2. Katılımcılara, tehditlerin nasıl işlediği ve potansiyel etkileri üzerine düşünerek, en endişe verici buldukları tehditleri not almaları için 5 dakika süre verin.
3. **Grup Tartışması:**

Aşağıdaki sorularla grup içinde bir tartışmayı kolaylaştırın:

- "Hangi siber tehdit size en endişe verici geliyor ve neden?"
- "Siz ya da tanıdığınız biri bu tehditlerden birini yaşadı mı? Neler oldu?"

4. **Tartışmayı Zenginleştirme (Gerekirse):**

Kimlik avı e-postaları veya fidye yazılımı saldırıları gibi örnekler ya da istatistiklerle tartışmaya katkı sağlayın.

5. **Senaryo Etkinliği:**

Katılımcılardan aşağıdakilere benzer şekilde, gerçek ya da hayali bir siber tehdit senaryosu yazmalarını isteyin:

- Kimlik Avı: "Sahte bir e-posta, birini hesap giriş bilgilerini paylaşmaya ikna etti."
- Zararlı Yazılım: "Şüpheli bir bağlantıya tıklamak kötü amaçlı bir yazılım indirdi ve dosyalar kilitlendi."

6. **Senaryoların Paylaşımı ve Tartışma:**

Her katılımcının senaryosunu grup içinde paylaşmasını sağlayın ve şu sorular etrafında tartışmayı yönetin:

- "Senaryoda ne yanlış gitti?"
- "Bu durum nasıl önlenebilirdi?"
- "Hangi önleyici tedbirler yardımcı olurdu?"

7. İsteğe bağlı olarak her siber tehdit türü için gerçek dünyadan alınmış etkili önleyici stratejileri vurgulayarak tartışmayı derinleştirin.

3 Adım: Siber Güvenlik İçin İyi Uygulama Stratejileri (10 dakika)

1. **İyi uygulamalara genel bakış:**

- Basit ve etkili stratejileri sunun:
- Güçlü ve benzersiz parolalar kullanın.
- Çok faktörlü kimlik doğrulama (MFA) etkinleştirin.
- Şüpheli bağlantılardan ve eklerden kaçının.
- Yazılımları ve cihazları güncel tutun.
- Güvenli Wi-Fi veya bir VPN kullanın.
- Her stratejinin etkisini göstermek için gerçek hayat örnekleri veya kısa demonstrasyonlar kullanın.

2. Mümkünse, ilgili "Araçlar" bölümünde yer alan bir aracı kurma veya kullanma sürecini gösterin ya da açıklayın, böylece katılımcılarla ilişkilendirilebilir hale getirin.

3. **Etkinlik: Siber güvenlik kontrol listesi:**

- Stratejilerin listelendiği basit bir kontrol listesi şablonu dağıtın.
- Katılımcılardan her madde için uygulanabilir bir adım yazmalarını isteyin.
- Örnek: "E-posta hesabımda MFA'yı etkinleştireceğim."
- Katılımcıları, basit ve hemen uygulanabilir adımlara odaklanmaya teşvik edin ve gerektiğinde adımları netleştirmelerine yardımcı olun.

4. **Grup paylaşımı:**

- Katılımcılar planladıkları bir adımı paylaşsın.
- Hızlı geri bildirim verin ve bu değişikliklerin faydaları hakkında tartışmaları teşvik edin.
- Katılımcıları, alışkanlıklarını güncellemek için kontrol listelerini düzenli olarak gözden geçirmeye teşvik edin.

4. Adım: Kapanış Yansıtması ve Temel Çıkarımlar (5 dakika)

1. Öğrenilen bilgileri pekiştirin ve katılımcıları öğrendiklerini uygulamaya teşvik edin.
2. Katılımcılara şu soruları yöneltin:

- "Bugünden itibaren değiştirmeyi ya da benimsemeyi planladığınız bir alışkanlık nedir?"
- "Bugün öğrendiklerinizi başkalarıyla nasıl paylaşacaksınız?"

3. Grup paylaşımı:

- Gönüllüleri, düşüncelerini veya önemli bir çıkarımlarını paylaşmaya davet edin.

4. Kapanış mesajı:

- Katılımcılara hatırlatın: "Siber güvenlik herkesin sorumluluğudur. Küçük ama bilinçli adımlar, çevrim içi ortamda güvende kalmak için büyük fark yaratır."
- Tüm katılımcılara aktif katılımları için teşekkür edin ve hemen harekete geçmeleri için cesaretlendirin.

Temel Çıkarımlar:

Katılımcılara, teknik uzmanlık düzeyi ne olursa olsun siber güvenliğin herkesin ihtiyaç duyduğu bir beceri olduğunu vurgulayın. Dersin temel noktalarını kullanarak, yaygın tehditleri anlamanın ve güçlü parolalar kullanmak ya da MFA (çok faktörlü kimlik doğrulama) etkinleştirmek gibi önleyici adımlar atmanın çevrim içi riskleri önemli ölçüde azaltabileceğini belirtin. Katılımcıları, çevrim içi alışkanlıklarını iyileştirmek için basit ve ulaşılabilir hedefler koyarak proaktif bir zihniyet benimsemeye teşvik edin. Bu çıkarımları, sonraki tartışmalar veya bu kavramları yeniden ele alan etkinliklerle pekiştirerek, katılımcıların dikkatli kalmalarını ve güçlü siber güvenlik uygulamalarını sürdürmelerini sağlayın.

Takip ve Evde Yapılacak Etkinlikler

Katılımcıları, öğrendiklerini uygulamaya koymaları için önümüzdeki hafta boyunca çevrim içi aktivitelerini takip etmeye teşvik edin. Kendilerini en savunmasız hissettikleri alanları belirleyebilir ve her gün yeni bir siber güvenlik stratejisini uygulamaya alabilirler. Ayrıca, evde LastPass veya Bitdefender gibi araçları denemelerini ve bir sonraki oturumda deneyimlerini grupla paylaşmalarını önerin.

Eğiticiler İçin İpuçları:
Siber güvenlik konularını, öğrencilerin deneyimlerine hitap eden gerçek hayat örnekleri üzerinden günlük konuşmalara veya ders içeriklerine entegre edin; örneğin sosyal medya güvenliği ya da yaygın dolandırıcılık yöntemleri gibi. Konuyu ilgi çekici ve uygulanabilir hâle getirmek için grup tartışmaları veya canlandırma (rol yapma) gibi etkileşimli yöntemler kullanın. Düzenli olarak ilerlemeyi kontrol edin ve güçlü siber güvenlik alışkanlıkları oluşturmanın önemini pekiştirmek için destek sağlayın.

Araçlar

LastPass

LastPass, tüm çevrimiçi hesaplar için güçlü, benzersiz şifreler oluşturup güvenli bir şekilde saklayarak siber güvenliği artırmak üzere tasarlanmış güçlü bir şifre yönetimi aracıdır. Birden fazla karmaşık parolayı, yalnızca ana parolayla erişilebilen şifrelenmiş bir dijital kasada saklayarak hatırlama ihtiyacını ortadan kaldırır.

www.lastpass.com

Bitdefender

Bitdefender, kötü amaçlı yazılım, kimlik avı, fidye yazılımı ve diğer çevrimiçi tehditlere karşı kapsamlı koruma sunan gelişmiş bir siber güvenlik aracıdır. Kişisel ve profesyonel kullanım için çok katmanlı güvenlik sağlamak amacıyla güçlü antivirüs yazılımını akıllı kimlik avı önleme önlemleriyle birleştirir.

www.bitdefender.com

Kaynakça

- Bitdefender. (n.d.). Retrieved from https://www.bitdefender.com
- Cisco Networking Academy. (n.d.). Cybersecurity Essentials. Cisco Networking Academy: Learn Cybersecurity, Python & More. Retrieved from https://www.netacad.com/courses/cybersecurity-essentials?courseLang=en-US
- IBM. (2024, March 25). Types of cyberthreats. Retrieved from https://www.ibm.com/think/topics/cyberthreats-types
- Lakhwani, S. (2024, June 19). Fundamentals of Cybersecurity [2024 Beginner's Guide]. upGrad KnowledgeHut Blog. Retrieved from https://www.knowledgehut.com/blog/security/cyber-security-fundamentals
- LastPass. (n.d.). Retrieved from https://www.lastpass.com
- Simplilearn. (2020, June 10). What Is Cyber Security | How It Works? | Cyber Security In 7 Minutes | Cyber Security | Simplilearn. [Video]. YouTube. https://youtu.be/inWWhr5tnEA?si=3XP97c0H4JmHxWSo

SINAV

1. Siber güvenliğin temel amaçlarından biri nedir?

A. Kimsenin izinsiz olarak internete erişememesini sağlamak
B. İşletmelerin kullanıcı etkinliklerini izlemesine izin vermek
C. Dijital varlıkları risk ve güvenlik açıklarını yöneterek korumak
D. Bilinmeyen gönderenlerden gelen tüm e-postaları engellemek

2. Aşağıdakilerden hangisi çok faktörlü kimlik doğrulama (MFA) kullanımını gösterir?

A. Bir güvenlik sorusunu yanıtlayarak giriş yapmak
B. E-posta şifresi ve yedek e-posta kullanarak hesap kurtarmak
C. Şifreyle birlikte telefona gönderilen geçici bir kodu kullanmak
D. Şifreleri bilgisayarda şifrelenmiş bir dosyada saklamak

3. Kimlik avı , diğer çevrim içi tehditlerden hangi yönüyle ayrılır?

A. Kullanıcının etkileşimi olmadan sistemlere doğrudan sızma içerir
B. Kullanıcıları hassas bilgileri paylaşmaları için kandıran aldatıcı taktikler kullanır
C. USB gibi fiziksel cihazlar yoluyla yayılır
D. Sadece bilgisayara kötü amaçlı yazılım yükleyerek çalışır

SINAV

4. Yazılımınızı güncellemek siber güvenliği nasıl artırır?
A. Uygulamalarınızın tasarımını ve kullanılabilirliğini geliştirir
B. Görevlerinizi engelleyebilecek hataların olasılığını azaltır
C. Saldırganların kullanabileceği güvenlik açıklarını kapatır
D. Daha eski donanımlarla daha iyi uyumluluk sağlar

5. Şifre yöneticisi kullanmak neden faydalıdır?
A. Tüm şifrelerinizin paylaşılan bir sunucuda yedeklenmesini sağlar
B. Belirli bir süreden sonra sizi hesaplardan otomatik olarak çıkarır
C. Her hesap için karmaşık şifreler oluşturur ve güvenli şekilde saklar
D. Birisi e-postanıza eriştiğinde size uyarı gönderir

Cevaplar

Soru 1: C
Soru 2: A
Soru 3: B
Soru 4: B
Soru 5: A

ERASMEDIAH

Educational Reinforcement Against the Social Media Hyperconnectivity

Lélekben Otthon Közhasznú Alapítvány

AdM Archivio della Memoria

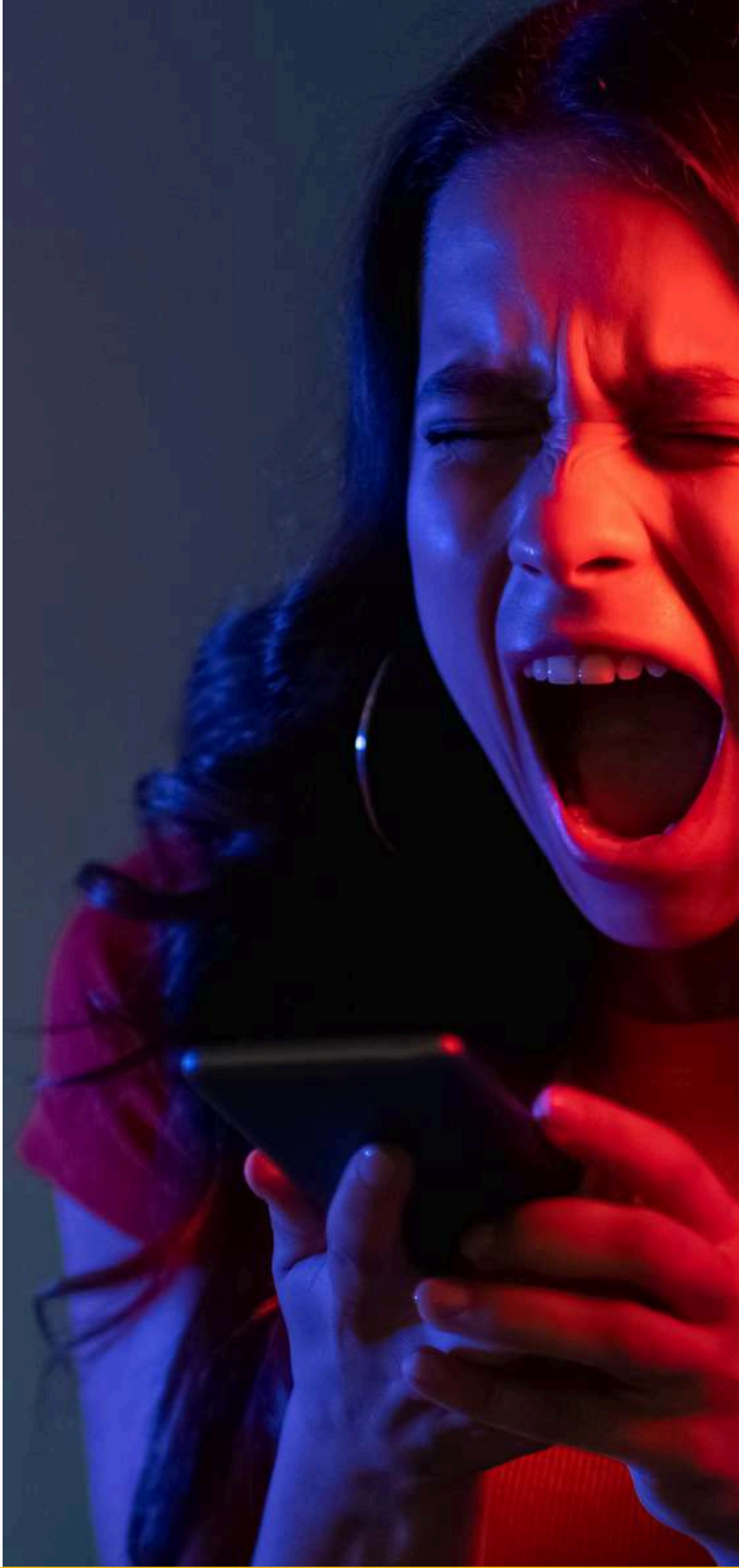
LABC

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.