



MODÜL 5

SİBER GÜVENLİK VE ÇEVİRİMİÇİ

GÜVENLİK



erasmediah.eu



**Co-funded by
the European Union**



Ders 5.2

Kişisel Bilgilerin ve Çevrimiçi Gizliliğin Korunması



ERASMEDIAH

Educational Reinforcement Against
the Social Media Hyperconnectivity



**Co-funded by
the European Union**

Ders 5.2

Kişisel Bilgilerin ve Çevrimiçi Gizliliğin Korunması

Hedefler:

- Kişisel bilgilerin çevrimiçi ortamda paylaşılmasının riskleri ve bu bilgilerin nasıl kötüye kullanılabileceği konusunda farkındalık oluşturmak.
- Veri gizliliği ayarları, güvenli iletişim ve aşırı paylaşımın önlenmesi gibi uygulamalı stratejilerle öğrenenleri dijital ayak izlerini kontrol altına alma konusunda donatmak.
- Bireyleri etkileyen gizlilik ihlali örneklerini inceleyerek, bu durumların etkilerini göstermek ve nasıl önlenebileceğini tartışmak.
- Uygulama izinlerini gözden geçirme, hizmet şartlarını anlama ve gizlilik araçlarını kullanma gibi alışkanlıklar kazandırarak proaktif davranışları teşvik etmek.

Temel Mesaj(lar):

- İnternette paylaştığınız her bilgi, fotoğraflar ve beğenilerden konum verilerine kadar siber suçlular veya şirketler tarafından kötüye kullanılabilir. Erişimi sınırlamayı bilmek ilk savunma hattınızdır.
- Gizliliğinizi korumak, internetten uzak durmak anlamına gelmez; akıllı ve bilinçli hareket etmek anlamına gelir. Basit araçlar ve bilinçli kararlar, dijital hayatınızdan ödün vermeden verilerinizi korumanıza yardımcı olur.



DERSİN TÜRÜ:



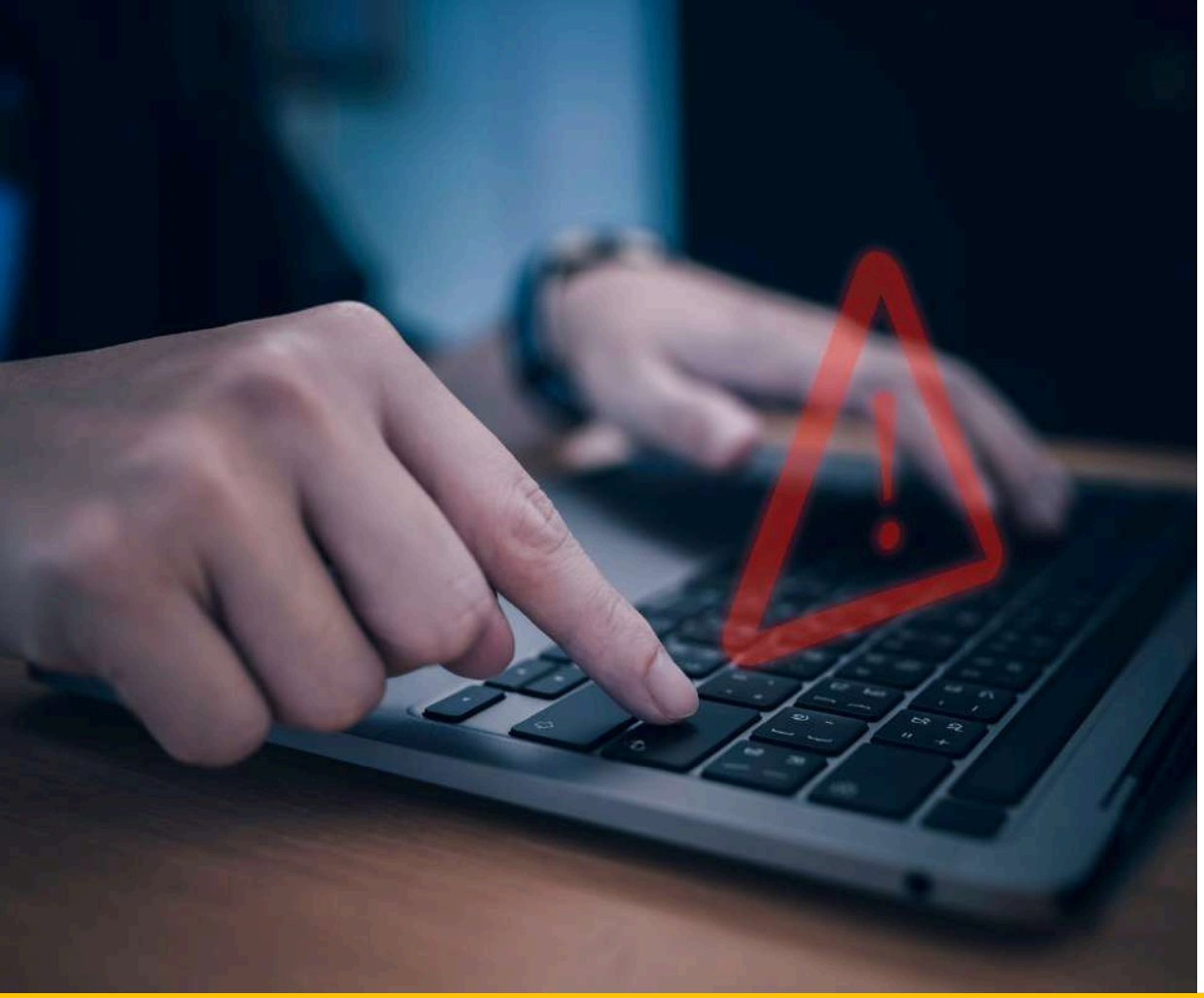


Derse Genel Bakış

Günümüzde yaşamımızın büyük bir kısmı çevrimiçi olarak gerçekleştiği için kişisel bilgileri güvende tutmak her zamankinden daha önemli hâle geldi. Bu ders, gizliliğinizi korumanın neden önemli olduğunu vurgular. Sosyal medyada fazlaca bilgi paylaşmak ya da düşünmeden uygulama izinlerini kabul etmek gibi basit alışkanlıkların verilerinizi nasıl savunmasız bırakabileceğini birlikte inceleyeceğiz. Bu riskleri fark ederek ve uygulanabilir stratejiler geliştirerek, dijital kimliğinizi korumanıza ve çevrimiçi güvenliğinizi kontrol altına almanıza yardımcı olacak araçları kazanacaksınız.

Atölye çalışması 4 adımda yapılandırılmıştır:

- 1: Çevrimiçi gizlilik risklerine giriş (15 dakika)
- 2: Gerçek dünya gizlilik ihlallerini keşfetme (10 dakika)
- 3: Kişisel bilgileri korumaya yönelik pratik stratejiler (10 dakika)
- 4: Kapanış, yansıtma ve temel çıkarımlar (5 dakika)



1 Ders

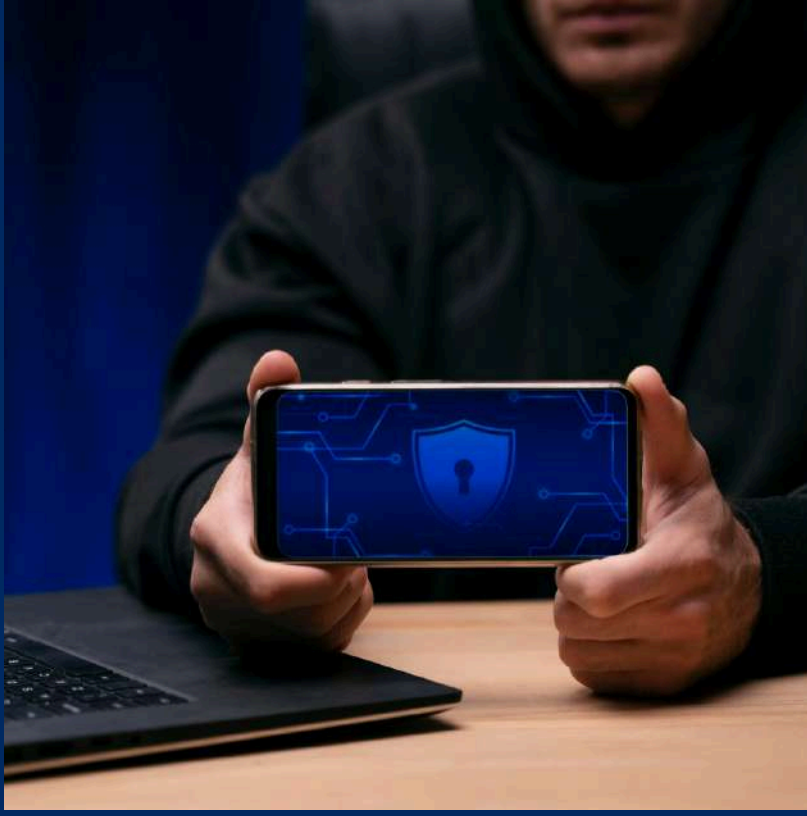
Çevrimiçi gizlilik risklerine giriş

Hiç yeni bir uygulama indirip, izinlerini kabul ettiniz ve sonra bu uygulamanın hangi bilgileri topladığını düşünmediniz mi? İnterneti kullandığımızda, konumumuz, şifrelerimiz ve gezinme alışkanlıklarımız gibi kişisel verilerimiz kolayca açığa çıkabilir. Şimdi, hangi gizlilik risklerinin var olduğunu ve bunların sizi nasıl etkileyebileceğini keşfedeceğiz.

İlk adım olarak, şu makaleden **“Yaygın Çevrimiçi Gizlilik Tehditleri”** bölümünü okuyun: builtin.com/articles

Okurken, bir kâğıda birkaç kelimeyle şunları yazın:

- Sizi en çok rahatsız eden gizlilik tehdidi nedir?
- Bu tehdit neden size çarpıcı ya da tehlikeli görünüyor?



1 Adım

Çevrimiçi gizlilik risklerine giriş

Okumayı bitirdikten sonra gelin birlikte tartışalım:

- Sizi en çok şaşırtan gizlilik tehdidi hangisiydi ve neden?
- Bu tehditlerin günlük yaşantımızı nasıl etkilediğini düşünüyorsunuz?
- Bu tehditleri görmezden gelirsek ne gibi sonuçlarla karşılaşabiliriz?
-

Deneyiminizden kısa bir örnek paylaşabilirsiniz zayıf şifreler, veri takibi veya gördüğünüz ya da duyduğunuz başka bir durum olabilir. Emin değilseniz sadece diğerlerini dinlemek bile size fikir verecektir!



2 Adım

Gerçek dünyadaki gizlilik ihlallerini keşfetme

Haydi, kişisel bilgilerimizi çevrimiçi ortamda dikkatsizce paylaştığımızda neler olabileceğine dair gerçek bir örneğe bakalım.

Hayal edin: Sarah sosyal medyada hayatını paylaşmayı çok seviyor. Yeni dairesinden fotoğraflar paylaşıyor, günlük rutinlerinden bahsediyor ve favori kafesindeyken konumunu bile bildiriyor. Bir gün, Sarah banka hesabının boşaltıldığını fark ediyor. Peki nasıl? Bir siber suçlu, Sarah'nın herkese açık gönderilerinden kişisel bilgilerini konumu, yaşam tarzı alışkanlıkları ve hatta şifrelerine dair ipuçları birleştirerek hesaplarına erişiyor. Tüm bunlar, aşırı paylaşım yüzünden oluyor!

Şimdi şu sorular üzerine düşünün:

- Ne yanlış gitti? Hangi davranışlar ya da alışkanlıklar gizlilik ihlaline yol açtı?
- Bu durum nasıl önlenebilirdi? Hangi basit değişiklikler fark yaratırdı?

Yanıtlarınızı bir yere yazın ve grupla paylaşmaya hazır olun.



2 Adım

Gerçek dünyadaki gizlilik ihlallerini keşfetme

Haydi birlikte konuşalım:

- Sizce Sarah'nın yaşadığı durumda ne yanlış gitti?
- Böyle gizlilik ihlalleri sizce neden bu kadar kolay yaşanıyor?

Son olarak, biraz düşünün:

- Siz ya da tanıdığınız biri hiç çevrim içi bir gizlilik sorunu yaşadı mı?
- Bu; şüpheli bir e-posta, ele geçirilmiş bir hesap ya da sosyal medyada aşırı paylaşım olabilir.
- Nasıl gerçekleşti ve sonuç ne oldu?

Kendinizi rahat hissediyorsanız hikayenizi grupta paylaşabilirsiniz. Paylaşmak istemezseniz de sorun değil yalnızca dinlemek bile size değerli fikirler kazandıracaktır.



3 Adım

Kişisel bilgileri korumaya yönelik pratik stratejiler

Şimdi, gizlilik risklerini ve gerçek bir örneği incelediğimize göre, çevrimiçi ortamda kendimizi (verilerimizi) korumak için atabileceğimiz pratik adımlara odaklanalım.

Kısa bir video ile başlayacağız hep birlikte izleyelim:

Paylaşılan temel ipuçlarına dikkat edin.

Videoyu izledikten sonra, çevrimiçi gizliliğinizi artırmak için atabileceğiniz üç somut adımı yazın. Şu konuları düşünün:

- Sosyal medya hesaplarınızın gizlilik ayarlarını düzenlemek.
- Telefonunuzdaki uygulama izinlerini gözden geçirmek.
- Özellikle herkese açık platformlarda hangi kişisel bilgileri paylaştığınıza karşı dikkatli olmak.



3 Adım

Kişisel bilgileri korumaya yönelik pratik stratejiler

Şimdi, uygulamayı planladığınız bir stratejiyi paylaşalım. Örneğin:

- “Bu akşam telefonumdaki tüm uygulamaları gözden geçirip kullanmadıklarımı sileceğim.”
- “Facebook/Instagram gönderilerimi kimlerin görebileceğini sınırlayacağım ve profilimin herkese açık görünürliğini kapatacağım.”

Haydi tartışalım:

1.Bu gizlilik alışkanlıklarını benimsemek sizce neden kolay veya zor görünüyor?

- İnternette bilgi paylaşma konusunda fazla mı rahatız?
- Gizlilik ayarlarını ve izinlerini karmaşık veya zaman alıcı mı buluyoruz?

2. İnsanlar neden riskleri bilseler bile bu basit gizlilik önlemlerini göz ardı ediyorlar?

- Bu, kendilerine böyle bir ihlalin olmayacağını düşünmelerinden mi kaynaklanıyor?
- Yoksa hangi araçları veya alışkanlıkları kullanmaları gerektiğini bilmemelerinden mi?

3. Bu alışkanlıklara bağlı kalmak için nasıl motive olabilirsiniz?

- Örneğin, şifreleri güncellemek için hatırlatıcılar kurmak veya sosyal medya ayarlarını düzenli olarak gözden geçirmek gibi.

4 Adım

Kapanış deęerlendirmesi ve temel ıkarımlar

Bu atölyeyi sonlandırmadan önce, öğrendiklerimizi gözden geçirip günlük hayatımıza nasıl uygulayabileceğimizi düşünmek için kısa bir yansıma yapalım.

Kendinize şunu sorun: Çevrim içi gizliliğinizi artırmak için bugün deęiştirebileceğiniz bir alışkanlık nedir?

Bu, konum paylaşımını kapatmak, sosyal medya gizlilik ayarlarını kontrol etmek ya da ne paylaştığınıza daha dikkatli olmak gibi basit bir şey olabilir.

Şimdi de başkalarına nasıl yardımcı olabileceğinizi düşünün:

Bugün öğrendiklerinizi bir arkadaşınızla, ailenizden biriyle ya da bir meslektaşınızla nasıl paylaşacaksınız?

Güçlü şifrelerin neden önemli olduğunu anlatmak ya da birine uygulama izinlerini nasıl kontrol edeceğini göstermek gibi küçük ipuçları bile büyük fark yaratabilir.





Temel Çıkarım Özeti

- Çevrim içi paylaşımlarınız konusunda dikkatli olun. Konumlar veya günlük alışkanlıklar gibi küçük detaylar, yanlış kişilerin eline geçerse kötüye kullanılabilir.
- Gizlilik ayarlarınızı gözden geçirin ve düzenleyin. Sosyal medya, uygulama izinleri ve hesap ayarlarınızı düzenli olarak kontrol ederek gereksiz veri paylaşımını sınırlayın.
- Kamusal olarak paylaştığınız kişisel bilgileri sınırlayın. Adres, rutinler veya kişisel tanımlayıcılar gibi hassas bilgileri sosyal medya veya diğer platformlarda paylaşmaktan kaçının.
- Uygulamalar ve bağlantılar konusunda temkinli olun. Bağlantılara tıklamadan, uygulama indirmeden veya izin vermeden önce düşünün yalnızca doğrulanmış kaynaklara güvenin.
- Küçük adımlarla başlayın. Konum takibini kapatmak veya herkese açık paylaşımları sınırlamak gibi basit alışkanlıklar, gizliliğinizi koruma konusunda büyük fark yaratabilir.



Gençlik çalışanları, eğitimciler ve öğretmenlere yönelik yönergeler

Hedef:

Bu dersin amacı, katılımcılara kişisel bilgilerini korumak ve çevrim içi gizliliklerini sürdürmek için pratik beceriler ve bilgiler kazandırmaktır. Etkileşimli etkinlikler, gerçek yaşam örnekleri ve yansıtıcı tartışmalar aracılığıyla katılımcılar, yaygın çevrim içi gizlilik risklerini tanımlayacak, gizlilik ihlallerinin etkileri hakkında farkındalık geliştirecek ve verilerini korumaya yönelik uygulanabilir stratejiler oluşturacaklardır. Oturum sonunda katılımcıların dijital güvenliklerini artırmaya yönelik alışkanlıklar edinme konusunda daha bilinçli, hazırlıklı ve kararlı olmaları hedeflenmektedir.

Gerekli Materyaller:

- Video gösterimi veya makale erişimi için internet bağlantısı
- Projeksiyon cihazı ve ekran
- Hoparlör
- Önerilen siber güvenlik araçlarına erişim
- Büyük boy kağıt veya yazı tahtası ve kalemleri
- Kalemler ve not kâğıtları





1 Adım: Çevrim İçi Gizlilik Risklerine Giriş (15 dakika)

- 1.İlgi çekici bir soruyla başlayın: “En son ne zaman bir uygulama indirdiniz, izinlerini kabul ettiniz ya da çevrim içi bir gönderi paylaştınız? Bu sırada hangi kişisel bilgileri paylaşıyor olabileceğinizi hiç düşündünüz mü?”
2. Katılımcılara, bu gibi günlük eylemlerin farkında olmadan konum, gezinme alışkanlıkları veya kişisel rutinler gibi özel bilgileri üçüncü şahıslara ya da siber suçlulara ifşa edebileceğini açıklayın.
- 3.Kişisel verileri korumanın önemi üzerinde durun: Günümüz dijital dünyasında kişisel verileri korumanın vazgeçilmez olduğunu vurgulayın. Masum görünen davranışların örneğin bir fotoğraf paylaşmak ya da bir uygulamaya kişilerinize erişim izni vermenin beklenmedik sonuçlar doğurabileceğini belirtin. Basit bir benzetme kullanın: “Kişisel bilgileriniz bir yapbozun parçaları gibidir. Tek başına zararsız görünen bir parça, diğerleriyle birleştğinde sizinle ilgili pek çok şeyi ortaya çıkarabilir.”
- 4.Etkinlik – makale okuma ve yansıtma:
5. Katılımcılara "Çevrim İçi Gizliliğin Yaygın Tehditleri" başlıklı makale bölümünü dağıtın veya bağlantı üzerinden paylaşın: [Çevrimiçi Gizlilik Nedir?](#)

Katılımcılardan şunları yapmalarını isteyin:

- En endişe verici buldukları gizlilik tehdidini belirleyin.
- Bu tehdidin neden özellikle tehlikeli veya şaşırtıcı geldiğini düşünün.
- Grup tartışmasına hazırlanmak için kısa notlar alsınlar.





1 Adım: Çevrim İçi Gizlilik Risklerine Giriş (15 dakika)

4. Kısa bir tartışmayı aşağıdaki sorularla yönlendirin:

- “Size en çok hangi gizlilik tehdidi çarpıcı geldi ve neden?”
- “Bu tür riskler çevrim içi davranışlarınızı veya alışkanlıklarınızı nasıl etkiliyor?”

Bazı katılımcıları düşüncelerini paylaşmaya davet edin. Bu paylaşımlar sırasında şu mesajı pekiştirin: Bu risklerin farkında olmak, kişisel bilgileri daha iyi korumanın ilk adımıdır.

5. Kapanış – Tartışmanın temel mesajını özetleyin:

Örneğin:

“Bu gizlilik risklerini fark ederek çevrim içi varlığınız üzerinde kontrol kazanmaya başlıyorsunuz. Farkındalık, neyi paylaşacağınız ve çevrim içi ortamda nasıl etkileşim kuracağınız konusunda daha akıllıca kararlar almanızı sağlar.”





2 Adım: Gerçek dünyadan gizlilik ihlallerini keşfetme (10 dakika)

1. Aşırı paylaşımın çevrim içi ortamda nasıl ciddi gizlilik ihlallerine yol açabileceğini göstermek için katılımcılarla ilişkilendirilebilir ve etkileyici bir senaryo paylaşarak başlayın. Katılımcılara, bu hikâyenin benzersiz olmadığını açıklayın. Pek çok kişi, siber suçluların veya kötü niyetli kişilerin onları takip etmek, hesaplarına sızmak ya da kimliklerini çalmak için kullanabileceği kişisel bilgileri farkında olmadan paylaşır. Gizlilik ihlallerinin genellikle küçük, zararsız gibi görünen bilgi parçalarıyla başladığını vurgulayın.

2. Katılımcılara yazılı kısa bir senaryo gösterin; bu, Sarah'nın hikâyesine dayalı ya da benzer şekilde varsayımsal bir durum olabilir:

Başka bir senaryo örneği:

“Alex, ücretsiz bir mobil uygulama indirdi ancak izinleri okumadı. Uygulama onun konumuna, kişilerine ve medya dosyalarına erişebiliyordu. Kısa bir süre sonra, arkadaşlarına garip mesajlar gönderildiğini fark etti. Uygulama, verilerini topluyor ve hesabını kullanarak spam mesajlar gönderiyordu.”





2 Adım: Gerçek dünyadan gizlilik ihlallerini keşfetme (10 dakika)

3. Katılımcılara talimat verin:

- Durumu analiz etmek için bireysel olarak ya da küçük gruplar hâlinde çalışın.
- Ne yanlış gitti? Bu ihlale neden olan eylemler veya davranışlar nelerdi?
- Bu nasıl önlenebilirdi? Kişisel bilgileri korumak için basit adımları veya alışkanlıkları belirleyin.

Düşüncelerinizi kısaca yazın.

4. Katılımcıların aşağıdaki şekilde düşüncelerini paylaşmalarına izin verin:

- “Sen ya da tanıdığın biri daha önce benzer bir sorunla karşılaştı mı? (örneğin: ortalama, hesap ele geçirme ya da aşırı paylaşım)”
- “İnsanlar neden bu kadar çok kişisel bilgiyi, riskleri düşünmeden paylaşıyor?”

Olası nedenler:

- Uygulamalara veya platformlara güvenmek.
- Sonuçlarının farkında olmamak.
- Gizlilik ayarlarının kafa karıştırıcı olması.

Katılımcıları deneyimlerini veya görüşlerini açık ve destekleyici bir şekilde paylaşmaya teşvik edin.





3 Adım: Kişisel bilgileri korumaya yönelik pratik stratejiler (10 dakika)

1.Video gösterimi

“Kişisel Verilerinizi Çevrim İçi Ortamda Nasıl Korursunuz” başlıklı videoyu izletin. Katılımcılardan videoda paylaşılan pratik ve uygulanabilir stratejilere dikkat etmelerini isteyin. Bu ipuçlarının uygulanmasının kolay olduğunu ama çevrim içi gizliliği önemli ölçüde artırabileceğini vurgulayın.

2. Etkinlik – “Kişisel gizlilik planı”

Katılımcılardan çevrim içi gizliliklerini korumak için alacakları üç önlemleri yazmalarını isteyin. Aşağıdakileri göz önünde bulundurmalarını teşvik edin:

- Sosyal medya gizlilik ayarlarını düzenlemek.
- Cihazlarındaki uygulama izinlerini gözden geçirmek.
- Kamusal alanda ne paylaştıklarına dikkat etmek.

3. Grup içinde paylaşım

Katılımcılardan uygulamayı planladıkları bir adımı grupta paylaşmalarını isteyin. Aşağıdaki soruları tartışmayı yönlendirmek için kullanın:

- “Bugün başlaman en kolay gelen strateji hangisi ve neden?”
- “Bu alışkanlıkları edinmeye çalışırken ne gibi zorluklarla karşılaşabilirsin?”
- “Ayarları değiştirmeyi unutmak veya gizlilik araçlarını karmaşık bulmak gibi yaygın engellerin üstesinden nasıl gelebiliriz?”

Grubu pratik öneriler paylaşmaya veya benzer zorlukları nasıl aştıklarına dair kişisel deneyimlerini aktarmaya teşvik edin. Küçük ama istikrarlı adımların çevrim içi gizliliği önemli ölçüde iyileştirebileceğini vurgulayın.

4. Ayrıca, katılımcılardan bu stratejileri arkadaşları veya aileleriyle nasıl paylaşabileceklerini düşünmelerini isteyebilirsiniz.





4 Adım: Kapanış değerlendirmesi ve temel çıkarımlar

1. Katılımcılardan şu sorular üzerinde düşünmelerini isteyin:

- “Bugünden itibaren çevrim içi gizliliğini geliştirmek için hangi alışkanlığını değiştireceksin?”
- “Bugün öğrendiklerini arkadaşlarıyla veya ailenle nasıl paylaşacaksın?”

2. Dersin ana noktalarını pekiştirin:

- Küçük değişiklikler ayarları düzenlemek veya neyi paylaştığını sınırlamak gibi büyük fark yaratır.
- Verilerini korumak, dijital kimliğin üzerinde kontrol sahibi olmanı sağlar.

3. Oturumu şu gibi bir kapanış cümlesiyle sonlandırın:

- “Kişisel bilgileriniz değerlidir. Onları korumak için küçük ve akıllıca adımlar atın, çevrim içi ortamda daha güvende kalırsınız.”

Temel Çıkarımlar:

Dersin sonunda katılımcılar, çevrim içi gizliliğin farkındalıkla başladığını ve küçük, uygulanabilir adımlarla geliştiğini açıkça anlamış olmalıdır.

Uygulama izinlerini düzenlemek, sosyal medya gizlilik ayarlarını gözden geçirmek ve herkese açık olarak ne paylaşıldığına dikkat etmek gibi basit değişiklikler riskleri önemli ölçüde azaltabilir.

Katılımcıları, verilerine kimin erişimi olduğunu kontrol etmek ve şüpheli bağlantı veya mesajlara karşı dikkatli olmak gibi alışkanlıklar geliştirerek dijital davranışları üzerinde kontrol sahibi olmaya teşvik edin.

Kişisel bilgileri korumanın, bireylere dijital kimliklerini ve güvenliklerini koruma gücü verdiği fikrini pekiştirin.





Takip ve Evde Uygulanacak Etkinlikler

Katılımcılardan, oturum sırasında belirledikleri gizlilik eylemlerinden en az birini önümüzdeki günlerde hayata geçirmeleri istenmelidir. Bu; bir sosyal medya platformunda gizlilik ayarlarını gözden geçirmek, kullanılmayan uygulamaları silmek veya gizlilikle ilgili ipuçlarını arkadaşları ya da aile üyeleriyle paylaşmak gibi eylemleri içerebilir. Katılımcıların ilerlemelerini belgelemeleri ve bu değişikliklerin çevrim içi ortamda kendilerini daha güvende hissettirip hissettirmedikleri üzerine düşünmeleri önerilir. Ayrıca katılımcılar, çevrim içi güvenliklerini kolayca nasıl artıracabileceklerini görmek için DuckDuckGo (özel bir arama motoru) veya Google Gizlilik Kontrolü gibi araçları keşfetmeye teşvik edilmelidir. Katılımcıların deneyimlerini paylaşabilecekleri ve karşılaştıkları zorlukları tartışabilecekleri bir takip oturumu düzenlenmesi de değerlendirilebilir.

Öğretmenler İçin İpuçları:

Çevrim içi gizlilik kavramının anlaşılmasını kolaylaştırmak için tartışmalarda gerçek hayattan örnekler kullanılması önerilir. Aşırı sosyal medya paylaşımı, veri ihlalleri veya uygulama izinleri gibi senaryolar kullanılarak küçük alışkanlıkların nasıl büyük sonuçlar doğurabileceği gösterilmelidir. Katılımcıların yargılanmadan deneyimlerini paylaşabilecekleri destekleyici bir ortam oluşturulmalıdır. Sürekli katılımı sağlamak için derslere kısa, uygulamalı görevler entegre edilmeli; örneğin gizlilik ayarlarının nasıl düzenleneceği veya şüpheli bağlantıların nasıl tanınacağı gösterilmelidir. Konu düzenli olarak yeniden ele alınmalı ve öğrencilere, kişisel bilgilerini korumanın yaşam boyu sürecek bir alışkanlık olduğu farkındalığı kazandırılmalıdır.





Araçlar

DuckDuckGo



DuckDuckGo, arama geçmişinizi izlemeyen veya kişisel veri toplamayan, gizlilik odaklı bir arama motorudur. Aramalarınızın gizli kalmasını sağlar ve gezinirken bıraktığınız dijital ayak izini en aza indirmeye yardımcı olur.

duckduckgo.com

Google Gizlilik Kontrolü



Google Gizlilik Kontrolü, Google hesap ayarlarınızı yönetmenize yardımcı olan yerleşik bir araçtır. Hangi kişisel verilerin toplandığını, etkinliğinizi kimlerin görebileceğini ve hangi uygulamaların bilgilerinize erişebileceğini incelemenize ve ayarlamanıza olanak tanır.

myaccount.google.com/privacycheckup



Kaynakça

- DuckDuckGo (n.d.). Retrieved from <https://duckduckgo.com>
- Farrier, E. (2024, August 21). A guide to protecting your personal information. Retrieved from <https://lifelock.norton.com/learn/internet-security/ways-to-help-protect-your-personal-information-online>
- Glover, E. (2024, January 24). What Is Online Privacy?. Built In. Retrieved from <https://builtin.com/articles/what-is-online-privacy>
- Google Privacy Checkup (n.d.). Retrieved from <https://myaccount.google.com/privacycheckup>
- Negrean, R. (n.d.). 10 Tips for Protecting Online Privacy: Strategies for Digital Security. Privacy Tutor. Retrieved from <https://privacytutor.net/10-tips-for-protecting-online-privacy>
- Tech Implement Infra Pvt Ltd. (2024, December 8). Essential Tips on Protecting Personal and Professional Data Online. [Video]. YouTube. <https://youtu.be/6WQzMAd6mJs?si=cq1NFnjxu7i8NRk5>
- Webb, M. (2023, November 26). How to Protect Your Online Privacy: 7 Best Practices to Implement Today. Techopedia. Retrieved from <https://www.techopedia.com/how-to/how-to-protect-your-privacy-online>





SINAV

1. Kişisel verilerin çevrim içi ortamda kötüye kullanılmasını sınırlamak için atılabilecek basit bir adım nedir?
 - A. Hiçbir sosyal medya hesabı oluşturmamak
 - B. Cihazlardaki tüm bildirimleri kapatmak
 - C. Uygulama izinlerini incelemeden kabul etmek
 - D. Sosyal medya gizlilik ayarlarını düzenli olarak gözden geçirmek
2. Kimlik hırsızlığına yol açabilecek aşırı paylaşım örneği aşağıdakilerden hangisidir?
 - A. Sadece yakın arkadaşlarla tatil fotoğrafı paylaşmak
 - B. Konumunuzu ve günlük rutinlerinizi herkese açık şekilde paylaşmak
 - C. Evcil hayvanlarınızın fotoğraflarını özel mesajla göndermek
 - D. Çevrim içi ruh halinizi emojilerle ifade etmek
3. Uygulama izinlerini gözden geçirmek çevrim içi gizliliğinizi nasıl geliştirir?
 - A. Uygulamaların gereksiz kişisel verilere erişimini kısıtlamanıza olanak tanır
 - B. Uygulamaları daha hızlı indirmenizi sağlar çünkü izin kontrollerini atlar
 - C. Cihazınızdaki tüm uygulamaların otomatik olarak güncellenmesini sağlar
 - D. Uygulamaların cihazınızda daha sorunsuz çalışmasına yardımcı olur.





SINAV

4. Birçok insan çevrim içi ortamda kişisel bilgilerini neden koruyamaz?

- A. Gizlilik araçları normal kullanıcılar için mevcut değildir
- B. İnsanlar şirketlere verilerini güvende tutmaları konusunda güvenir
- C. Gizlilik ayarları ve araçları genellikle göz ardı edilir veya kafa karıştırıcı bulunur
- D. Çoğu insan korunmaya değer kişisel verileri olmadığını düşünür

5. Kişisel bilgileri korumak için geliştirilebilecek iyi bir alışkanlık hangisidir?

- A. Kolaylık olması için aynı parolayı her yerde kullanmak
- B. Uygulamaların her zaman konumunuzu takip etmesine izin vermek
- C. Hizmet şartlarını görmezden gelmek
- D. Hassas bilgileri herkese açık platformlarda paylaşırken dikkatli olmak





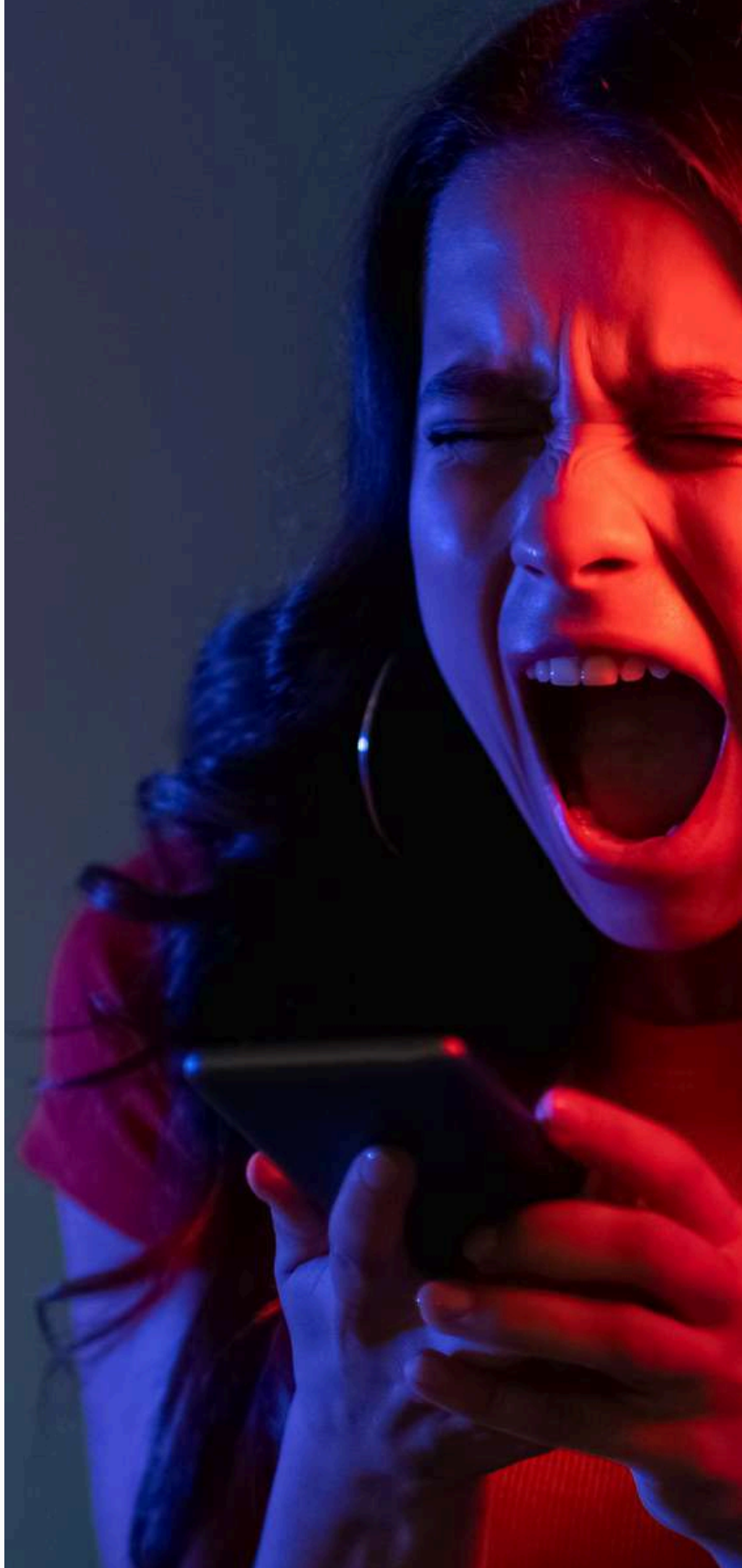
Cevaplar

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





Centrum Wspierania
Edukacji
i Przedsiębiorczości



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 yansıtmaması gerekmez. Ne Avrupa Birliği ne de EACEA bunlardan sorumlu tutulamaz.