



MODÜL 5

SİBER GÜVENLİK VE ÇEVİRİMİÇİ

GÜVENLİK



erasmediah.eu



**Co-funded by
the European Union**



Ders 5.6

Çevrimiçi Güvenlik İçin Pratik Araçlar



ERASMEDIAH

Educational Reinforcement Against
the Social Media Hyperconnectivity



**Co-funded by
the European Union**

Ders 5.6

Çevrimiçi Güvenlik İçin Pratik Araçlar

Hedefler:

- Katılımcılara ortalama , kötü amaçlı yazılım ve çevrimiçi dolandırıcılık gibi yaygın dijital tehditleri tanıma ve etkisiz hale getirme konusunda pratik araçlar ve teknikler kazandırmak.
- Parola yöneticileri, VPN'ler ve güvenli tarayıcılar gibi siber güvenlik kaynaklarını etkin kullanma becerisi geliştirmek ve çevrimiçi gizlilik yönetimi konusunda farkındalık oluşturmak.
- Dijital platformları eleştirel bakış açısıyla değerlendirme, siber tehditlerin uyarı işaretlerini tanıma ve şüpheli durumları bildirme gibi koruyucu alışkanlıklar edinerek güvenli ve sorumlu çevrimiçi davranışları teşvik etmek.

Temel Mesaj(lar):

- Farkındalık ve hazırlık, çevrimiçi güvenliğinizin ilk savunma hattıdır. Dijital tehditleri anlamak ve doğru araçlara sahip olmak, internet ortamında güvenle hareket etmenizi sağlar.
- Güvenliğiniz sizin elinizde. VPN, güvenli tarayıcılar ve gizlilik ayarları gibi araçları kullanarak kişisel verilerinizi koruyabilir, dijital dünyada kontrolü elinizde tutabilirsiniz.



TYPE OF LESSON:





Derse Genel Bakış

Çevrimiçi güvenlik, kişisel bilgileri korumak ve dijital tehditleri önlemek için tasarlanmış araçların etkili bir şekilde kullanılmasına büyük ölçüde bağlıdır. Bu ders, parola yöneticileri, VPN'ler ve gizlilik ayarları gibi temel siber güvenlik araçlarıyla pratik ve uygulamalı bir etkileşimi vurgular.

Katılımcılar bu araçların nasıl çalıştığını keşfedecek, özelliklerini test edecek ve günlük dijital alışkanlıklarına nasıl entegre edebileceklerini öğreneceklerdir. Rehberli etkinlikler yoluyla, bu araçları kullanma konusunda güven kazanacak ve dijital tehditlere karşı pratik çözümler geliştirme becerisi edineceklerdir.

Atölye çalışması 4 adımda yapılandırılmıştır:

- 1.Çevrimiçi güvenlik araçlarına giriş (10 dakika)
- 2.Araçlarla uygulamalı keşif (15 dakika)
- 3.Senaryoya dayalı risk yönetimi (10 dakika)
- 4.Son değerlendirme ve yansıtma (5 dakika)



1 Adım

Çevrimiçi güvenlik araçlarına giriş

Hiç çevrimiçi ortamda şüpheli görünen bir şeye karşılaştınız mı? Belki şifrenizi sıfırlamanızı isteyen garip bir e-posta, bedava ödül sunan bir açılır pencere ya da çok fazla kişisel bilgi isteyen bir web sitesi... Bu tür durumlar riskli hissettirebilir ve çoğu zaman gerçekten de öyledir.

İyi haber şu ki, bu gibi anlarda kendinizi korumak için kullanabileceğiniz pratik araçlar var. Bu etkinliğin sonunda, bu riskleri nasıl tanıyacağınızı ve parola yöneticileri, VPN'ler ve gizlilik ayarları gibi araçları kullanarak çevrimiçi ortamda nasıl güvende kalacağınızı öğrenmiş olacaksınız.

Haydi birlikte keşfedelim, bakalım bu araçlar size nasıl yardımcı olabilir



Step 1

Çevrimiçi güvenlik araçlarına giriş

İnternette daha güvenli olmanızı sağlayacak üç basit araç işte burada:

- Parola Yöneticileri: Güçlü ve benzersiz parolalar oluşturup saklamanıza yardımcı olur. Böylece tüm şifreleri hatırlamanız gerekmez.
- VPN'ler (Sanal Özel Ağlar): Özellikle halka açık Wi-Fi ağlarında çevrimiçi etkinliklerinizi korur ve bağlantınızı güvenli hale getirir.
- Tarayıcı Gizlilik Ayarları: Web sitelerinin sizin hakkınızda (konumunuz, gezinme alışkanlıklarınız gibi) hangi bilgileri toplayabileceğini kontrol etmenizi sağlar.

Bugün bu araçlara odaklanacağız çünkü çevrimiçi ortamda güvende kalmanızda gerçekten büyük fark yaratabilirler.

Birlikte düşünelim:

En son internette sizi rahatsız eden veya güvensiz hissettiren bir şeyle ne zaman karşılaştınız? Belki bir web sitesi size güven vermedi. O durumda ne yaptınız?

Yok saydınız mı, araştırdınız mı, yoksa tıkladınız mı?

Şimdi birlikte beyin fırtınası yapalım:

- Daha önce fark ettiğiniz çevrimiçi tehditler ya da riskler nelerdi?
- İnternette güvende kalmak için şu anda kullandığınız araçlar veya stratejiler var mı?

Birkaç dakikanızı ayırıp grupça fikirleri paylaşacağız. Bu tür bir deneyiminiz yoksa endişelenmeyin arkadaşlarınızın paylaşımları size yeni bakış açıları kazandırabilir.



2 Adım

Uygulamalı araç keşfi

Şimdi, basit araçların çevrimiçi varlığınızı nasıl daha güvenli hale getirebileceğini keşfetme zamanı! Bu etkinlikte tarayıcı gizlilik ayarlarınızı inceleyecek ve The Password Meter aracılığıyla güçlü şifre oluşturma becerilerinizi test edeceksiniz. Haydi başlayalım!

Bölüm 1: Tarayıcı Gizlilik Ayarları

Tarayıcınız, web sitelerinin sizin hakkınızda ne kadar bilgi toplayabileceğini kontrol etmenizi sağlar. Şimdi gizlilik ayarlarını kontrol edip gerektiğinde düzenleyelim:

1. Tarayıcınızın gizlilik ayarlarını açın.
2. ("Ayarlar" veya "Tercihler" bölümüne girin, ardından "Gizlilik" ya da "Güvenlik" sekmesini bulun.)
3. Aşağıdaki alanları inceleyin:
 - Takip koruması: Açık mı?
 - Çerezler: Üçüncü taraf çerezler engelleniyor mu?
 - İzinler: Hangi web siteleri konumunuza, kameranıza veya mikrofonunuza erişebiliyor?



2 Adım

Uygulamalı araç keşfi

3. Ayarları düzenleyin: Verilerinizi korumaya yardımcı olabilecek herhangi bir gizlilik ayarını etkinleştirin.

Örneğin:

- Takip çerezlerini engelleyin.
- Güvenmediğiniz web siteleri için konum paylaşımını devre dışı bırakın.

Hızlı yansıtma:

Mevcut ayarlarınızda sizi şaşırtan bir şey oldu mu? Herhangi bir değişiklik yaptınız mı?

Bölüm 2: The Password Meter ile şifre gücünü test etme

Güçlü bir şifre oluşturmak, hesaplarınızı korumanın en kolay yollarından biridir. Şimdi, şifrelerinizin ne kadar güvenli olduğunu görelim:

- 1.The Password Meter sitesine gidin.
- 2.Yeni bir şifre düşünün (hali hazırda kullandığınız bir şifreyi girmeyin!).



2 Adım

Uygulamalı araç keşfi

3. Şifrenizi The Password Meter'a girin ve geri bildirimine bakın:

- Şifreniz ne kadar güçlü?
- Daha güçlü hale getirmek için hangi önerileri veriyor?

4. Geri bildirimine göre şifrenizi değiştirerek denemeler yapın (örneğin: semboller ekleyin, daha uzun yapın ya da küçük ve büyük harfleri karıştırın).

Puanınızın nasıl geliştiğini gözlemleyin!

Hızlı yansıtma:

Güçlü bir şifre oluşturmak sizin için ne kadar kolay ya da zordu?

Gelecekte şifre oluştururken farklı yapacağınız bir şey nedir?

Bu etkinliğin sonunda, tarayıcınızın gizlilik ayarlarını geliştirmiş ve daha güçlü şifreler oluşturmayı öğrenmiş olacaksınız!



3 Adım

Senaryo temelli risk yönetimi

Bazı pratik araçlara baktıktan sonra, şimdi bunların gerçek yaşam durumlarında nasıl uygulanabileceğini görelim.

Küçük gruplar halinde çalışarak senaryoları analiz edecek, riskleri tanımlayacak ve tartıştığımız araçları kullanarak nasıl başa çıkılacağını belirleyeceksiniz.

Grubunuza verilen senaryoyu okuyun. İşte bazı örnekler:

- Bir e-posta alıyorsunuz ve bir ödül kazandığınız söyleniyor, ancak bağlantı şüpheli görünüyor. Ne yaparsınız?
- Bir sosyal medya uygulaması, kurulum sırasında konumunuza, kameranıza ve mikrofonunuza erişmek istiyor. Buna izin vermeli misiniz?
- Bir kafede halka açık Wi-Fi kullanıyorsunuz ve bilinmeyen bir web sitesine giriş yapmanız isteniyor. Güvende kalmak için ne yaparsınız?

Grubunuzla birlikte senaryonuzdaki riskleri tartışın. Kendinize şu soruları sorun:

- Dikkatli davranmazsanız ne olabilir?
- Bu durum neden güvensiz hissettiriyor?

Riski yönetmek için hangi pratik araçları kullanabileceğinize karar verin. Örneğin:

- Gereksiz izinleri engellemek için tarayıcı gizlilik ayarlarını kullanın.
- Şüpheli bağlantılara tıklamaktan kaçının ve e-postaları kimlik avı belirtileri açısından kontrol edin.
- Ortak Wi-Fi kullanırken bağlantınızı güvence altına almak için bir VPN açın.



3 Adım

Senaryo temelli risk yönetimi

Birkaç dakikanın ardından her grup şunları paylaşacak:

- Senaryoda fark ettiğiniz riskler nelerdi?
- Güvende kalmak için hangi araçları veya adımları kullandınız?

Şunu düşünün: Bu araçlar kendi çevrim içi etkinliklerinizde size nasıl yardımcı olabilir?

Tarayıcı gizlilik ayarları, VPN'ler ve kimlik avı tespiti gibi pratik araçlar, riskli durumları yönetilebilir hale getirebilir.

Bu araçları düzenli olarak kullanmak, çevrim içi ortamda güvende kalmayı çok daha kolaylaştırır!

Haydi, öğrendiklerinizi değerlendirelim ve çevrim içi ortamda güvende kalmak için nasıl kullanacağınızı düşünelim.

1 Adım: Düşün

Şu sorular üzerine düşünün:

- Hangi araç (ör. tarayıcı gizlilik ayarları, VPN'ler, parola yöneticileri) sizin için en faydalı oldu? Neden?
- Bu araçları kullandıktan sonra çevrim içi güvenlik konusundaki bakış açınız nasıl değişti?

2 Adım: Bir sonraki adımınızı planlayın

Çevrim içi güvenliğinizi artırmak için atacağınız bir eylemi yazın.

- Ne yapacaksınız? (ör. “Güçlü parolalar oluşturmak için bir parola yöneticisi kullanacağım.”)
- Ne zaman yapacaksınız? (ör. “Hafta sonuna kadar.”)

Pratik araçlar ilk adımınızdır çevrim içi güvenliğinizi güçlü tutmak için tutarlı olun!





Temel Çıkarım Özeti

- Tarayıcı gizlilik ayarları, parola yöneticileri ve VPN'ler çevrim içi güvenliğinizi artırmak için basit ama güçlü araçlardır.
- Gizlilik ayarlarınızı düzenleyerek ve gereksiz izinleri sınırlandırarak çevrim içi ortamda paylaştığınız bilgileri aktif şekilde yönetin.
- Gizlilik ayarlarını düzenli olarak güncelleyin, güvenli parolalar oluşturun ve uygulama izinlerini gözden geçirerek çevrim içi güvenliği dijital yaşamınızın rutin bir parçası hâline getirin.
- Proaktif olun araçları eleştirel düşünme ve güncel bilgiyle birleştirmek, gelişen çevrim içi tehditlere karşı hazırlıklı olmanızı sağlar.
- Ayrıca, diğer pratik çevrim içi araçları da test etmeye çalışın ne kadar çok aracı kullanmayı bilerseniz, dijital güvenliğinizi o kadar artırırsınız!



Gençlik çalışanları, eğitimciler ve öğretmenlere yönelik yönergeler

Hedef:

Bu ders, katılımcıların temel çevrim içi güvenlik araçlarını kullanma konusunda pratik beceriler kazanmalarına odaklanır. Bireysel ve grup çalışmaları ile yapılan tartışmalar aracılığıyla katılımcılar, yaygın çevrim içi tehditleri tanıma ve bunlarla başa çıkma, parola yöneticileri, VPN'ler ve gizlilik ayarları gibi araçlarla dijital korumalarını güçlendirme ve günlük çevrim içi alışkanlıklarına daha güvenli davranışları entegre etme becerisi kazanacaklardır.

Gerekli Materyaller:

- VPN'ler, parola yöneticileri gibi araçları test etmek için internet bağlantısı
- Uygulamalı egzersizler için dizüstü bilgisayar, tablet veya akıllı telefon
- Beyin fırtınası ve tartışmaların özetlenmesi için beyaz tahta veya flip chart
- Not almak için boş kâğıtlar
- Kalemler veya renkli işaretleyiciler





1 Adım: Çevrim İçi Güvenlik Araçlarına Giriş (10 dakika)

1. Katılımcıları şu soruyla sürece dahil edin: “Garip bir e-posta, bir ödül vadeden açılır pencere ya da çok fazla kişisel bilgi isteyen bir web sitesi gibi çevrim içi ortamda şüpheli görünen bir şeyle hiç karşılaştınız mı?” Bu tür durumların riskli hissettirebileceğini ve genellikle öyle olduğunu kısaca açıklayın. Ancak bu durumlarla başa çıkmak için kullanabileceğiniz pratik araçlar vardır.
2. Oturumun üç temel araca odaklanacağını açıklayın: parola yöneticileri, VPN'ler ve tarayıcı gizlilik ayarları. Bu araçların önemini şu şekilde vurgulayın: parola yöneticileri güçlü ve benzersiz parolalar oluşturmanıza ve saklamanıza yardımcı olur, VPN'ler özellikle halka açık Wi-Fi ağlarında çevrim içi etkinliğinizi korur ve tarayıcı gizlilik ayarları, web sitelerinin sizinle ilgili ne tür bilgiler toplayabileceğini (örneğin, konum veya gezinme alışkanlıkları) kontrol etmenizi sağlar.
3. Katılımcılardan çevrim içi risklerle ilgili kendi deneyimlerini hatırlamalarını isteyin: “En son çevrim içi ortamda şüpheli bir şeyle karşılaştığınızda ne yaptınız?”
4. “Daha önce fark ettiğiniz çevrim içi tehdit türleri nelerdi?” ve “Çevrim içi ortamda güvende kalmak için hâlihazırda hangi araçları veya stratejileri kullanıyorsunuz?” gibi sorularla kısa bir grup tartışması başlatın. Katılımcıları kendi fikirlerini veya yaşadıkları olayları paylaşmaya teşvik edin. Bu, başkalarının hikâyelerinden yeni düşünceler doğmasına yardımcı olabilir.
5. Şu ifadeyle etkinliği toparlayın: “Parola yöneticileri, VPN'ler ve gizlilik ayarları gibi araçları kullanarak, çevrim içi dünyada kişisel bilgilerinizi koruyabilir ve güvenle hareket edebilirsiniz.” Tartışmayı etkileşimli ve destekleyici bir şekilde yönetin; katılımcıların fikirlerini paylaşmalarını ve grup içinde öğrenmelerini teşvik edin.





2 Adım: Uygulamalı araç keşfi (15 Dakika)

1. Bu etkinliğin amacını açıklayarak başlayın: tarayıcı gizlilik ayarları ve parola gücü testi yoluyla çevrim içi güvenliği artıran pratik araçları keşfetmek.
2. Yapılandırılmış bir yaklaşım sağlamak için etkinliği iki bölüme ayırın.

Bölüm 1: Tarayıcı gizlilik ayarları (8 dakika)

1. Katılımcılara tarayıcılarının gizlilik ayarlarını açmalarını söyleyin (Ayarlar veya Tercihler sekmesine gidin, ardından Gizlilik veya Güvenlik bölümünü bulun). Aşağıdaki temel alanları gözden geçirmelerini isteyin:
 - İzleme önleme: Etkinleştirildiğinden emin olun.
 - Çerezler: Üçüncü taraf çerezlerin engellenip engellenmediğini kontrol edin.
 - İzinler: Hangi web sitelerinin konum, kamera veya mikrofona erişebildiğini inceleyin.
2. Katılımcıları, izleme çerezlerini engellemek veya gereksiz konum paylaşımını devre dışı bırakmak gibi ayarlamaları yapmaları için teşvik edin.
3. Sonrasında şu soruyla kısa bir yansıtma yapmalarını sağlayın: “Mevcut ayarlarınızda sizi en çok ne şaşırttı? Herhangi bir değişiklik yaptınız mı?” Bu, katılımcıların bulgularını bu araçların değeriyle ilişkilendirmelerine yardımcı olur.

Bölüm 2: Parola gücü testi (7 dakika)

1. Katılımcılara The Password Meter sitesine gitmelerini söyleyin. Halihazırda kullanmadıkları yeni bir parola oluşturarak bu parolanın gücünü test etmelerini isteyin.
2. Geri bildirimleri analiz etmeleri ve puanı nasıl artırabileceklerini görmek için semboller eklemek, büyük-küçük harf kullanmak ya da uzunluğu artırmak gibi değişiklikler yapmaları konusunda cesaretlendirin.
3. Şu sorularla etkinliği yansıtma ile sonlandırın: “Güçlü bir parola oluşturmak ne kadar kolay ya da zordu? Gelecekte parola belirlerken farklı yapacağınız bir şey var mı?”
4. Etkinliği, onun pratik değerini vurgulayarak tamamlayın.
5. Katılımcılar bu araçları keşfederken ve uygularken oturumu uygulamalı ve ilgi çekici tutun; gerektiğinde rehberlik sağlayın.



Adım 3: Senaryoya Temelli Risk Yönetimi (10 dakika)

1. Bu etkinlik, katılımcıların çevrim içi güvenlik araçlarını gerçek yaşam senaryolarında uygulamalarına yardımcı olur. Katılımcıları küçük gruplara ayırın ve her gruba bir senaryo atayın. Örneğin:
 - Ödül bağlantısı içeren şüpheli bir e-posta
 - Aşırı izinler isteyen bir sosyal medya uygulaması
 - Halka açık Wi-Fi kullanımı sırasında karşılaşılan bilinmeyen bir oturum açma ekranı
2. Gruplardan, şu soruları dikkate alarak riskleri tartışmalarını isteyin:
 - “Dikkatli davranmazsanız ne gibi sorunlar ortaya çıkabilir?”
 - “Bu durum neden güvensiz hissettiriyor?”
3. Riskin nasıl yönetileceğini belirlemelerini sağlayın; örneğin, tarayıcı gizlilik ayarlarının kullanılması, kimlik avı bağlantılarından kaçınma ya da VPN etkinleştirme gibi araçlarla.
4. Sonrasında, her grup belirlediği riskleri ve bunlara karşı kullandığı araçları sınıfla paylaşır.
5. Etkinliği şu vurguyla sonlandırın: “Gizlilik ayarları, VPN ve kimlik avı tespiti gibi araçlar çevrim içi risklerin yönetimini kolaylaştırır. Bu araçların düzenli kullanımı çevrim içi güvenliği güçlendirir.” Oturumu odaklı tutun ve pratik, uygulanabilir içgörülerini teşvik edin.





Adım 4: Son Yansımalar (5 dakika)

1. Oturumu, katılımcıların öğrendiklerini pekiştirmelerine yardımcı olacak kısa bir yansıtma etkinliğiyle tamamlayın. Aşağıdaki soruları düşünmelerini isteyerek başlayın:
 - “Sizin için en faydalı araç hangisiydi? (ör. tarayıcı gizlilik ayarları, VPN, parola yöneticileri) Neden?”
 - “Bu araçları kullandıktan sonra çevrim içi güvenliğe bakış açınız nasıl değişti?”
2. Katılımcıları, düşüncelerini kısaca paylaşımları için teşvik edin ve destekleyici bir tartışma ortamı yaratın.
3. Ardından, çevrim içi güvenliklerini artırmak için somut bir eylem planlamalarını isteyin:
 - “Ne yapacaksınız?” (ör. “Güçlü parolalar oluşturmak için bir parola yöneticisi kullanacağım.”)
 - “Ne zaman yapacaksınız?” (ör. “Hafta sonuna kadar uygulamaya başlayacağım.”)
4. Oturumu şu hatırlatmayla bitirin:
5. “Pratik araçlar ilk adımdır çevrim içi güvenliğinizi güçlü tutmak için tutarlılık gösterin!”
6. Tonu motive edici tutun ve öğrenilen bilgilerin günlük dijital yaşama nasıl entegre edileceğine odaklanın.

Temel Mesajlar:

Bu dersi tamamlayan katılımcılar, parola yöneticileri, VPN’ler ve tarayıcı gizlilik ayarları gibi temel araçları kullanarak çevrim içi güvenliklerini nasıl artıracaklarını net bir şekilde anlayacaklardır. Veri takibi gibi yaygın tehditleri tanıyacak ve kişisel bilgilerini korumak için proaktif adımlar atmayı öğreneceklerdir.

Bu araç ve stratejileri günlük alışkanlıklarına entegre ederek dijital dünyada daha güvenli ve özgüvenli bir şekilde hareket edebileceklerdir. Bu kazanımları etkili bir şekilde aktarmak için katılımcılara, bu araçların günlük çevrim içi güvenlik üzerindeki somut etkisini gösteren anlaşılır örnekler ve yaşanabilir senaryolar sunmalısınız.



Takip ve Evde Uygulama Etkinlikleri:

Katılımcıları, mevcut çevrim içi alışkanlıklarını daha yakından incelemeye teşvik edin. Tarayıcı gizlilik ayarlarını gözden geçirip düzenlemeleri, The Password Meter gibi araçlarla parolalarının gücünü test etmeleri ve VPN işlevlerini keşfetmeleri için yönlendirin. Sıklıkla kullandıkları uygulamaların izinlerini değerlendirmelerini isteyin; olası riskleri belirleyip daha güvenli alternatifler uygulamaya koymalarını sağlayın. Son olarak, yeni öğrendikleri bir güvenlik ipucunu bir arkadaşları ya da aile üyeleriyle paylaşmalarını isteyin. Bu, bilgilerini pekiştirirken dijital güvenlik farkındalığını yaymalarına da yardımcı olur.

Öğretmenler için İpuçları:

Parola yöneticileri, VPN'ler ve gizlilik ayarları gibi araçların çevrim içi güvenliği nasıl artırabileceğini göstermek için gerçek yaşamdan pratik örnekler ve etkileşimli uygulamalar kullanın. Katılımcılara bu araçların nasıl yapılandırılacağını adım adım gösterin ve oturumu uygulamalı, eyleme dönük hâle getirin.

Katılımcıların çevrim içi tehditlerle ilgili deneyimlerini rahatça paylaşabilecekleri, soru sorabilecekleri açık ve destekleyici bir ortam oluşturun.

Bu araçların düzenli kullanımının önemini vurgulayın ve bunları günlük dijital alışkanlıklarına entegre etmelerini teşvik edin. Bu sayede katılımcılar, dijital dünyada daha tutarlı ve proaktif bir şekilde korunma becerisi geliştirebilirler.





Araçlar

Çevrimiçi Güvende Olun



Çok çeşitli çevrimiçi güvenlik konuları hakkında ücretsiz ve anlaşılır tavsiyeler sunan kapsamlı bir web sitesi. Kişisel bilgilerin korunması, dolandırıcılığın önlenmesi ve çevrimiçi iletişimin güvenli hale getirilmesi konusunda pratik kılavuzlar içerir. İçerik kullanıcı dostudur ve minimum düzeyde teknik bilgisi olan kişiler için tasarlanmıştır.

www.getsafeonline.org

The Password Meter



Şifrelerin gücünü değerlendiren ve bunları geliştirmeye yönelik ipuçları sağlayan ücretsiz bir araç. Öğrenciler parola oluşturmayı deneyebilir ve güvenlik seviyeleri hakkında anında geri bildirim alabilir, bu da güçlü parolaların önemini anlamanın etkileşimli bir yolu haline gelir.

passwordmeter.com



Kaynakça

- Alice. (2022, October 3). 5 Tools That Help Keep People Safe Online. Ryadel. Retrieved from <https://www.ryadel.com/en/5-privacy-data-protection-security-tools>
- Get Safe Online. (n.d.). Retrieved from <https://www.getsafeonline.org>
- Goodwall Team. (2022, March 24). 7 Best Online Safety Tools and Privacy Settings to Keep Yourself Protected. Retrieved from <https://www.goodwall.io/blog/online-safety-tools-and-privacy-settings>
- 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>
- The Password Meter. (n.d.). Retrieved from <https://passwordmeter.com>
- Vodafone. (n.d.). Using online safety and wellbeing tools. Retrieved from <https://www.vodafone.co.uk/help-and-information/nspcc-phone-safety-toolkit/03-how-to-online-safety-tools>





SINAV

1. Sanal Özel Ağ'ın (VPN) temel işlevi nedir?

- A. Otomatik antivirüs koruması sağlamak
- B. İnternet hızını artırmak
- C. Tüm web sitelerinde açılır reklamları engellemek
- D. Çevrim içi etkinlikleri şifrelemek, özellikle halka açık Wi-Fi ağlarında

2. Aşağıdaki davranışlardan hangisi çevrim içi güvenliğinizi riske atabilir?

- A. Her hesap için güçlü ve benzersiz şifreler kullanmak
- B. Tarayıcı gizlilik ayarlarını düzenli olarak ayarlamak
- C. Giriş bilgilerini saklamak için bir şifre yöneticisi kullanmak
- D. İstenmeyen e-postalardaki her bağlantıya tıklamak

3. Tarayıcı gizliliğinizi artırmak için önerilen bir adım hangisidir?

- A. Varsayılan ayarları değiştirmeden kullanmak
- B. Takip çerezlerini engellemek ve gereksiz izinleri devre dışı bırakmak
- C. Tüm web siteleri için çerezleri kapatmak
- D. Tüm web sitelerinin konumunuza erişmesine izin vermek





SINAV

4. Tarayıcı gizlilik ayarlarının amacı nedir?

- A. Kullanıcının gezinme deneyimini hızlandırmak
- B. Kullanıcının şifrelerini güvenli bir şekilde saklamak
- C. Web sitelerinin kullanıcı hakkında hangi bilgileri toplayabileceğini kontrol etmek
- D. Tüm web sitelerinde açılır reklamları engellemek

5. Şifre gücünü nasıl artırabilirsiniz?

- A. Semboller ekleyerek, büyük-küçük harfleri karıştırarak ve uzunluğu artırarak
- B. Hatırlaması kolay yaygın ifadeler kullanarak
- C. Rakamlar ve özel karakterlerden kaçınarak
- D. Aynı şifreyi tekrar tekrar test ederek





Cevaplar

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





ERASMEDIAH

Educational Reinforcement Against
the Social Media Hyperconnectivity



Lélekben Otthon
Közhasznú Alapítvány

AdM
ArchiviodellaMemoria

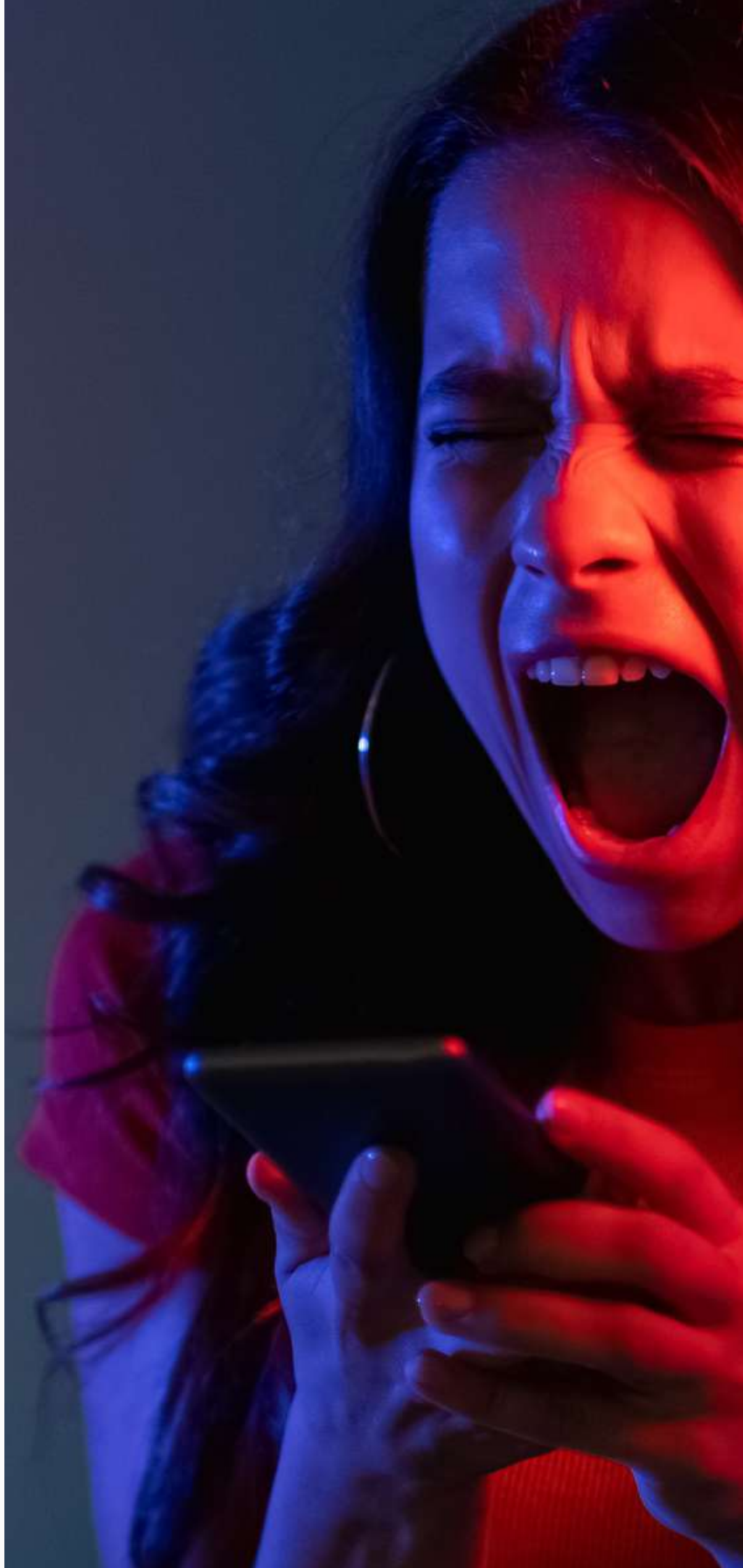


Centrum Wspierania
Edukacji
i Przedsiębiorczości

EDU
yayıncılık



@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 yansıtmaması gerekir. Ne Avrupa Birliği ne de EACEA bunlardan sorumlu tutulamaz.