Ad Soyad: _____ **Tarih:** _____ **Puan:** _____

Kimlik hırsızlığını önleme ve varlık Güvenlik Rehberi

Kimlik bilgisi sızıntıları, MFA, dark web izleme, kredi dondurma uyarıları, sosyal mühendislik

KİMLİK HIRSIZLIĞINI ÖNLEME ÖĞRENME ÖZETİ

GÜVENCEDE
VERİ ŞİFRELEME
256 bit AES Standardı

UYUMLU
KÜRESEL STANDARTLAR
GDPR ve CCPA çerçeveleri

SIFIR GÜVEN
ERİŞİM POLİTİKASI
Çok Faktörlü Kimlik Doğrulama

Hoş geldin! Bu etkinlik paketi sana kimlik hırsızlığını önleme ve azaltma konusunda rehberlik eder. Kimlik bilgisi sızıntılarını, çok faktörlü kimlik doğrulamayı, karanlık web izlemeyi, kredi dondurma uyarılarını ve sosyal mühendislik savunmasını keşfedeceksin.

ÇALIŞMA KÂĞIDI KONTROL NOKTALARI

- [ ] **Bölüm 1-4: Siber güvenlikte ve tehdit önlemede ustalaş.**
- [ ] **Bölüm 5-7: Çapraz bulmaca ve kelime avı bulmacalarını çöz.**
- [ ] **Bölüm 8-9: Vaka çalışmalarını ve şifre görevini çöz.**
- [ ] **Bölüm 10: Temel ve ileri düzey SSS sayfalarını gözden geçir.**
- [ ] **Bölüm 11: 10 ilginç gerçek dünya gerçeğini keşfet.**
- [ ] **Bonus: Hızlı Düşün görevi.**

VPN.com siber güvenlik rehberini aç

URL: https://www.vpn.com/tr/siber-guvenlik/kimlik-hirsizligi/

Kimlik Koruma Öğrenme Yol Haritan

- Karanlık web forumlarında kimlik bilgilerinin ifşa olma risklerini anla.
- Çok faktörlü kimlik doğrulama (MFA) ve kredi dondurma uyarıları uygula.
- Hedefli sosyal mühendislik dolandırıcılıklarına karşı kurumsal güvenlik savunmaları tasarla.

KİMLİK HIRSIZLIĞI REHBERİ TALİMATLARI

Çoktan seçmeli ve doğru/yanlış sorularını cevapla, boşluk doldurma cümlelerini kelime bankasını kullanarak tamamla, tanımları eşleştir, çapraz bulmacayı ve kelime avı bulmacasını çöz. Bilgini şu konulara uygula: kimlik koruması. Hızlı Düşün bonus etkinliğiyle bitir.

KİMLİK HIRSIZLIĞINI ÖNLEME VE VARLIK GÜVENLİĞİ (GİRİŞ)

Kimlik hırsızlığı, sızdırılmış kimlik bilgilerinden ve zayıf oturum açma yöntemlerinden yararlanarak kişisel ve kurumsal hesapları ele geçirir. MFA, kredi dondurma, dark web tarayıcıları ve SPF/DKIM/DMARC çerçevelerini kullanmak, dijital kimliğe bürünmeye karşı kritik bir savunma oluşturur.

HER KONTROL NOKTASINI DİKKATLE OKU VE DOĞRU CEVABI SEÇ YA DA YAZ.

Kontrol Noktası 1: Çoktan seçmeli görev

1 **1. Kimlik hırsızlarının oturum açma bilgilerini çalmak için kullandığı başlıca yöntem nedir?**

- A. Kullanıcıları sahte portallarda parola girmeye kandırmak için sahte e-posta uyarıları göndermek
- B. Kullanıcının kurumsal ofisinin yakınında radyo yayınlarını dinlemek
- C. Kullanıcının yerel sunucu depolama sürücüsünü birleştirmek (defrag)
- D. Harici ağ yedekleme yapılandırmalarının bağlantısını kesmek

2 **2. Hangi güvenlik kontrolü kimlik bilgisi sızıntılarına karşı en güçlü savunmayı sağlar?**

- A. Donanım anahtarları kullanan çok faktörlü kimlik doğrulama
- B. Varsayılan tarayıcı biçimlerini kullanarak uzun parolalar oluşturmak
- C. E-posta kullanıcı adlarını altı ayda bir değiştirmek
- D. Saklanan çerez izleme tarayıcı geçmişlerini silmek

3 **3. Kredi dondurmayı ne temsil eder?**

- A. Hırsızların izinsiz kredi açmasını önlemek için kredi raporlarını kilitlemek
- B. Banka hesabı işlem geçmişlerini veritabanlarından silmek
- C. Tarayıcılardaki kredi kartı manyetik şerit okuyucularını devre dışı bırakmak
- D. Yerel veritabanı sabit disklerini durağan hâlde şifrelemek

4 **4. Dark web izlemesi neden yararlıdır?**

- A. Sızdırılmış kimlik bilgileri yasa dışı veritabanlarında göründüğünde kullanıcıları uyarır
- B. Etkin kötü amaçlı yazılımın sanal korumalı alanlarda çalışmasını engeller
- C. Sanal ağlarda tarayıcı yönlendirme hızlarını artırır
- D. Arka uç veritabanı SQL enjeksiyonu erişim girişimlerini engeller

5 **5. Sosyal mühendislik ne anlama gelir?**

- A. İnsanları gizli kimlik bilgilerini gönüllü olarak vermeye yönlendirmek
- B. Etkin güvenlik istismarları için kurumsal sunucu portlarını taramak
- C. Sistem veritabanı dosyalarını çevrimdışı sabit disklere yedeklemek
- D. Ağ paketlerini şifreli üç onion düğümü üzerinden yönlendirmek

Kontrol Noktası 2: Doğru/Yanlış görevi

6 Soru 6

6. Kimlik hırsızlığı yalnızca çevrimiçi dijital hesapları etkiler, fiziksel posta kutusunu etkilemez.

Doğru Yanlış

7 Soru 7

7. Tüm kişisel hesaplarda MFA'yı zorunlu kılmak, kimlik bilgisi doldurma botu saldırılarının çoğunu engeller.

Doğru Yanlış

8 Soru 8

8. Kredi dondurma, kredi kontrollerini engeller ancak kendi banka hesabınıza erişmenizi de engeller.

Doğru Yanlış

9 Soru 9

9. Parola yöneticileri, sahte alan adlarında parolaları otomatik doldurmayı reddederek kullanıcıları kimlik avından korur.

Doğru Yanlış

10 Soru 10

10. Kimlik avı e-postaları, duygusal ve hızlı tepkileri tetiklemek için sıklıkla aciliyet bildiren bir dil kullanır.

Doğru Yanlış

Kontrol Noktası 3: Anahtar terim yerleştirme

Aşağıdaki her cümleyi oku ve boşluğu Kelime Bankası'ndaki doğru terimle doldur.

1. Kimlik hırsızlarının hedefi, kişisel parolalar ve kullanıcıların _____ .
2. Kullanıcıları veritabanı ihlalleri konusunda uyarmak, özel hesap kayıtlarındaki _____ tespit etmeye yarar.
3. Oturum açmak için geçici bir kod istemeye _____ kimlik doğrulama denir.
4. Çalınmış verileri bulmak için hacker forumlarını taramaya karanlık ağ _____ denir.
5. Yetkisiz kredi sorgularını engellemek için kredi dosyasında bir _____ işlemi gerekir.
6. Çalışanları kimlik avı farkındalığı konusunda eğitmek, etkin bir güvenlik _____ oluşturur.

KELİME BANKASI

ÇOK FAKTÖRLÜ | DONDURMA | HESAP BİLGİLERİ | İZLEME | KİMLİK AVI | SAVUNMA | SIZINTILAR | TAKLİT

Cevaplarını buraya yaz:

1.
2.
3.
4.
5.
6.

Kontrol Noktası 4: Güvenlik kavramı eşleştirme

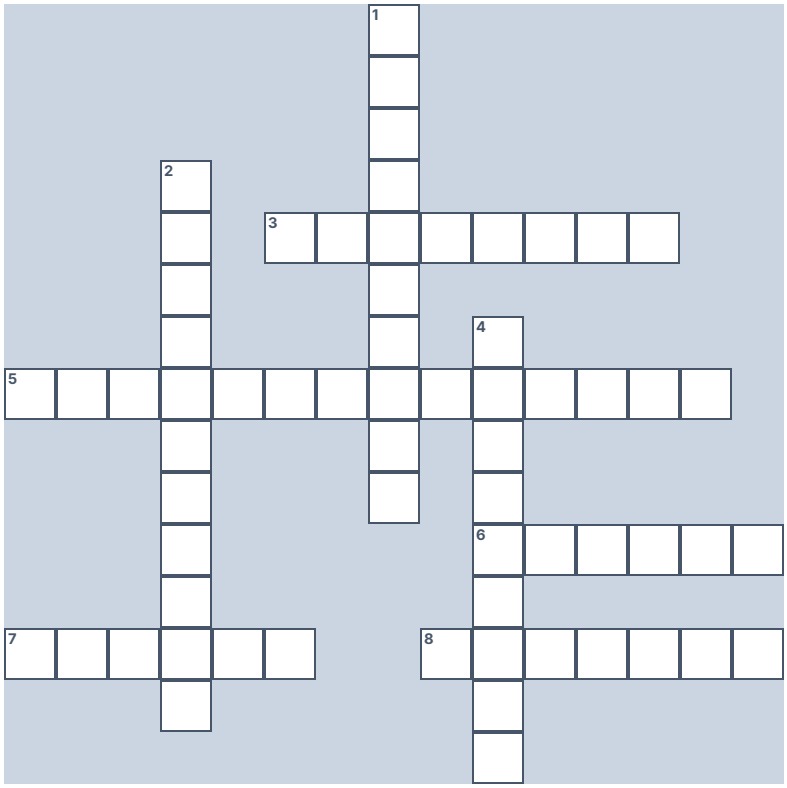
TANIM EŞLEŞTİRME

Soldaki her kelimeyi, doldurulabilir giriş kutusuna ilgili harfi (A-H) yazarak sağdaki doğru tanımıyla eşleştir.

☐	1. KİMLİK BİLGİLERİ	A	Hesap girişlerini koruyan ikincil doğrulama adımı (donanım anahtarları gibi).
☐	2. SIZINTILAR	B	Meşru bir kuruluşu taklit etmek için sahte bir web sitesi veya e-posta oluşturma.
☐	3. MFA	C	Hileli kredi başvurularını önlemek için kredi dosyalarına erişimi kısıtlamak.
☐	4. İZLEME	D	Kişisel kullanıcı kayıtlarını içeren özel veri tabanlarının yetkisiz ifşası.
☐	5. DONDURMA	E	Kimlik hırsızlığına karşı korunmak için kullanılan eğitim ve teknik denetimler.
☐	6. SAVUNMA	F	Kullanıcıları kimlik bilgilerini vermeye kandırmak için sahte mesajlar gönderme.
☐	7. SAHTEKÂRLIK	G	Çalınan kurumsal veriler için çevrimiçi forumları ve bilgisayar korsanı kanallarını taramak.
☐	8. KİMLİK AVI	H	Dijital kimlikleri doğrulamak için kullanılan kullanıcı adları, parolalar ve özel belirteçler.

Kontrol Noktası 5: Bulmaca

Bulmacayı, etkin beyaz kutulara harf yazarak çöz. Sayılar aşağıdaki ipuçlarına karşılık gelir.



SOLDAN SAĞA

3. Hileli kredi başvurularını önlemek için kredi dosyalarına erişimi kısıtlama. (8)

5. Dijital kimlikleri doğrulamak için kullanılan kullanıcı adları, parolalar ve özel jetonlar. (14)

6. Çalınmış kurumsal verileri bulmak için çevrimiçi forumları ve hacker kanallarını tarama. (6)

7. Meşru bir kuruluşu taklit eden sahte bir web sitesi veya e-posta oluşturma. (6)

8. Kimlik hırsızlığına karşı korunmak için kullanılan eğitim ve teknik kontroller. (7)

YUKARIDAN AŞAĞI

1. Kişisel kullanıcı kayıtlarını içeren özel veritabanlarının yetkisiz biçimde açığa çıkması. (10)

2. Hesap girişlerini koruyan ikincil doğrulama adımı (donanım anahtarları gibi). (11)

4. Kullanıcıları kimlik bilgilerini vermeye kandırmak için sahte mesajlar gönderme. (9)

Kontrol Noktası 5, alternatif: Erişilebilir bulmaca ipuçları

Ekran okuyucu ve klavye kullanıcıları, bulmaca cevaplarını aşağıdaki metin alanlarına doğrudan yazabilir.

SOLDAN SAĞA

3 soldan sağa: Hileli kredi başvurularını önlemek için kredi dosyalarına erişimi kısıtlama. (8 harf):

5 soldan sağa: Dijital kimlikleri doğrulamak için kullanılan kullanıcı adları, parolalar ve özel jetonlar. (14 harf):

6 soldan sağa: Çalınmış kurumsal verileri bulmak için çevrimiçi forumları ve hacker kanallarını tarama. (6 harf):

7 soldan sağa: Meşru bir kuruluşu taklit eden sahte bir web sitesi veya e-posta oluşturma. (6 harf):

8 soldan sağa: Kimlik hırsızlığına karşı korunmak için kullanılan eğitim ve teknik kontroller. (7 harf):

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: Kişisel kullanıcı kayıtlarını içeren özel veritabanlarının yetkisiz biçimde açığa çıkması. (10 harf):

2 yukarıdan aşağı: Hesap girişlerini koruyan ikincil doğrulama adımı (donanım anahtarları gibi). (11 harf):

4 yukarıdan aşağı: Kullanıcıları kimlik bilgilerini vermeye kandırmak için sahte mesajlar gönderme. (9 harf):

Kontrol Noktası 6: Gizli kelime bulmacası

Aşağıdaki ızgarada gizlenmiş 8 temel kelimeyi bul. Kelimeler yatay, dikey veya çapraz olabilir.

S A V U N M A S H Ç P Ö K E H

Ü A R Z R F Ö I U E K A A Ö N

L M L O Ş V Ö Z İ P İ Ş R Ç L

R R Y B T F R I Ü Ü M I A P Z

Ö U Y Y A J G N H L L P İ K K

T D S N K Ğ Ö T Ö G İ Z A N T

K N F T L C Y I P Y K B Ğ K Z

A O G I İ M O L M Ü A C K Z Y

F D F V T N U A T J V T O B M

K U S K G T Ç R Y T I İ P B Ü

O H E S A P B İ L G İ L E R İ

Ç Z V K P Ö V H N D A Ç İ Ö U

Ü Ü İ Z L E M E J I Ğ Ş Ğ F B

E H İ S R U P Z E Ğ E R C A J

O C Z K İ U P Ş A R Ü I K K G

KELİME LİSTESİ

HESAPBİLGİLERİ SIZINTILAR ÇOKFAKTÖRLÜ İZLEME DONDURMA SAVUNMA TAKLİT KİMLİKAVI

Kontrol Noktası 6, alternatif: Erişilebilir kelime eşleştirme

Kelime Bulmaca'daki 8 kelimenin her birini, boşluğa harfi (A-H) yazarak doğru tanımıyla eşleştir.

KELİME TERİMLERİ

- **A. HESAPBİLGİLERİ**
- **B. SIZINTILAR**
- **C. ÇOKFAKTÖRLÜ**
- **D. İZLEME**
- **E. DONDURMA**
- **F. SAVUNMA**
- **G. TAKLİT**
- **H. KİMLİKAVI**

TANIMLAR VE EŞLEŞTİRME ALANLARI

1. Kullanıcıları kimlik bilgilerini vermeye kandırmak için sahte mesajlar gönderme.
2. Dijital kimlikleri doğrulamak için kullanılan kullanıcı adları, parolalar ve özel jetonlar.
3. Meşru bir kuruluşu taklit eden sahte bir web sitesi veya e-posta oluşturma.
4. Kimlik hırsızlığına karşı korunmak için kullanılan eğitim ve teknik kontroller.
5. Çalınmış kurumsal verileri bulmak için çevrimiçi forumları ve hacker kanallarını tarama.
6. Hileli kredi başvurularını önlemek için kredi dosyalarına erişimi kısıtlama.
7. Kişisel kullanıcı kayıtlarını içeren özel veritabanlarının yetkisiz biçimde açığa çıkması.
8. Hesap girişlerini koruyan ikincil doğrulama adımı (donanım anahtarları gibi).

Kontrol Noktası 7: Karışık harflerden kelime bulma görevi

Temel siber güvenlik kavramlarını ve terimlerini ortaya çıkarmak için aşağıdaki harfleri doğru sıraya diz. Cevaplarını verilen giriş kutularına yaz.

1. LBLİİSEGEHRİ PA
2. AÜOÇLKKRÖT F
3. DODURAMN
4. TLKİTA
5. LTRIIINSAZ
6. MEİLEZ
7. SMNAAUV
8. İİVKLİKAM

Bonus etkinlik: Hızlı Düşün

HER KATEGORİ İÇİN 3 CEVAP. LİSTEYİ İLK TAMAMLAYAN KAZANIR.

1	Kimliğin çalınırsa yapılacaklar			
2	Sosyal medyada paylaşılmaması gereken şeyler			
3	Yedeklediğin şeyler			
4	Cüzdanındaki kartlar veya kimlikler			
5	Korumaman gereken belgeler			
6	Veri sızıntısından sonra yapılacaklar			
7	Yazılımı güncelleme nedenleri			
8	Kimlik hırsızının istediği bilgiler			
9	Hacklenebilecek cihazlar			
10	Verilerinin sızabileceği yerler			
11	Bugün başlayabileceğin güvenli alışkanlıklar			
12	Bir bilgisayarın virüslü olduğunu gösteren işaretler			
13	Kim olduğunu kanıtlama yolları			
14	Kimlik hırsızlığı işaretleri			
15	E-postadaki uyarı işaretleri			

Kontrol Noktası 8: Siber güvenlik vaka çalışmaları

Öğrendiğin kavramları aşağıdaki gerçek dünya senaryolarını çözmek için uygula.

VAKA ÇALIŞMASI 1: YÖNETİCİ KİMLİĞİNE BÜRÜNMEYE KARŞI KORUMA

👷

Senaryo: Üst düzey bir C seviyesi yönetici, müşterileri dolandırmak amacıyla kişisel e-postasını taklit eden yazım hatası temelli (typo-squatting) alan adlarının hedefi oldu. Bir marka koruma planı tasarla.

Tartışma sorusu: Marka taklidi risklerini analiz et ve SPF/DKIM/DMARC ile kimlik doğrulama denetimlerini ayrıntılı anlat.

VAKA ÇALIŞMASI 2: KURUMSAL KİMLİK BİLGİLERİNİN DARK WEB'DE AÇIĞA ÇIKMASI

👷

Senaryo: Bir karanlık ağ veritabanı dökümü, bir kuruluşun sistem yöneticilerine ait birkaç yüz kurumsal kimlik bilgisi içeriyor. Bir risk azaltma stratejisi tasarla.

Tartışma sorusu: Kimlik bilgisi temizleme sürecini özetle ve bir parola yöneticisi kullanıma alma planı yap.

Kontrol Noktası 9: Şifreyi Çöz

Bir siber güvenlik uzmanı, ağ varlıklarını çevrimiçi tehdit aktörlerine karşı korur. Aşağıdaki Harf-Sayı anahtarını kullanarak, eşleşen harfleri boşluklara yazıp mesajın şifresini çöz.

HARFTEN SAYIYA ŞİFRELEME ANAHTARI

A=1 B=2 C=3 Ç=4 D=5 E=6 F=7 G=8 Ğ=9 H=10
I=11 İ=12 J=13 K=14 L=15 M=16 N=17 O=18 Ö=19 P=20
R=21 S=22 Ş=23 T=24 U=25 Ü=26 V=27 Y=28 Z=29

5 12 13 12 24 1 15 14 12 16 15 12 9 12 17 12 4 18 14

7 1 14 24 19 21 15 26

5 18 9 21 25 15 1 16 1 28 15 1 14 18 21 25

Çözülen mesaj:

İPUCU: HER SAYI, O HARFİN ALFABEDEKİ SIRASINI GÖSTERİR (ÖR. 1 = A, 2 = B, 29 = Z).

Kontrol Noktası 10: Siber güvenlik hakkında sık sorulan sorular – temel düzey (Bölüm A)

Çevrimiçi tehditlerin azaltılmasına ilişkin sık sorulan soruları ve cevapları incele.

Q1: Kimlik hırsızlığı nedir?

Bir saldırganın mali kazanç için başkasının kimliğine bürünmek amacıyla kişisel kayıtları (parolalar veya SSN gibi) çaldığı suç.

Q2: Kimlik hırsızlığının en yaygın nedeni nedir?

Kimlik avı, hırsızların parola elde etmesinin önde gelen yollarından biridir ve kullanıcıları sahte, taklit web sitelerine çeker.

Q3: Çok faktörlü kimlik doğrulama (MFA) kimlikleri nasıl korur?

MFA, oturum açmak için ikinci bir kanıt (donanım anahtarı gibi) ister ve parolanı çalsalar bile saldırganları engeller.

Q4: Kredi dondurma nedir?

Kredi bürolarının kredi dosyanızı paylaşmasını engelleyen ve hırsızların adınıza yeni krediler açmasını durduran ücretsiz hizmet. [2]

Q5: Karanlık ağ izleme nedir?

Bilgisayar korsanı forumlarında sızdırılmış e-postaları, parolaları ve kişisel kayıtları tarayan ve verilerin açığa çıkarsa seni uyaran yazılım.

Kontrol Noktası 10: Siber güvenlik hakkında sık sorulan sorular – temel düzey (Bölüm B)

Çevrimiçi tehditlerin azaltılmasına ilişkin sık sorulan soruları ve cevapları incele.

Q6: Kimlik bilgisi doldurma (credential stuffing) ne demektir?

Etkin hesapları ele geçirmek için yüzlerce web sitesinde sızdırılmış parola listelerini deneyen otomatik botlar.

Q7: E-posta sahteciliği neden tehlikelidir?

Saldırganların e-postalarda gönderen adını taklit etmesine olanak tanır; bu da kimlik avı mesajlarının güvenilir iş arkadaşlarından gelmiş gibi görünmesine yol açar.

Q8: Parola yöneticileri kimlik hırsızlığını nasıl durdurur?

Her hesap için karmaşık, benzersiz parolalar saklar ve sahte kimlik avı alan adlarında kimlik bilgilerini otomatik doldurmayı reddederler.

Q9: Hedefli kimlik avı (spear phishing) nedir?

Aldatma olasılığını artırmak için kurbanın adı ve ayrıntılarıyla özelleştirilmiş, son derece hedefli kimlik avı saldırısı.

Q10: Kredi uyarısı, dondurmadan nasıl farklıdır?

Bir uyarı, borç verenlere hesap açmadan önce kimliğinizi doğrulamalarını söyler; dondurma ise kredi dosyanıza erişimi tamamen engeller. [2]

Kontrol Noktası 10: Güvenlik hakkında sık sorulan sorular – ileri düzey (Bölüm C)

Güvenlik çerçevelerinin, kötü amaçlı yazılım analizinin ve veri uyumluluğunun ileri düzey teknik yönlerini keşfet.

Q1: SIM değiştirme (SIM swapping) kimlik hırsızlığına nasıl yol açar?

Saldırganlar operatör çalışanlarını, kurbanın telefon numarasını yeni bir SIM karta aktarmaya ikna ederek SMS tabanlı 2FA kodlarını ele geçirir.

Q2: DMARC'ın kimlik hırsızlığını önlemedeki rolü nedir?

DMARC, alan adı sahiplerinin sahte e-postaların gelen kutularına ulaşmasını engellemesine olanak tanır ve sahte e-postaların kurumsal alan adlarını taklit etmesini durdurur.

Q3: Sentetik kimlik hırsızlığının tespiti neden zordur?

Hırsızlar, gerçek SSN'leri sahte adlar ve doğum tarihleriyle birleştirerek temel dolandırıcılık uyarılarını atlatan yepyeni kredi profilleri oluşturur.

Q4: Veri komisyoncuları kişisel kimlikleri nasıl istismar eder?

Aracılar, sızdırılabilen veya satılabilen profil dosyaları oluşturmak için kamu kayıtlarını, web davranışını ve satın alma geçmişlerini toplar.

Q5: SMS tabanlı MFA neden savunmasız sayılır?

SMS trafiği ele geçirmeye, kimlik avına ve operatör düzeyindeki SIM değiştirme istismarlarına karşı savunmasızdır.

Kontrol Noktası 10: Güvenlik hakkında sık sorulan sorular – ileri düzey (Bölüm D)

Güvenlik çerçevelerinin, kötü amaçlı yazılım analizinin ve veri uyumluluğunun ileri düzey teknik yönlerini keşfet.

Q6: Kredi dosyası kilidi nedir?

Dondurmaya benzer, kullanıcıların kredi dosyalarını bir mobil uygulama üzerinden anında açıp kilitlemesine olanak tanıyan ticari hizmet.

Q7: Kurumsal veri ihlalleri kimlik hırsızlığını nasıl körükler?

Sızdırılan veritabanları milyonlarca düz metin kimlik bilgisini açığa çıkarır ve hırsızlara hedefli kimlik dolandırıcılığı için gereken ham veriyi verir.

Q8: Sosyal medyada aşırı paylaşımın riski nedir?

Evcil hayvan adlarını, doğum yerlerini ve annenin kızlık soyadını herkese açık paylaşmak, hırsızlara yaygın hesap kurtarma sorularının cevaplarını verir.

Q9: Biyometrik girişler kimlik profillerini nasıl korur?

Biyometri, girişleri parmak izi veya yüz gibi özelliklere bağlar; cihazda tutulduğunda çalınması zordur, ancak depolanan biyometrik veriler sızabilir.

Q10: Red Flags Rule kimlik hırsızlığıyla nasıl mücadele eder?

Finansal kuruluşların kimlik hırsızlığı uyarı işaretlerini tespit etmek ve bunlara yanıt vermek için yazılı programlar geliştirmesini zorunlu kılan federal düzenleme.

Bölüm 11: Siber güvenlikle ilgili 10 gerçek dünya gerçeği ve içgörüsü

Güvenlik ihlalleri, savunma mekanizmaları ve uyumluluk standartlarıyla ilgili gerçek dünya bilgilerini incele.

1. GÜVENLİK İPUCU

FTC tarafından işletilen IdentityTheft.gov, ABD'li mağdurların kimlik hırsızlığını bildirmesine ve kişisel bir kurtarma planı almasına olanak tanır. [1]

2. GÜVENLİK İPUCU

Donanım güvenlik anahtarları, CISA'nın önerdiği en güçlü MFA türü olan kimlik avına dayanıklı MFA'dır. [4]

3. GÜVENLİK İPUCU

Ele geçirilmiş parolalar veri ihlallerinde yaygın bir giriş noktasıdır ve sonraki kimlik dolandırıcılığını besler.

4. GÜVENLİK İPUCU

Kredi dondurma federal yasalara göre ücretsizdir ve kredi dosyası kilidi açılana kadar borç verenlerin dosyayı kontrol etmesini engeller. [2]

5. GÜVENLİK İPUCU

DMARC, alan adı sahiplerinin posta sunucularına denetimlerden geçemeyen sahte e-postaları reddetmelerini veya karantinaya almalarını söylemesine olanak tanır. [7]

6. GÜVENLİK İPUCU

SIM değiştirme, bilgisayar korsanlarının bankacılık portallarındaki SMS tabanlı iki faktörlü kimlik doğrulamayı aşmasına olanak tanır.

7. GÜVENLİK İÇGÖRÜSÜ

Sentetik kimlik dolandırıcılığı gerçek ve sahte ayrıntıları karıştırır ve borç verenlerin tespit etmesini zorlaştırır.

8. GÜVENLİK İÇGÖRÜSÜ

Birçok kişi çevrimiçi hesaplarında aynı parolayı yeniden kullanır; bu yüzden tek bir ihlal birkaçını birden açığa çıkarabilir.

9. GÜVENLİK İÇGÖRÜSÜ

Veri komisyoncuları çok sayıda tüketici hakkında ayrıntılı dosyalar derleyerek yoğunlaşmış bir gizlilik riski oluşturur.

10. GÜVENLİK İPUCU

Kimlik hırsızlığından kurtulmak, itiraz edilen ücretler ve düzeltilen kredi raporları gibi aylar süren çalışma gerektirebilir.

Teknik Referanslar ve Kaynaklar

Çalışma kılavuzu ve etkileşimli bulmacalar, küresel NIST, OWASP ve veri gizliliği uyum standartlarından derlenmiştir.

AKADEMİK VE SEKTÖREL KAYNAKLAR

[1] Federal Trade Commission. (n.d.). IdentityTheft.gov: Report identity theft and get a recovery plan.

https://www.identitytheft.gov/

[2] Federal Trade Commission. (2025). Credit Freezes and Fraud Alerts.

https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts

[3] Federal Trade Commission. (n.d.). What To Know About Identity Theft.

https://consumer.ftc.gov/articles/what-know-about-identity-theft

[4] CISA. (n.d.). More than a Password.

https://www.cisa.gov/MFA

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[6] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.

https://pages.nist.gov/800-63-4/sp800-63b.html

[7] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).

https://www.rfc-editor.org/rfc/rfc7489.html

Cevap Anahtarı: Kontrol Noktası 1 - Çoktan Seçmeli

1 **Soru 1** — **Doğru cevap: A**

ÖĞRETMEN NOTU

Kimlik hırsızlarının oturum açma bilgilerini çalmak için kullandığı başlıca yöntem nedir? → Kullanıcıları sahte portallarda parola girmeye kandırmak için sahte e-posta uyarıları göndermek

2 **Soru 2** — **Doğru cevap: A**

ÖĞRETMEN NOTU

Hangi güvenlik kontrolü kimlik bilgisi sızıntılarına karşı en güçlü savunmayı sağlar? → Donanım anahtarları kullanan çok faktörlü kimlik doğrulama

3 **Soru 3** — **Doğru cevap: A**

ÖĞRETMEN NOTU

Kredi dondurmayı ne temsil eder? → Hırsızların izinsiz kredi açmasını önlemek için kredi raporlarını kilitlemek

4 **Soru 4** — **Doğru cevap: A**

ÖĞRETMEN NOTU

Dark web izlemesi neden yararlıdır? → Sızdırılmış kimlik bilgileri yasa dışı veritabanlarında göründüğünde kullanıcıları uyarır

5 **Soru 5** — **Doğru cevap: A**

ÖĞRETMEN NOTU

Sosyal mühendislik ne anlama gelir? → İnsanları gizli kimlik bilgilerini gönüllü olarak vermeye yönlendirmek

Cevap Anahtarı: Kontrol Noktası 2 - Doğru veya Yanlış

6 **Soru 6** — **Doğru cevap: Yanlış**

ÖĞRETMEN NOTU

Kimlik hırsızlığı, çalınan posta veya belgeler gibi çevrimdışı da başlayabilir.

7 **Soru 7** — **Doğru cevap: Doğru**

ÖĞRETMEN NOTU

Tüm kişisel hesaplarda MFA'yı zorunlu kılmak, kimlik bilgisi doldurma botu saldırılarının çoğunu engeller.

8 **Soru 8** — **Doğru cevap: Yanlış**

ÖĞRETMEN NOTU

Kredi dondurma yeni kredi sorgularını durdurur, ancak mevcut hesaplarını etkilemez.

9 **Soru 9** — **Doğru cevap: Doğru**

ÖĞRETMEN NOTU

Parola yöneticileri, sahte alan adlarında parolaları otomatik doldurmayı reddederek kullanıcıları kimlik avından korur.

10 **Soru 10** — **Doğru cevap: Doğru**

ÖĞRETMEN NOTU

Kimlik avı e-postaları, duygusal ve hızlı tepkileri tetiklemek için sıklıkla aciliyet bildiren bir dil kullanır.

Kelime anahtarları ve puanlama ölçeği

Öğretmen notlandırma ölçeği: 1 puan ver — doğru her eşleştirme için (toplam 8 puan) ve her bağlam terimi için (toplam 6 puan).

KONTROL NOKTASI 4: CEVAP ANAHTARI – KAVRAM EŞLEŞTİRME

H 1. KİMLİK BİLGİLERİ	D 2. SIZINTILAR	A 3. MFA	G 4. İZLEME
C 5. DONDURMA	E 6. SAVUNMA	B 7. SAHTEKÂRLIK	F 8. KİMLİK AVI

KONTROL NOKTASI 3: CEVAP ANAHTARI – ANAHTAR TERİMLER

1 HESAP BİLGİLERİ	2 SIZINTILAR	3 ÇOK FAKTÖRLÜ	4 İZLEME
5 DONDURMA	6 SAVUNMA		

KONTROL NOKTASI 6, ALTERNATİF: CEVAP ANAHTARI – KELİME EŞLEŞTİRME

1 H – KİMLİKAVI	2 A – HESAPBİLGİLERİ	3 G – TAKLİT	4 F – SAVUNMA
5 D – İZLEME	6 E – DONDURMA	7 B – SIZINTILAR	8 C – ÇOKFAKTÖRLÜ

EĞİTMENLER İÇİN TARTIŞMA NOTLARI

Anahtar terimler:
Öğrencilerin KİMLİK BİLGİLERİ, SIZINTILAR ve MFA terimlerini kendi sözcükleriyle açıklayıp her biri için bir örnek verebildiğini kontrol et.

Vaka çalışmaları:
Öğrencilerden önerilerini varsayımlarla değil, çalışma kâğıdındaki bilgilerle desteklemelerini iste.

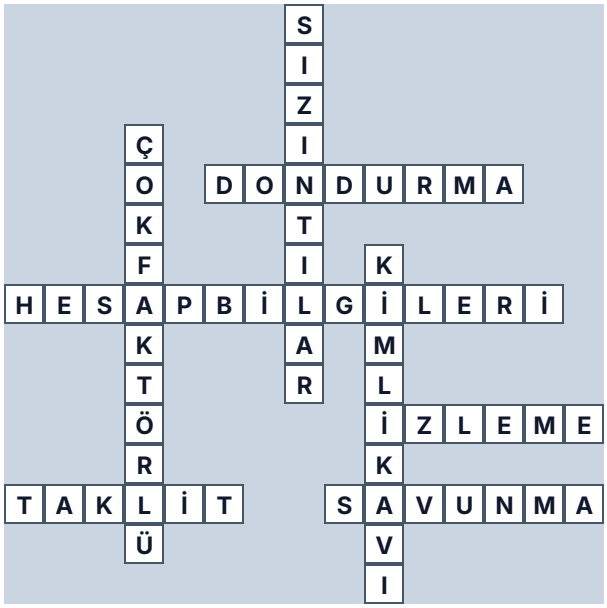
Kaynakların değerlendirilmesi:
Öğrencilerden çalışma kâğıdının kaynaklarında en az bir iddiayı doğrulamalarını iste ve rakamların, fiyatların ve kuralların zamanla neden değişebileceğini tartışın.

Bulmaca anahtarları ve öğretmen notları

KELİME BULMACA ÇÖZÜMÜ



BULMACA ÇÖZÜMÜ



BULMACA ÇÖZÜMLERİ İÇİN ÖĞRETMEN REHBERİ

SOLDAN SAĞA

3 soldan sağa: DONDURMA Hileli kredi başvurularını önlemek için kredi dosyalarına erişimi kısıtlama. (8 harf)

5 soldan sağa: HESAPBİLGİLERİ Dijital kimlikleri doğrulamak için kullanılan kullanıcı adları, parolalar ve özel jetonlar. (14 harf)

6 soldan sağa: İZLEME Çalınmış kurumsal verileri bulmak için çevrimiçi forumları ve hacker kanallarını tarama. (6 harf)

7 soldan sağa: TAKLİT Meşru bir kuruluşu taklit eden sahte bir web sitesi veya e-posta oluşturma. (6 harf)

8 soldan sağa: SAVUNMA Kimlik hırsızlığına karşı korunmak için kullanılan eğitim ve teknik kontroller. (7 harf)

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: SIZINTILAR Kişisel kullanıcı kayıtlarını içeren özel veritabanlarının yetkisiz biçimde açığa çıkması. (10 harf)

2 yukarıdan aşağı: ÇOKFAKTÖRLÜ Hesap girişlerini koruyan ikincil doğrulama adımı (donanım anahtarları gibi). (11 harf)

4 yukarıdan aşağı: KİMLİKAVI Kullanıcıları kimlik bilgilerini vermeye kandırmak için sahte mesajlar gönderme. (9 harf)

Karışık Kelimeler ve Şifre Çözüm Anahtarı

Kelime karıştırma etkinliği ve Gizli Şifre Görevi için notlandırma anahtarı.

KELİME KARIŞTIRMA ANAHTARI

1.	LBLİİSEGEHRİPA	HESAPBİLGİLERİ	5.	LTRIIINSAZ	SIZINTILAR
2.	AÜOÇLKKRÖTF	ÇOKFAKTÖRLÜ	6.	MEİLEZ	İZLEME
3.	DODURAMN	DONDURMA	7.	SMNAAUV	SAVUNMA
4.	TLKİTA	TAKLİT	8.	İİVKLİKAM	KİMLİKAVI

GİZLİ ŞİFRE GÖREVİ CEVAP ANAHTARI

"DİJİTAL KİMLİĞİNİ ÇOK FAKTÖRLÜ DOĞRULAMAYLA KORU"

Vaka çalışmaları cevap anahtarı

A Vaka Çalışması 1: Yönetici Kimliğine Bürünmeye Karşı Koruma

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Üst düzey bir yönetici, müşterileri dolandırmak için kişisel e-postasını taklit eden yazım hatalı alan adlarının hedefi oldu. Bir marka koruma planı tasarla.
- Önerilen Strateji ve Çözüm: Yöneticinin adının yaygın tüm yazım varyantlarını kaydet. Alan adı sahtekârlığını önlemek için e-posta kimlik doğrulama protokollerini (DMARC, DKIM, SPF) devreye al. Tüm üst düzey yönetici kurumsal girişlerinde donanım tabanlı MFA uygula.

B Vaka Çalışması 2: Kurumsal Kimlik Bilgilerinin Dark Web'de Açığa Çıkması

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Bir karanlık ağ veritabanı dökümü, bir kuruluşun sistem yöneticilerine ait birkaç yüz kurumsal kimlik bilgisi içeriyor. Bir azaltma stratejisi tasarla.
- Önerilen strateji ve çözüm: Şirket genelinde parola sıfırlaması yap. Kurumsal bir parola yöneticisi kullanımını zorunlu kıl. Tüm sistem portallarında MFA uygula ve sürekli, otomatik karanlık ağ izleme uyarıları kur.