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

Çevrimiçi dolandırıcılık ve sosyal mühendislik Koruma rehberi

E-posta kimlik avı, sahte alan adları, sesli kimlik avı (vishing), destek dolandırıcılıkları, bant dışı doğrulama, BEC

ÇEVRİMİÇİ DOLANDIRICILIĞA GENEL BAKIŞ

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 çevrim içi dolandırıcılığa karşı savunma konusunda rehberlik eder. Sahte kimlik avı web sitelerini, sosyal mühendislik taktiklerini, destek dolandırıcılıklarını, havale dolandırıcılığı yollarını ve ödeme doğrulama yöntemlerini 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/cevrimici-dolandiricili/

Çevrimiçi Dolandırıcılıktan Korunma Öğrenme Yol Haritan

- Destek dolandırıcılıklarının ve typosquatting alan adlarının yaygın göstergelerini belirle.
- Sahteciliğe karşı e-posta doğrulama protokolleri (SPF, DKIM, DMARC) uygula.
- İşletme havale dolandırıcılığını önlemek için bant dışı işlem doğrulaması oluştur.

ÇEVRİMİÇİ DOLANDIRICILIK REHBERİ YÖNERGELERİ

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: çevrimiçi dolandırıcılık koruması. Hızlı Düşün bonus etkinliğiyle bitir.

ÇEVRİMİÇİ DOLANDIRICILIK VE SOSYAL MÜHENDİSLİKTEN KORUNMA (GİRİŞ)

Çevrimiçi dolandırıcılıklar, kimlik avı, destek açılır pencereleri, sesli kimlik avı (vishing) ve banka havalesi dolandırıcılığı yoluyla insan davranışını istismar eder. Bant dışı işlem doğrulaması ve SPF/DKIM/DMARC alan adı kurallarını uygulamak, sosyal mühendislik yöntemlerini ağ geçidinde engellemeye yardımcı olur.

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

Kontrol Noktası 1: Çoktan seçmeli görev

1. Teknik destek dolandırıcılığının başlıca göstergesi nedir?

- A. Sisteminizin virüslü olduğunu iddia eden ve bir telefon numarasını aramanızı talep eden açılır pencere
- B. Resmî bir kayıt defterinden indirilen otomatik güvenlik güncellemesi
- C. Bir parola yöneticisinin kurumsal alan adında kimlik bilgilerini doldurmayı reddetmesi
- D. Harici sürücü yapılandırmasında çalışan arka plan dosya yedeklemesi

2. Banka bilgilerini çalmak için sahte gönderen alan adlarını hangi teknik kullanır?

- A. E-posta kimlik avı
- B. Port taraması
- C. Bellek enjeksiyonu
- D. Şifreli imha

3. Havale dolandırıcılığını ne temsil eder?

- A. Sosyal mühendislik kullanarak kurbanları sahte kurumsal hesaplara para göndermeye kandırmak
- B. Fidye yazılımı yükleriyle sistem veritabanlarını şifrelemek
- C. SQL enjeksiyon komutlarıyla veritabanlarını sorgulamak
- D. Sistem dosyalarını çevrimdışı depolama disklerine yedeklemek

4. Dolandırıcılar neden sahte alışveriş siteleri oluşturur?

- A. Alıcıların kredi kartı bilgilerini ve ödeme kimlik bilgilerini çalmak için
- B. Korumalı alanda kötü amaçlı yazılım analizi veritabanı tablolarını barındırmak
- C. Çevrimiçi siparişlerin teslimatını hızlandırmak için
- D. Yeni web sitesi tasarımlarını ücretsiz test etmek için

5. Vishing ne anlama gelir?

- A. Kimlik bilgilerini çalmak için telefon ağları üzerinden yapılan sesli kimlik avı dolandırıcılıkları
- B. Güvenli olmayan sistem cihazları için yerel ağları taramak
- C. Yetkisiz bir ihlalden sonra sistem veritabanlarını geri yüklemek
- D. Güvenilmeyen kodu güvenli sanal konteynerlerde çalıştırmak

Kontrol Noktası 2: Doğru/Yanlış görevi

6 Soru 6

6. Kimlik avı dolandırıcılıkları yalnızca son kullanıcıları hedef alır, üst düzey yönetici (whaling) hedeflerini asla.

○ Doğru ○ Yanlış

7 Soru 7

7. Sahte alan adları, güvenilir markaları taklit etmek için sıklıkla küçük yazım hataları (amaz0n.com gibi) kullanır.

○ Doğru ○ Yanlış

8 Soru 8

8. Destek dolandırıcılıkları, arayana uzaktan erişim verilerek çözülebilir.

○ Doğru ○ Yanlış

9 Soru 9

9. Sosyal mühendislik, güvenlik kurallarını aşmak için korku ve aciliyet gibi insan psikolojisinden yararlanır.

○ Doğru ○ Yanlış

10 Soru 10

10. Havale talepleri her zaman bant dışı iletişim kanalları kullanılarak doğrulanmalıdır.

○ Doğru ○ Yanlış

Kontrol Noktası 3: Anahtar terim yerleştirme

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

1. Kullanıcıları kandıran sahte e-postalara _____ denir.
2. Güvenilir markaların görünümünü kopyalayan web adreslerine _____ denir.
3. Banka bilgilerini hedef alan sesli dolandırıcılıklara _____ denir.
4. Virüs temizliği karşılığı para isteyen açılır pencere, bir destek tuzağıdır; bu tür düzenlere genel olarak _____ denir.
5. Bir ödeme talebini onaylamak, bant dışı _____ gerektirir.
6. İş işlemlerini hırsız hesaplarına yönlendirmek, _____ dolandırıcılığıdır.

KELİME BANKASI

BALİNA AVI · DOĞRULAMA · DOLANDIRICILIK · HAVALE · KİMLİK AVI · SMISHING · TAKLİT ADRES · VISHING

Cevaplarını buraya yaz:

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

Kontrol Noktası 4: Güvenlik kavramı eşleştirme

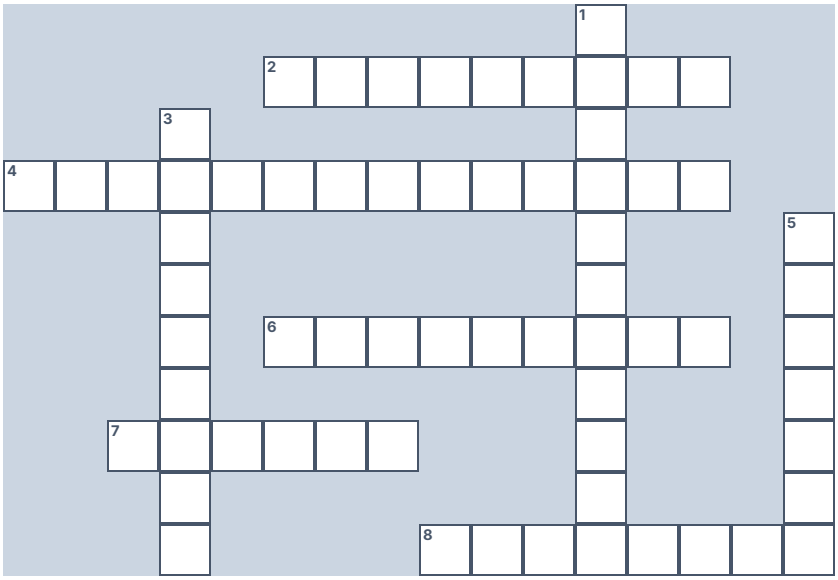
TANIM EŞLEŞTİRME

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

☐	1. KİMLİK AVI	A	Banka işlemlerinin hileli biçimde suçluların hesaplarına yönlendirilmesi.
☐	2. SAHTE	B	Mağdurlardan para veya erişim bilgilerini çalmak için tasarlanmış dolandırıcılık düzeni.
☐	3. VİŞİNG	C	Mobil hesap kimlik bilgilerini çalmak için dolandırıcılık amaçlı kısa mesajlar gönderme.
☐	4. DOLANDIRICILIK	D	Kimlik bilgilerini ve hesap ayrıntılarını çalmak için tasarlanmış sahte sesli aramalar.
☐	5. DOĞRULAMA	E	C seviyesi yöneticilerin kimlik bilgilerini çalmayı amaçlayan hedefli kimlik avı saldırıları.
☐	6. WIRE	F	Meşru görünmesi için taklit edilmiş e-posta göndericisi veya web sitesi adresi.
☐	7. WHALING	G	Oturum açma bilgilerini ve parolaları çalmak için tasarlanmış sahte e-posta kampanyaları.
☐	8. SMISHING	H	Ödeme ayrıntılarını güvenilir ikincil bir iletişim yöntemiyle doğrulama.

Kontrol Noktası 5: Bulmaca

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



SOLDAN SAĞA

2. Ödeme ayrıntılarını güvenilir ikincil bir iletişim yöntemiyle teyit etme. (9)

4. Kurbanlardan para veya kimlik bilgisi erişimi çalmak için tasarlanmış hileli düzen. (14)

6. Oturum açma bilgilerini ve parolaları çalmak için tasarlanmış hileli e-posta kampanyaları. (9)

7. Banka işlemlerinin hileli biçimde suçlu hesaplara yönlendirilmesi. (6)

8. Mobil hesap kimlik bilgilerini çalmak için dolandırıcılık amaçlı kısa mesajlar gönderme. (8)

YUKARIDAN AŞAĞI

1. Meşru görünecek şekilde taklit edilmiş e-posta göndericisi veya web sitesi adresi. (11)

3. Üst düzey yöneticilerin kimlik bilgilerini çalmayı hedefleyen hedefli kimlik avı saldırıları. (9)

5. Kimlik bilgilerini ve hesap ayrıntılarını çalmak için tasarlanmış hileli sesli aramalar. (7)

Kontrol Noktası 5, alternatif: Erişilebilir bulmaca ipuçları

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

SOLDAN SAĞA

2 soldan sağa: Ödeme ayrıntılarını güvenilir ikincil bir iletişim yöntemiyle teyit etme. (9 harf):

4 soldan sağa: Kurbanlardan para veya kimlik bilgisi erişimi çalmak için tasarlanmış hileli düzen. (14 harf):

6 soldan sağa: Oturum açma bilgilerini ve parolaları çalmak için tasarlanmış hileli e-posta kampanyaları. (9 harf):

7 soldan sağa: Banka işlemlerinin hileli biçimde suçlu hesaplara yönlendirilmesi. (6 harf):

8 soldan sağa: Mobil hesap kimlik bilgilerini çalmak için dolandırıcılık amaçlı kısa mesajlar gönderme. (8 harf):

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: Meşru görünecek şekilde taklit edilmiş e-posta göndericisi veya web sitesi adresi. (11 harf):

3 yukarıdan aşağı: Üst düzey yöneticilerin kimlik bilgilerini çalmayı hedefleyen hedefli kimlik avı saldırıları. (9 harf):

5 yukarıdan aşağı: Kimlik bilgilerini ve hesap ayrıntılarını çalmak için tasarlanmış hileli sesli aramalar. (7 harf):

Kontrol Noktası 6: Gizli kelime bulmacası

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

H I R Z R F Ö K U E A A Ö N L
S V O Ş V Ö İ İ P Ş D R Ç L Y
E A E B F R Ü M Ü I O A P Z Y
R A L Y V J G L H L Ğ P İ K K
D N A S I N Ğ İ Ö Ö R G Z A N
A İ V T S F T K C Y U P Y B Ğ
T L A K H Z G A I M L O M Ü C
İ A H K I Z Y V F V A N U T J
L B T O N B M I U S M K G T Ç
K Y T İ G P B Ü Z V A K P Ö V
A D O L A N D I R I C I L I K
T H N D A Ç İ Ö U Ü Ü J I Ğ Ş
Ğ F S M I S H I N G 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 Ğ L Ğ P

KELİME LİSTESİ

KİMLİKAVI, TAKLİTADRES, VISHING, DOLANDIRICILIK, DOĞRULAMA, HAVALE, BALİNAAVI, SMISHING

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. KİMLİKAVI**
- **B. TAKLİTADRES**
- **C. VISHING**
- **D. DOLANDIRICILIK**
- **E. DOĞRULAMA**
- **F. HAVALE**
- **G. BALİNAAVI**
- **H. SMISHING**

TANIMLAR VE EŞLEŞTİRME ALANLARI

1. Meşru görünecek şekilde taklit edilmiş e-posta göndericisi veya web sitesi adresi.
2. Ödeme ayrıntılarını güvenilir ikincil bir iletişim yöntemiyle teyit etme.
3. Banka işlemlerinin hileli biçimde suçlu hesaplara yönlendirilmesi.
4. Mobil hesap kimlik bilgilerini çalmak için dolandırıcılık amaçlı kısa mesajlar gönderme.
5. Üst düzey yöneticilerin kimlik bilgilerini çalmayı hedefleyen hedefli kimlik avı saldırıları.
6. Kimlik bilgilerini ve hesap ayrıntılarını çalmak için tasarlanmış hileli sesli aramalar.
7. Oturum açma bilgilerini ve parolaları çalmak için tasarlanmış hileli e-posta kampanyaları.
8. Kurbanlardan para veya kimlik bilgisi erişimi çalmak için tasarlanmış hileli düzen.

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. **KİLİKAVIM** _____
2. **VSGNIHI** _____
3. **DLUOAARMĞ** _____
4. **NIVİAABAL** _____
5. **RADAKSİTTEL** _____
6. **DIINLLRICDOI KA** _____
7. **LHAEVA** _____
8. **SMHGSNII** _____

Bonus etkinlik: Hızlı Düşün

HER KATEGORİ İÇİN 3 CEVAP. LİSTEYİ İLK TAMAMLAYAN KAZANIR.

1	Hacklenebilecek cihazlar			
2	Dolandırıcıların sık kullandığı ifadeler			
3	Dolandırıcıların istediği ödeme yöntemleri			
4	Çevrimiçi dolandırıcılık türleri			
5	Gerçek olamayacak kadar iyi teklifler			
6	Dolandırıcılığı bildireceğin yerler			
7	Siber güvenlikle ilgili sözcükler			
8	Dolandırıcılıklar konusunda uyarabileceğin kişiler			
9	Yedeklediğin şeyler			
10	E-postadaki uyarı işaretleri			
11	Bir bilgisayarın virüslü olduğunu gösteren işaretler			
12	Bir çevrimiçi mağazayı kontrol etme yolları			
13	Hesaplarını koruma yolları			
14	Dolandırılırsan yapılacaklar			
15	Veri sızıntısından sonra yapılacaklar			

Kontrol Noktası 8: Siber güvenlik vaka çalışmaları

Öğrendiğin kavramları aşağıdaki gerçek dünya senaryolarını çözmek için uygula.

VAKA ÇALIŞMASI 1: KURUMSAL HAVALE DOLANDIRICILIĞINI ÖNLEME



Senaryo: Bir finans departmanı, sahte bir tedarikçi adresinden, gelecekteki fatura havalelerinin yeni bir yönlendirme numarasına gönderilmesini isteyen acil bir e-posta alıyor.

Tartışma sorusu: Havale dolandırıcılığı doğrulama politikasını özetle ve e-posta kimlik doğrulama engellerini belirt.

VAKA ÇALIŞMASI 2: YÖNETİCİYE YÖNELİK BALİNA AVI KİMLİK AVI OLAYI



Senaryo: Bir yönetici, güvenli bir yönetim kurulu toplantısı belgesi içerdiğini öne süren bir kimlik avı bağlantısına tıklayıp birincil kurumsal kimlik bilgilerini sahte bir portala giriyor.

Tartışma sorusu: Olay müdahale adımlarını ayrıntılı anlat ve yönetici oturum açma kayıtlarının nasıl denetleneceğini açıkla.

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

14 12 16 15 12 14 1 27 11

8 12 21 12 23 12 16 15 6 21 12 17 12

5 18 9 21 25 15 1 16 1 28 15 1 24 6 22 20 12 24

6 24

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: Çevrimiçi dolandırıcılık nedir?

Kurbanları para göndermeye veya kişisel kimlik bilgilerini vermeye kandırmak için dijital kanalları kullanan sahte düzen.

Q2: E-posta kimlik avının ana göstergesi nedir?

Aciliyet iddia eden (hesap askıya alma gibi) ve sizi resmî alan adıyla eşleşmeyen bir bağlantıya yönlendiren mesaj.

Q3: Typosquatting nedir?

Sahte kimlik avı siteleri barındırmak için popüler markaların yaygın yazım hatalarını içeren alan adları (amaz0n.com gibi) kaydetmek.

Q4: Teknik destek dolandırıcılığı nedir?

Bilgisayarınızın virüslü olduğunu iddia eden, sizi bir numarayı aramaya ve sahte temizlik yazılımı ya da uzaktan erişim hizmetleri için ödeme yapmaya yönlendiren açılır pencere. [1]

Q5: Vishing nedir?

Kurbanları banka hesabı veya oturum açma bilgilerini vermeye kandırmak için sesli telefon aramaları kullanan kimlik avı saldırıları.

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

Çevrimiçi tehditlerin azaltılmasına ilişkin sık sorulan soruları ve cevapları incele.

Q6: Telekomünikasyon dolandırıcılığı (wire fraud) ne demektir?

Satıcıları veya yöneticileri taklit ederek ödeme işlemlerinin dolandırıcılık hesaplarına yönlendirilmesi.

Q7: Whaling nedir?

Doğrudan üst düzey kurumsal yöneticiler gibi yüksek değerli hedefleri amaçlayan, son derece hedefli bir hedefli kimlik avı biçimi.

Q8: Smishing nedir?

Mobil cihazlara gönderilen, sahte portallara veya takip güncellemelerine yönlendiren bağlantı istemleri içeren dolandırıcılık kısa mesajları.

Q9: Bant dışı doğrulama neden kritiktir?

İşlem ayrıntılarını ayrı bir iletişim kanalıyla (telefon görüşmesi gibi) doğrular ve ele geçirilmiş e-posta zincirlerinden kaçınır.

Q10: Sahte emanet hesabı (escrow) dolandırıcılığı nasıl işler?

Dolandırıcılar sahte bir emanet hesabı (escrow) sitesi oluşturur, fonların güvenle tutulduğunu iddia eder, ardından alıcının havale ettiği depozitoyu çalar.

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: Dolandırıcılar banka havalesi dolandırıcılığı yürütmek için BEC'i (İş E-postası İhlali) nasıl kullanır?

Meşru bir çalışanın e-posta hesabını ele geçirir, fatura yazışmalarını izler ve dolandırıcılık amaçlı banka hesaplarını içeren güncellenmiş fatura bilgileri gönderirler.

Q2: Çevrimiçi dolandırıcılıklarda IDN homograf saldırılarının riski nedir?

Gerçek markaları taklit eden sahte alan adları kaydetmek için normal harflerle aynı görünen ASCII dışı karakterler (örneğin Kiril 'a') kullanma.

Q3: E-posta başlığı incelemesi dolandırıcılık tespitinde neden önemlidir?

Gerçek kaynak sunucu IP'sini ve SPF/DKIM doğrulama durumunu ortaya çıkarır; gönderen alan adının sahte olup olmadığını gösterir.

Q4: Teknik destek dolandırıcıları uzak masaüstü yazılımını nasıl istismar eder?

Kurbanın cihazına bağlanmak, kötü amaçlı yazılım yerleştirmek ve kayıtlı parolaları çalmak için AnyDesk veya TeamViewer gibi araçları kullanırlar.

Q5: Ön ödemeli dolandırıcılıkların amacı nedir?

Var olmayan büyük bir mali ödül karşılığında kurbanları peşin işlem ücreti ödemeye kandırma.

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: Dolandırıcılar hedefli kimlik avı için sosyal medya profillemesini nasıl kullanır?

İkna edici hedefli kimlik avı e-postaları hazırlamak için kurumsal organizasyon yapılarını ve çalışan adlarını derlerler.

Q7: Sahte web mağazaları neden yüksek indirimler sunar?

Alıcıları kredi kartı bilgilerini girmeye yönlendirmek ve kimlik bilgilerini yeniden kullanmak veya carding forumlarında satmak üzere ele geçirmek için.

Q8: DMARC kayıtları kimlik avı dolandırıcılıklarını nasıl engeller?

DMARC, alan adı sahiplerinin alıcılardan, hizalanmış SPF ve DKIM denetimlerinden geçemeyen postaları karantinaya almalarını veya reddetmelerini istemesine olanak tanır ve doğrudan sahtecilik girişimlerini engeller. [5]

Q9: Kimlik bilgisi toplama portallarının tehdidi nedir?

Microsoft 365 veya Google çalışma alanları gibi görünecek şekilde tasarlanmış, girilirken oturum açma kimlik bilgilerini çalan sahte giriş sayfaları.

Q10: Güvenlik ekipleri dolandırıcılık alan adlarını nasıl bildirir ve devre dışı bırakır?

Dolandırıcılık kanıtlarını kayıt şirketinin kötüye kullanım e-postasına, barındırma sağlayıcısına ve Google Safe Browsing kaydına göndererek.

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

Kimlik avı ve sahtecilik, 2025'te FBI'ın IC3'üne en çok bildirilen suç türüydü ve 191.561 şikâyet vardı. [2]

2. GÜVENLİK İPUCU

İş E-postası Dolandırıcılığı (BEC), 2025'te FBI'ın IC3'üne bildirilen 3 milyar $'ın üzerinde zarara neden oldu. [2]

3. GÜVENLİK İPUCU

Yazım hatası tuzağı alan adları gerçek marka adlarından bir iki karakterle ayrılır; bu yüzden hızlı bir bakışta gözden kaçabilir.

4. GÜVENLİK İPUCU

Teknik destek dolandırıcılıkları, 2025'te FBI'ın IC3'üne bildirilen 2,1 milyar $'dan fazla zarara neden oldu. [2]

5. GÜVENLİK İPUCU

Homograf saldırıları, tarayıcı punycode yapılandırmalarını göstermedikçe tarayıcı adres çubuklarında birebir aynı görünür.

6. GÜVENLİK İPUCU

SMS metin dolandırıcılıkları (smishing), bağlantı içeren kısa ve acil mesajlar kullanır; bu da kurbanlara dolandırıcılığı fark etmek için çok az bağlam bırakır.

7. GÜVENLİK İÇGÖRÜSÜ

Whaling saldırıları, büyük ödeme havalelerine erişimi kontrol ettikleri için yönetici e-postalarını hedef alır.

8. GÜVENLİK İÇGÖRÜSÜ

Ödeme değişikliklerini bilinen, kayıtlı bir telefon numarasını arayarak doğrulamak, BEC havale dolandırıcılığına karşı temel bir savunmadır.

9. GÜVENLİK İÇGÖRÜSÜ

Sahte emanet hesabı (escrow) web siteleri çevrimiçi pazar yerlerinde yaygın bir dolandırıcılıktır: güvenli bir ödeme hizmeti gibi görünürler ancak alıcının havalesini çalarlar.

10. GÜVENLİK İPUCU

Google Safe Browsing, kimlik avı veya kötü amaçlı yazılım nedeniyle işaretlediği siteleri açmadan önce kullanıcıları uyarır.

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.). How To Spot, Avoid, and Report Tech Support Scams.

https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

[2] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[3] 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

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] 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

Teknik destek dolandırıcılığının başlıca göstergesi nedir? → Sisteminizin virüslü olduğunu iddia eden ve bir telefon numarasını aramanızı talep eden açılır pencere

2 Soru 2

Doğru cevap: A

ÖĞRETMEN NOTU

Banka bilgilerini çalmak için sahte gönderen alan adlarını hangi teknik kullanır? → E-posta kimlik avı

3 Soru 3

Doğru cevap: A

ÖĞRETMEN NOTU

Havale dolandırıcılığını ne temsil eder? → Sosyal mühendislik kullanarak kurbanları sahte kurumsal hesaplara para göndermeye kandırmak

4 Soru 4

Doğru cevap: A

ÖĞRETMEN NOTU

Dolandırıcılar neden sahte alışveriş siteleri oluşturur? → Alıcıların kredi kartı bilgilerini ve ödeme kimlik bilgilerini çalmak için

5 Soru 5

Doğru cevap: A

ÖĞRETMEN NOTU

Vishing ne anlama gelir? → Kimlik bilgilerini çalmak için telefon ağları üzerinden yapılan sesli kimlik avı dolandırıcılıkları

Cevap Anahtarı: Kontrol Noktası 2 - Doğru veya Yanlış

6 **Soru 6**

Doğru cevap: Yanlış

ÖĞRETMEN NOTU

Yanlış: kimlik avı yöneticileri de hedef alır; whaling, üst düzey liderleri hedefleyen kimlik avıdır.

7 **Soru 7**

Doğru cevap: Doğru

ÖĞRETMEN NOTU

Sahte alan adları, güvenilir markaları taklit etmek için sıklıkla küçük yazım hataları (amaz0n.com gibi) kullanır.

8 **Soru 8**

Doğru cevap: Yanlış

ÖĞRETMEN NOTU

Yanlış: bir destek dolandırıcısına uzaktan erişim vermek, onun kötü amaçlı yazılım yerleştirmesine ve veri çalmasına olanak tanır.

9 **Soru 9**

Doğru cevap: Doğru

ÖĞRETMEN NOTU

Sosyal mühendislik, güvenlik kurallarını aşmak için korku ve aciliyet gibi insan psikolojisinden yararlanır.

10 **Soru 10**

Doğru cevap: Doğru

ÖĞRETMEN NOTU

Havale talepleri her zaman bant dışı iletişim kanalları kullanılarak doğrulanmalıdır.

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

G 1. KİMLİK AVI	F 2. SAHTE	D 3. VİŞİNG	B 4. DOLANDIRICILIK
H 5. DOĞRULAMA	A 6. WIRE	E 7. WHALING	C 8. SMISHING

KONTROL NOKTASI 3: CEVAP ANAHTARI – ANAHTAR TERİMLER

1 KİMLİK AVI	2 TAKLİT ADRES	3 VISHING	4 DOLANDIRICILIK
5 DOĞRULAMA	6 HAVALE		

KONTROL NOKTASI 6, ALTERNATİF: CEVAP ANAHTARI – KELİME EŞLEŞTİRME

1 B – TAKLİTADRES	2 E – DOĞRULAMA	3 F – HAVALE	4 H – SMISHING
5 G – BALİNAAVI	6 C – VISHING	7 A – KİMLİKAVI	8 D – DOLANDIRICILIK

EĞİTMENLER İÇİN TARTIŞMA NOTLARI

Anahtar terimler:
Öğrencilerin KİMLİK AVI, SAHTE ve VİŞİNG 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

H	I	R	Z	R	F	Ö	K	U	E	A	A	Ö	N	L
S	V	O	Ş	V	Ö	İ	İ	P	Ş	D	R	Ç	L	Y
E	A	E	B	F	R	Ü	M	Ü	I	O	A	P	Z	Y
R	A	L	Y	V	J	G	L	H	L	Ğ	P	İ	K	K
D	N	A	S	I	N	Ğ	İ	Ö	Ö	R	G	Z	A	N
A	İ	V	T	S	F	T	K	C	Y	U	P	Y	B	Ğ
T	L	A	K	H	Z	G	A	I	M	L	O	M	Ü	C
İ	A	H	K	I	Z	Y	V	F	V	A	N	U	T	J
L	B	T	O	N	B	M	I	U	S	M	K	G	T	Ç
K	Y	T	İ	G	P	B	Ü	Z	V	A	K	P	Ö	V
A	D	O	L	A	N	D	I	R	I	C	I	L	I	K
T	H	N	D	A	Ç	İ	Ö	U	Ü	Ü	J	I	Ğ	Ş
Ğ	F	S	M	I	S	H	I	N	G	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	Ğ	L	Ğ	P

BULMACA ÇÖZÜMÜ

							T							
				D	O	Ğ	R	U	L	A	M	A		
		B								K				
D	O	L	A	N	D	I	R	I	C	I	L	I	K	
		L								İ				V
		İ								T				I
		N		K	İ	M	L	İ	K	A	V	I		S
		A								D				H
	H	A	V	A	L	E				R				I
		V								E				N
		I					S	M	I	S	H	I	N	G

BULMACA ÇÖZÜMLERİ İÇİN ÖĞRETMEN REHBERİ

SOLDAN SAĞA

2 soldan sağa: DOĞRULAMA Ödeme ayrıntılarını güvenilir ikincil bir iletişim yöntemiyle teyit etme. (9 harf)

4 soldan sağa: DOLANDIRICILIK Kurbanlardan para veya kimlik bilgisi erişimi çalmak için tasarlanmış hileli düzen. (14 harf)

6 soldan sağa: KİMLİKAVI Oturum açma bilgilerini ve parolaları çalmak için tasarlanmış hileli e-posta kampanyaları. (9 harf)

7 soldan sağa: HAVALE Banka işlemlerinin hileli biçimde suçlu hesaplara yönlendirilmesi. (6 harf)

8 soldan sağa: SMISHING Mobil hesap kimlik bilgilerini çalmak için dolandırıcılık amaçlı kısa mesajlar gönderme. (8 harf)

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: TAKLİTADRES Meşru görünecek şekilde taklit edilmiş e-posta göndericisi veya web sitesi adresi. (11 harf)

3 yukarıdan aşağı: BALİNAAVI Üst düzey yöneticilerin kimlik bilgilerini çalmayı hedefleyen hedefli kimlik avı saldırıları. (9 harf)

5 yukarıdan aşağı: VISHING Kimlik bilgilerini ve hesap ayrıntılarını çalmak için tasarlanmış hileli sesli aramalar. (7 harf)

Karışık Kelimeler ve Şifre Çözüm Anahtarı

Kelime karıştırma etkinliği ve Gizli Şifre Görevi için notlandırma anahtarı.

KELİME KARIŞTIRMA ANAHTARI

1.	KİLİKAVIM	KİMLİKAVI	5.	RADAKSİTTEL	TAKLİTADRES
2.	VSGNIHI	VISHING	6.	DIINLLRICDOIKA	DOLANDIRICILIK
3.	DLUOAARMĞ	DOĞRULAMA	7.	LHAEVA	HAVALE
4.	NIVİAABAL	BALİNAAVI	8.	SMHGSNII	SMISHING

GİZLİ ŞİFRE GÖREVİ CEVAP ANAHTARI

"KİMLİK AVI GİRİŞİMLERİNİ DOĞRULAMAYLA TESPİT ET"

Vaka çalışmaları cevap anahtarı

A Vaka Çalışması 1: Kurumsal Havale Dolandırıcılığını Önleme

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Bir finans departmanı, sahte bir satıcı adresinden, gelecekteki fatura havalelerinin yeni bir yönlendirme numarasına yönlendirilmesini isteyen acil bir e-posta alır.
- Önerilen Strateji ve Çözüm: Tüm ödemeler için çift onay politikası uygula. Önceden kaydedilmiş bir telefon numarasıyla bant dışı doğrulama yap ve sahte alan adlarından gelen e-postaları ağ geçidinde engelle.

B Vaka Çalışması 2: Yöneticiye Yönelik Balina Avı Kimlik Avı Olayı

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Bir yönetici, güvenli bir yönetim kurulu toplantısı belgesi içerdiğini iddia eden bir kimlik avı bağlantısına tıklıyor ve sahte bir portala birincil kurumsal kimlik bilgilerini giriyor.
- Önerilen Strateji ve Çözüm: Yöneticinin cihazını izole et. Tüm kurumsal oturum belirteçlerini ve kimlik bilgilerini sıfırla. Veri çıkışı için erişim günlüklerini incele ve tüm girişlerde donanım tabanlı MFA uygula.