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

Kimlik avı saldırıları ve sosyal mühendislik

Hedefli kimlik avı, whaling dolandırıcılıkları, SPF/DKIM/DMARC protokolleri, gönderen sahteciliği ve çalışan güvenlik eğitimi.

KİMLİK AVI SALDIRILARINA 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 kimlik avı saldırıları ve sosyal mühendislik konusunda rehberlik eder. Hedefli kimlik avını, balina avcılığını (whaling), alan adı taklidini, SPF/DKIM/DMARC protokollerini, bağlantı güvenliğini ve çalışan farkındalık eğitimini 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-avi-saldirilari/

Kimlik Avını Azaltma Öğrenme Yol Haritan

- Yaygın kimlik avı, vishing ve destek açılır pencere dolandırıcılıklarını belirle.
- Bant dışı işlem doğrulama prosedürleri uygula.
- Sahte alan adlarını engellemek için SPF, DKIM ve DMARC kurallarını yapılandır.

KİMLİK AVI SALDIRILARI 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: e-posta kimlik doğrulaması. Hızlı Düşün bonus etkinliğiyle bitir.

KİMLİK AVI SALDIRILARI VE SOSYAL MÜHENDİSLİK (GİRİŞ)

Kimlik avı saldırıları, kullanıcı oturum açma bilgilerini toplamak için hedefli mesajlar, balina avı (whaling) dolandırıcılıkları ve alan adı sahteciliği kullanır. Kurumsal sistemleri güvence altına almak, bant dışı onay adımlarının yanı sıra ağ geçidinde SPF, DKIM ve DMARC kurallarının uygulanmasını gerektirir.

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

Kontrol Noktası 1: Çoktan seçmeli görev

1 **1. Hedefli kimlik avı (spear phishing) nedir?**

- A. Belirli bir kişiye veya kuruluşa göre uyarlanmış hedefli kimlik avı e-postası
- B. Milyonlarca rastgele adrese gönderilen geniş kapsamlı toplu e-posta
- C. Web sunucularını trafikle dolduran bir ağ saldırısı
- D. Kullanıcı kayıtlarını hedef alan bir veritabanı çıkarma tekniği

2 **2. Hangi protokol, sahtecilikle (spoofing) mücadele etmek için bir alan adının yetkili gönderim IP adreslerini DNS'te listelemesine olanak tanır?**

- A. SPF
- B. DKIM
- C. DMARC
- D. HTTPS

3 **3. Whaling saldırısı nedir?**

- A. Özellikle tanınmış kurumsal yöneticileri hedef alan kimlik avı kampanyası
- B. Veritabanı yedeklerini hedef alan bir SQL enjeksiyonu saldırısı
- C. Yerel ağ yönlendirici ekipmanlarının fiziksel hırsızlığı
- D. Otomatik bir kimlik bilgisi doldurma kaba kuvvet taraması

4 **4. DKIM ne işe yarar?**

- A. Gönderen özgünlüğünü doğrulamak için e-postalara kriptografik imza ekler
- B. Gelen ağ paketi trafiğini güvenlik duvarında engeller
- C. Veritabanı depolama birimlerini beklemede (at rest) şifreler
- D. E-posta eklerini imza tabanlı kötü amaçlı yazılımlar için tarar

5 **5. DMARC'ın rolü nedir?**

- A. Alıcı e-posta sunucularına başarısız SPF/DKIM kontrollerinin nasıl ele alınacağını bildirmek
- B. Önceden hesaplanmış gökkuşağı tablolarıyla sistem parolalarının şifresini çözmek
- C. E-posta eklerini teslimattan önce sıkıştırmak
- D. Ağ yönlendirme erişim ayrıcalıklarını yapılandırmak

Kontrol Noktası 2: Doğru/Yanlış görevi

6 Soru 6

6. Hedefli kimlik avı (spear phishing), milyonlarca rastgele adrese gönderilen genel toplu e-postalara dayanır.

Doğru Yanlış

7 Soru 7

7. DMARC ilkeleri, posta sunucularına yetkisiz sahte iletileri reddetmelerini söyleyebilir.

Doğru Yanlış

8 Soru 8

8. SPF doğrulaması, e-posta gövdesinin kriptografik imzasını doğrulayarak çalışır.

Doğru Yanlış

9 Soru 9

9. Whaling saldırıları, veri tabanı dosyalarına erişmek için alt düzey kurumsal yöneticileri hedef alır.

Doğru Yanlış

10 Soru 10

10. Ödeme taleplerinin kanal dışı (out-of-band) doğrulanması, mali havale dolandırıcılıklarının durdurulmasına yardımcı olur.

Doğru Yanlış

Kontrol Noktası 3: Anahtar terim yerleştirme

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

1. Belirli bir çalışanı kişiselleştirilmiş bilgilerle hedeflemek _____ kimlik avıdır.

2. Mesajları meşru göstermek için e-posta üstbilgisini değiştirmek, gönderici adresiyle yapılan bir _____ eylemidir.

3. Yetkili posta sunucusu IP'lerinin DNS kayıt listesi: _____ .

4. Gönderici doğrulaması sağlayan e-posta imza standardı: _____ .

5. Başarısız SPF/DKIM kontrollerini reddetme politikaları oluşturmak _____ kullanır.

6. C düzeyi yöneticileri hedef alan kimlik avı kampanyasına _____ denir.

KELİME BANKASI

BALİNA AVI | DKIM İMZASI | DMARC | MIZRAK | SAHTECİLİK | SMISHING | SPF KAYDI | VISHING

Cevaplarını buraya yaz:

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

Kontrol Noktası 4: Güvenlik kavramı eşleştirme

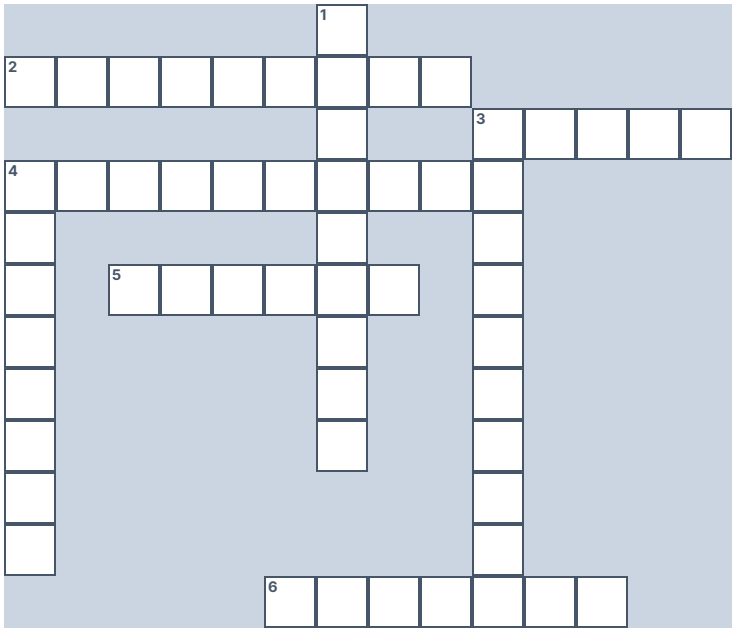
TANIM EŞLEŞTİRME

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

☐	1. HEDEFLİ	A	Ses tabanlı dolandırıcılık aramaları.
☐	2. SAHTEKÂRLIK	B	C seviyesi yöneticileri hedef alır.
☐	3. SPF	C	İlke reddi talimatları.
☐	4. DKIM	D	DNS yetkili gönderen IP'leri.
☐	5. DMARC	E	Sosyal mühendislik e-postası.
☐	6. WHALING	F	Kişiye özel hedefli e-posta.
☐	7. KİMLİK AVI	G	Gönderen e-posta adresini sahteleme.
☐	8. VİŞİNG	H	E-postadaki şifreleme imzası.

Kontrol Noktası 5: Bulmaca

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



SOLDAN SAĞA

2. Sosyal mühendislik e-postası (9)

3. Reddetme talimatlarını içeren politika (5)

4. Gönderici e-posta adresini taklit etme (10)

5. Kişiselleştirilmiş hedefli e-posta (6)

6. Sese dayalı dolandırıcılık aramaları (7)

YUKARIDAN AŞAĞI

1. Üst düzey yöneticileri hedef alma (9)

3. E-postadaki kriptografik imza (10)

4. Yetkili gönderici IP'lerini listeleyen DNS kaydı (8)

Kontrol Noktası 5, alternatif: Erişilebilir bulmaca ipuçları

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

SOLDAN SAĞA

2 soldan sağa: Sosyal mühendislik e-postası (9 harf):

3 soldan sağa: Reddetme talimatlarını içeren politika (5 harf):

4 soldan sağa: Gönderici e-posta adresini taklit etme (10 harf):

5 soldan sağa: Kişiselleştirilmiş hedefli e-posta (6 harf):

6 soldan sağa: Sese dayalı dolandırıcılık aramaları (7 harf):

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: Üst düzey yöneticileri hedef alma (9 harf):

3 yukarıdan aşağı: E-postadaki kriptografik imza (10 harf):

4 yukarıdan aşağı: Yetkili gönderici IP'lerini listeleyen DNS kaydı (8 harf):

Kontrol Noktası 6: Gizli kelime bulmacası

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

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

KELİME LİSTESİ

MIZRAK · SAHTECİLİK · SPFKAYDI · DKIMİMZASI · DMARC · BALİNAAVI · KİMLİKAVI · VISHING

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. MIZRAK**
- **B. SAHTECİLİK**
- **C. SPFKAYDI**
- **D. DKIMİMZASI**
- **E. DMARC**
- **F. BALİNAAVI**
- **G. KİMLİKAVI**
- **H. VISHING**

TANIMLAR VE EŞLEŞTİRME ALANLARI

1. Gönderici e-posta adresini taklit etme.
2. Kişiselleştirilmiş hedefli e-posta.
3. Sese dayalı dolandırıcılık aramaları.
4. Yetkili gönderici IP'lerini listeleyen DNS kaydı.
5. Sosyal mühendislik e-postası.
6. Reddetme talimatlarını içeren politika.
7. E-postadaki kriptografik imza.
8. Üst düzey yöneticileri hedef alma.

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. **ZMRAKI** _____
2. **KSIPDYAF** _____
3. **ADCRM** _____
4. **İIVLAKKİM** _____
5. **LCKATİESİH** _____
6. **SİMZADKMII** _____
7. **ABVIAİANL** _____
8. **IHGVNIS** _____

Bonus etkinlik: Hızlı Düşün

HER KATEGORİ İÇİN 3 CEVAP. LİSTEYİ İLK TAMAMLAYAN KAZANIR.

1	Hacklenebilecek cihazlar			
2	Kimlik avı e-postasının işaretleri			
3	Bir bilgisayarın virüslü olduğunu gösteren işaretler			
4	Sahte aciliyet yaratan sözcükler			
5	Göndereni kontrol etme yolları			
6	BT yardımı için sorabileceğin kişiler			
7	Yedeklediğin şeyler			
8	Bildiğin balıklar veya deniz canlıları			
9	Dolandırıcıların taklit ettiği şirketler			
10	Bugün başlayabileceğin güvenli alışkanlıklar			
11	Sahte bağlantıya tıkladıktan sonra yapılacaklar			
12	Veri sızıntısından sonra yapılacaklar			
13	Kimlik avının yaşandığı kanallar			
14	E-postayla asla göndermemen gereken şeyler			
15	Hesaplarını koruma yolları			

Kontrol Noktası 8: Siber güvenlik vaka çalışmaları

Öğrendiğin kavramları aşağıdaki gerçek dünya senaryolarını çözmek için uygula.

VAKA ÇALIŞMASI 1: ÜST YÖNETİMİ HEDEF ALAN BALİNA AVI SALDIRISINI GİDERME

👷

Senaryo: Bir Mali İşler Direktörü, gizli bir alan adı satın alımını tamamlamak için hızlıca 50.000 $ havale yapılmasını isteyen, CEO'dan geldiğini iddia eden son derece kişiselleştirilmiş bir e-posta alıyor.

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

VAKA ÇALIŞMASI 2: SPF/DKIM/DMARC AĞ GEÇİDİ POLİTİKALARINI UYGULAMA

👷

Senaryo: Bir kuruluş, giden pazarlama e-postaları sık sık spam olarak işaretlendiği ve hackerlar şirketin marka alan adını aktif olarak taklit ettiği için güvenlik denetimlerinde başarısız oluyor.

Tartışma sorusu: E-posta gerçekliğini doğrulamak için teknik ve yönetimsel denetimler oluştur.

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

22 18 22 28 1 15 16 26 10 6 17 5 12 22 15 12 9 12

6 20 18 22 24 1 5 6 17 6 24 12 16 12 28 15 6

2 25 15

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 avı nedir?

Kimlik avı, suçluların hassas verileri paylaşmaları için kullanıcıları kandırmak amacıyla sahte mesajlar gönderdiği bir sosyal mühendislik saldırısıdır.

Q2: Kimlik avı ile hedefli kimlik avı arasındaki fark nedir?

Kimlik avı, genel içerikle geniş grupları hedef alırken hedefli kimlik avı, özelleştirilmiş ayrıntıları kullanarak belirli kurbanları hedef alır.

Q3: Whaling nedir?

Whaling, yönetim yetkisine sahip üst düzey yöneticileri hedef alan, son derece hedefli bir kimlik avı saldırısıdır.

Q4: E-posta sahteciliği nedir?

E-posta sahteciliği, alıcıyı kaynağa güvenmesi için kandırmak amacıyla sahte gönderen adresiyle e-posta iletileri oluşturmaktır.

Q5: SPF sahteciliği nasıl önler?

DNS'te yetkili gönderen IP adreslerinin bir listesini yayımlar ve alıcı sunucuların posta kaynağını doğrulamasına olanak tanır. [1]

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

Çevrimiçi tehditlerin azaltılmasına ilişkin sık sorulan soruları ve cevapları incele.

Q6: DKIM nedir?

DomainKeys Identified Mail, e-posta başlıklarına kriptografik bir imza ekleyerek bir alan adının sorumluluğu üstlendiğini ve iletinin değiştirilmediğini kanıtlar.

Q7: DMARC neyin kısaltmasıdır?

Alan Adı Tabanlı İleti Kimlik Doğrulama, Raporlama ve Uyumluluk. [2]

Q8: DMARC politikası nedir?

Posta sunucularına SPF/DKIM doğrulamasını geçemeyen iletilere nasıl davranacaklarını (yok say, karantina veya reddet) bildiren politika. [2]

Q9: Vishing nedir?

Saldırganların yönetici veya finansal verileri almak için sahte telefon aramaları kullandığı ses tabanlı kimlik avı.

Q10: Bağlantı tarayıcıları nasıl yardımcı olur?

Gelen e-posta bağlantılarını tarar ve yeniden yazarlar; böylece tıklama anında hedef web sayfalarının güvenliğini doğrularlar.

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: Homograf saldırısı nasıl çalışır?

Saldırganlar, meşru bir alan adını görsel olarak taklit etmek için ASCII olmayan, benzer görünen Unicode karakterlerle alan adları kaydeder.

Q2: Punycode gösterimi nedir?

DNS'in işleyebilmesi için Unicode alan adlarını 'xn--' ile başlayan ASCII uyumlu dizelere dönüştüren kodlama.

Q3: 'p=reject' neden en güvenli DMARC durumudur?

Alıcı sunuculardan SMTP oturumu sırasında DMARC'ı (hizalanmış SPF/DKIM) geçemeyen postaları reddetmesini ister ve doğrudan sahtekârlığı engeller. [2]

Q4: Saldırganlar SPF kurallarını nasıl atlatır?

Benzer görünen alan adlarını (typosquatting) kullanarak veya meşru üçüncü taraf posta hizmetlerindeki ele geçirilmiş hesapları kullanarak.

Q5: İş e-postası ihlali (BEC) nedir?

Saldırganların sahte ödemeleri onaylamak için iş e-postası hesaplarını ele geçirdiği veya taklit ettiği kurumsal dolandırıcılık.

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: Çok faktörlü kimlik doğrulama kimlik avını nasıl durdurur?

Yalnızca benzer görünümlü giriş sayfalarıyla çalınamayan ikincil belirteçler (donanım anahtarları gibi) gerektirir.

Q7: Kimlik bilgisi toplama açılış sayfası nedir?

Girilen kullanıcı adlarını, parolaları ve MFA belirteçlerini gerçek zamanlı yakalamak için tasarlanmış, birebir benzeyen sahte oturum açma portalı.

Q8: Alt alan adı kaçırma nedir?

Bir saldırganın kullanılmayan bir DNS alt alan adı işaretçisinin denetimini ele geçirerek güvenilir bir üst alan adı altında kötü amaçlı kimlik avı açılış sayfaları barındırması.

Q9: DKIM hizalama kontrolü nasıl çalışır?

'From' başlığındaki alan adının, DKIM başlığında iletiyi kriptografik olarak imzalayan alan adıyla eşleştiğini doğrular.

Q10: E-posta ağ geçidinin rolü nedir?

Gelen e-postayı filtreleme, bağlantıları denetleme, ekleri korumalı alanda çalıştırma ve SPF/DKIM/DMARC uyumluluğunu doğrulama.

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. [4]

2. GÜVENLİK İPUCU

İş e-postası dolandırıcılığı (BEC), 2025'te FBI'ın IC3'üne bildirilen 3 milyar $'ın üzerinde zarara neden oldu. [4]

3. GÜVENLİK İPUCU

Homograf saldırıları, tarayıcılarda tam eşleşen marka alan adlarını görsel olarak kopyalamak için Kiril alfabesindeki benzer harfleri kullanır.

4. GÜVENLİK İPUCU

'p=reject' ile bir alan adı, alıcılardan doğrulamayı geçemeyen postayı teslimat sırasında reddetmesini ister; spam olarak dosyalamasını değil. [2]

5. GÜVENLİK İPUCU

CEO'ları hedef alan whaling saldırıları genellikle gizli birleşmeler veya alan adı satın alımları için acil ödeme ister.

6. GÜVENLİK İPUCU

Kimlik bilgisi toplama portalları gerçek giriş sayfalarını kopyalar; böylece kurbanlar parolalarını doğrudan saldırganın formuna yazar.

7. GÜVENLİK İÇGÖRÜSÜ

CISA'nın ortak kimlik avı rehberi, DMARC, SPF, DKIM ve kimlik avına dirençli MFA ile birlikte kullanıcı eğitimini önerir. [3]

8. GÜVENLİK İÇGÖRÜSÜ

SPF değerlendirmesi DNS sorgulayan 10 terimle sınırlıdır; sınırın aşılması 'permerror' sonucu döndürür. [1]

9. GÜVENLİK İÇGÖRÜSÜ

FIDO2 donanım güvenlik anahtarları, uzaktan kimlik bilgisi toplamaya karşı kriptografik destekli koruma sağlar.

10. GÜVENLİK İPUCU

Kimlik avı, saldırganların bir kuruma ilk girişinin en yaygın yollarından biridir; bu yüzden düzenli farkındalık eğitimi etkili bir savunmadır.

Teknik Referanslar ve Kaynaklar

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

AKADEMİK VE SEKTÖREL KAYNAKLAR

[1] IETF. (2014). RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1.

https://www.rfc-editor.org/rfc/rfc7208.html

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

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

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

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

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

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

Cevap Anahtarı: Kontrol Noktası 1 - Çoktan Seçmeli

1 **Soru 1** — **Doğru cevap: A**

ÖĞRETMEN NOTU

Hedefli kimlik avı (spear phishing) nedir? → Belirli bir kişiye veya kuruluşa göre uyarlanmış hedefli kimlik avı e-postası

2 **Soru 2** — **Doğru cevap: A**

ÖĞRETMEN NOTU

SPF, bir alan adının yetkili gönderen sunucularını DNS'te yayımlar, böylece alıcılar zarf göndericisini kontrol edebilir.

3 **Soru 3** — **Doğru cevap: A**

ÖĞRETMEN NOTU

Whaling saldırısı nedir? → Özellikle tanınmış kurumsal yöneticileri hedef alan kimlik avı kampanyası

4 **Soru 4** — **Doğru cevap: A**

ÖĞRETMEN NOTU

DKIM ne işe yarar? → Gönderen özgünlüğünü doğrulamak için e-postalara kriptografik imza ekler

5 **Soru 5** — **Doğru cevap: A**

ÖĞRETMEN NOTU

DMARC'ın rolü nedir? → Alıcı e-posta sunucularına başarısız SPF/DKIM kontrollerinin nasıl ele alınacağını bildirmek

Cevap Anahtarı: Kontrol Noktası 2 - Doğru veya Yanlış

6 **Soru 6** — Doğru cevap: Yanlış

ÖĞRETMEN NOTU

Yanlış: hedefli kimlik avı (spear phishing), genel toplu kimlik avının aksine belirli kişilere göre uyarlanır.

7 **Soru 7** — Doğru cevap: Doğru

ÖĞRETMEN NOTU

DMARC ilkeleri, posta sunucularına yetkisiz sahte iletileri reddetmelerini söyleyebilir.

8 **Soru 8** — Doğru cevap: Yanlış

ÖĞRETMEN NOTU

Yanlış: SPF gönderen IP'yi DNS'e göre kontrol eder; kriptografik imzayı doğrulayan DKIM'dir.

9 **Soru 9** — Doğru cevap: Yanlış

ÖĞRETMEN NOTU

Yanlış: whaling, ödemeleri onaylayabilen ve hassas verilere erişebilen üst düzey yöneticileri hedef alır.

10 **Soru 10** — Doğru cevap: Doğru

ÖĞRETMEN NOTU

Doğru: ödeme taleplerini ayrı, bilinen bir kanal üzerinden doğrulamak havale dolandırıcılığını durdurmaya yardımcı olur.

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

F 1. HEDEFLİ	G 2. SAHTEKÂRLIK	D 3. SPF	H 4. DKIM
C 5. DMARC	B 6. WHALING	E 7. KİMLİK AVI	A 8. VİŞİNG

KONTROL NOKTASI 3: CEVAP ANAHTARI – ANAHTAR TERİMLER

1 MIZRAK	2 SAHTECİLİK	3 SPF KAYDI	4 DKIM İMZASI
5 DMARC	6 BALİNA AVI		

KONTROL NOKTASI 6, ALTERNATİF: CEVAP ANAHTARI – KELİME EŞLEŞTİRME

1 B – SAHTECİLİK	2 A – MIZRAK	3 H – VISHING	4 C – SPFKAYDI
5 G – KİMLİKAVI	6 E – DMARC	7 D – DKIMİMZASI	8 F – BALİNAAVI

EĞİTMENLER İÇİN TARTIŞMA NOTLARI

Anahtar terimler:
Öğrencilerin HEDEFLİ, SAHTEKÂRLIK ve SPF 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

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

BULMACA ÇÖZÜMÜ

						B								
K	İ	M	L	İ	K	A	V	I						
						L			D	M	A	R	C	
S	A	H	T	E	C	İ	L	İ	K					
P						N			I					
F		M	I	Z	R	A	K		M					
K						A			İ					
A						V			M					
Y						I			Z					
D									A					
I									S					
				V	I	S	H	I	N	G				

BULMACA ÇÖZÜMLERİ İÇİN ÖĞRETMEN REHBERİ

SOLDAN SAĞA

2 soldan sağa: KİMLİKAVI Sosyal mühendislik e-postası (9 harf)

3 soldan sağa: DMARC Reddetme talimatlarını içeren politika (5 harf)

4 soldan sağa: SAHTECİLİK Gönderici e-posta adresini taklit etme (10 harf)

5 soldan sağa: MIZRAK Kişiselleştirilmiş hedefli e-posta (6 harf)

6 soldan sağa: VISHING Sese dayalı dolandırıcılık aramaları (7 harf)

YUKARIDAN AŞAĞI

1 yukarıdan aşağı: BALİNAAVI Üst düzey yöneticileri hedef alma (9 harf)

3 yukarıdan aşağı: DKIMİMZASI E-postadaki kriptografik imza (10 harf)

4 yukarıdan aşağı: SPFKAYDI Yetkili gönderici IP'lerini listeleyen DNS kaydı (8 harf)

Karışık Kelimeler ve Şifre Çözüm Anahtarı

Kelime karıştırma etkinliği ve Gizli Şifre Görevi için notlandırma anahtarı.

KELİME KARIŞTIRMA ANAHTARI

1. ZMRAKI — **MIZRAK**
2. KSIPDYAF — **SPFKAYDI**
3. ADCRM — **DMARC**
4. İIVLAKKİM — **KİMLİKAVI**
5. LCKATİESİH — **SAHTECİLİK**
6. SİMZADKMII — **DKIMİMZASI**
7. ABVIAİANL — **BALİNAAVI**
8. IHGVNIS — **VISHING**

GİZLİ ŞİFRE GÖREVİ CEVAP ANAHTARI

"SOSYAL MÜHENDİSLİĞİ EPOSTA DENETİMİYLE BUL"

Vaka çalışmaları cevap anahtarı

A Vaka Çalışması 1: Üst Yönetimi Hedef Alan Balina Avı Saldırısını Giderme

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Bir Finans Direktörü, CEO'dan geldiği iddia edilen, gizli bir alan adı alımını kapatmak için hızlı bir $50,000 havale isteyen son derece kişiselleştirilmiş bir e-posta alır.
- Önerilen strateji ve çözüm: Sahte gönderen alan adlarını engellemek için DMARC'ı 'p=reject' ilkesiyle yapılandır. Ağ geçidinde harici gönderen uyarı bannerları ekle ve tüm mali işlemler için sözlü, bant dışı onay iste.

B Vaka Çalışması 2: SPF/DKIM/DMARC Ağ Geçidi Politikalarını Uygulama

Öğretmen çözümü

NOTLANDIRMA YÖNERGESİ

Öğrenci cevapları şu noktaları kapsamalıdır:

- Senaryo analizi: Bir kuruluş, giden pazarlama e-postaları sık sık spam olarak işaretlendiği ve bilgisayar korsanları şirketin marka alan adını aktif olarak taklit ettiği için güvenlik denetimlerinde başarısız oluyor.
- Önerilen Strateji ve Çözüm: Yetkili gönderen IP'lerini belirten bir SPF TXT kaydı yayımla. Giden posta sunucularında DKIM imzalama anahtarlarını yapılandır ve kötüye kullanımı belirlemek için gelen DMARC XML geri bildirim raporlarını analiz et.