Phishing Dedektifi — Güvenli E-posta Analizi

ÖĞRETMEN KILAVUZU

Kategori	Siber Güvenlik	Süre	1–2 ders saati
Seviye	Başlangıç	Hedef	Başlangıç seviye lise öğrencileri

Amaç

• Kimlik avı belirtilerini güvenli bir sınıf senaryosunda tanımak ve doğru bildirim davranışını geliştirmek.

Problem durumu

• Yanıltıcı e-postalar kullanıcıyı acele ettirip bağlantıya tıklamaya veya bilgi paylaşmaya yöneltebilir

Kazanımlar

• Gönderici alan adını inceler.

• Aciliyet ve tehdit dilini fark eder.

• Bağlantıya tıklamadan hedefi kontrol etmeyi açıklar.

• Güvenli bildirim adımlarını sıralar.

Hazırlık

• Phishing Dedektifi — Güvenli E-posta Analizi için örnek girdileri, güvenlik sınırlarını ve test ölçütlerini dersten önce kontrol etmek.

Araç / malzemeler

• Çevrimdışı sahte e-posta kartları

• Belirti kontrol listesi

Uygulama

1. Sahte örneği dağıt.
2. İpuçlarını tek tek işaretle.
3. Risk düzeyini gerekçelendir.
4. Güvenli tepki adımlarını yaz.
5. Sınıfla karşılaştır.

Test aşaması

1. Yazım hatalı sahte örnek
2. Görünüşü düzgün ama alan adı farklı örnek
3. Meşru bildirim örneği

Olası hatalar ve çözümler

• Bağlantıya tıklayarak test etmek: Girdiyi veya bağlantıyı tek tek doğrula; değişiklikten sonra aynı testi yeniden çalıştır.

• Yalnız yazım hatasına bakmak: Girdiyi veya bağlantıyı tek tek doğrula; değişiklikten sonra aynı testi yeniden çalıştır.

• Gönderici görünen adına güvenmek: Girdiyi veya bağlantıyı tek tek doğrula; değişiklikten sonra aynı testi yeniden çalıştır.

Güvenlik

• Gerçek bağlantı, credential formu veya gönderim altyapısı oluşturmayın.

• Gerçek kullanıcı adı/parola toplamayın.

• Şüpheli mesajı kurumun bilinen güvenli kanalından doğrulayın.

Öğretmen yönergeleri

• Hazır çözümü vermeden önce öğrenciden tahminini ve denediği adımı açıklamasını isteyin.

• Sonucu yalnız çalışıyor/çalışmıyor olarak değil; test kanıtı ve açıklamayla değerlendirin.

Geliştirme önerileri

• Sınıf güvenlik posteri

• Bildirim akış şeması

• Alan adı karşılaştırma kartları

Savunma kontrol listesi

Gönderici alan adı tutarlı mı?
Mesaj acil işlem baskısı kuruyor mu?
Bağlantının görünen metni ile hedefi uyuşuyor mu?
Parola veya ödeme bilgisi istiyor mu?
Doğrulama için bilinen resmi kanal kullanılabilir mi?