Kimlik Avı Saldırısı - Pishing Saldırıları

- Güncel PDF'i İndir
- En güncel eğitimlerimiz için www.vebende.com.tr ziyaret edin

Eğitim Süresi

- **Süre:** 1 gün
- **Ders Süresi:** 50 dakika
- **Eğitim Saati:** 10:00 - 17:00
- > Eğitim formatında eğitimler 50 dakika + 10 dakika moladır. 12:00-13:00 saatleri arasında 1 saat yemek arasındaki verilir. Günde toplam 6 saat eğitim verilir. 1 günlük formatta 6 saat eğitim verilmektedir.

- > Eğitimler uzaktan eğitim formatında tasarlanmıştır. Her eğitim için teams linkleri gönderilir. Katılımcılar bu linklere girerek eğitimlere katılırlar. Ayrıca farklı remote çalışma araçları da eğitmen tarafından tüm katılımlara sunulur. Katılımcılar bu araçları kullanarak eğitimlere katılırlar.

- > Eğitim içeriğinde github ve codespace kullanılır. Katılımcılar bu platformlar üzerinden örnek projeler oluşturur ve eğitmenle birlikte eğitimlerde sorulan sorulara ve taleplere uygun iceriğe cevap verir. Katılımcılar bu araçlarla eğitimlerde sorulan sorulara ve taleplere uygun iceriğe cevap verir.
- > Eğitim yapay zeka destekli kendi kendine öğrenme formasyonu ile tasarlanmıştır. Katılımcılar eğitim boyunca kendi kendine öğrenme formasyonu ile eğitimlere katılırlar. Bu eğitim formatı sayesinde tüm katılımcılar gelecek tüm yaşamlarında kendilerini güncellemeye devam edebilecekler ve her türlü sorunun karşısında çözüm bulabilecekleri yeteneklere sahip olacaklardır.

PHISHING SALDIRILARINA KARŞI FARKINDALIK EĞİTİMİ

Şirket çalışanlarınızın **phishing (oltalama) saldırılarına** karşı bilinçli olmasını sağlamak için kapsamlı bir eğitim programı sunuyoruz.
Bu eğitim kapsamında şunları öğreneceksiniz:

- **Phishing saldırı yöntemleri** ve saldırganların kullandığı taktikler,
- **E-posta güvenliği** ve şüpheli bağlantıları tespit etme yöntemleri,
- **Kimlik doğrulama ve erişim kontrolü** gibi güvenlik önlemleri,
- **Gerçek dünya senaryoları ile interaktif uygulamalar**.

Bu eğitim, **çalışanlarınızın dijital tehditlere karşı farkındalığını artırmak, güvenlik protokollerine uyumlarını güçlendirmek ve şirketinizin verilerini korumak** amacıyla tasarlanmıştır.

Eğitim Hedefi

Bu eğitimin amacı, **kurum çalışanlarının phishing saldırılarına karşı temel farkındalığını artırmak** ve **bu tür tehditleri tanıyıp etkili önlemler almalarını sağlamak**tır. Katılımcılar:

- **Phishing saldırılarının temel türlerini tanımlayabilecek**,
- **Şüpheli e-postaları ve sahte bağlantıları ayırt edebilecek**,
- **Güvenli parola yönetimi ve kimlik doğrulama yöntemlerini kullanabilecek**,
- **Phishing saldırılarına karşı alınması gereken adımları öğrenecek**,
- **Gerçekleşen bir saldırı durumunda nasıl hareket etmeleri gerektiğini bileceklerdir**.

Eğitim sonunda, katılımcılar **phishing saldırılarına karşı bilinçli ve proaktif** hale gelerek **kurumsal güvenliği güçlendiren bir yapı** oluşturacaklardır.

Eğitim İçeriği

PHISHING TEHDİTLERİNE KARŞI FARKINDALIK

1. Phishing Nedir?

- **Tanım:** Oltalama (phishing), kullanıcıları kandırarak kişisel verilerini toplamak için kullanılan bir dolandırıcılık yöntemidir.
- **Önemi:** Dijital bilgilerin güvenliğini sağlamak için phishing saldırılarını tanımak ve önlemek kritik bir öneme sahiptir.
- **Temel Kavramlar:**
  - **Oltalama E-postaları:** Sahte e-posta göndererek kullanıcıları tuzağa düşüren mesajlar.
  - **Kimlik Avı Siteleri:** Gerçek sitelerin kopyaları, kullanıcıların bilgilerini çalmak için oluşturulur.

2. Phishing Türleri

- **Email Phishing:** Kullanıcıları sahte e-posta ile kandırma.
- **SMS Phishing (Smishing):** Kısa mesaj yoluyla kişisel verilerin talep edilmesi.
- **VoIP Phishing (Vishing):** Sesli aramalarla dolandırıcılık yapma.
- **Spear Phishing:** Belirli bir kişiyi hedef alan daha ince ve kişisel dolandırıcılık yöntemleri.

3. Phishing Saldırılarına Karşı Korunma Yöntemleri

- **İletişim Dikkati:** Şüpheli e-postalara ve SMS'lere dikkat edilmesi.
- **Güvenli Bağlantılar:** HTTPS kullanılmayan sitelerden uzak durmak.
- **Eğitim ve Farkındalık:** Çalışanların düzenli olarak phishing saldırıları konusunda eğitilmesi.

4. Şüpheli İletişim Bildirimi

- **İleti Bildirimi:** Şüpheli e-posta veya mesajların şirket güvenlik ekiplerine bildirilmesi.

SİBER GÜVENLİK PROTOKOLLERİ

1. Temel Siber Güvenlik Prosedürleri

- **Parola Güçlendirme:** Parola oluşturma ve yönetim kuralları.
- **Güncellemeler ve Yamanlar:** Yazılımların sürekli güncellenmesi ve zayıflıkların onarılması.

2. Ağ Güvenliği Protokolleri

- **Firewall Kuralları:** İnternet trafiğini kontrol etme ve izleme.
- **Güvenlik Günlüğü Tutma:** Ağ aktivitelerinin kaydedilmesi ve analiz edilmesi.

3. Veri Gizliliği Standartları

- **KVKK ve GDPR Uyumluluğu:** Kişisel verilerin korunması ile ilgili düzenlemelere uyum sağlamak.

ACİL DURUM PLANI VE YANIT STRATEJİLERİ

1. Siber Olaylara Müdahale Planı

- **Olay Tanımlama:** Olayın tespiti ve sınıflandırılması süreçleri.
- **Müdahale Süreci:** Belirlenen adımlar ve sorumluluklar.

2. İletişim Stratejileri

- **İç ve Dış İletişim:** Olay sonrası hem iç hem de dış paydaşlarla iletişim kurma yöntemleri.

3. Olay Analizi ve Raporlama

- **Olay sonrası analiz ve gelişmiş raporların hazırlanması.**

EĞİTİM YÖNTEMİ

- **Teorik Bilgi:** Siber güvenlik kavramları, tehdit türleri ve korunma yöntemlerinin anlatımı.
- **Uygulamalı Geliştirme:** Gerçek hayattan alınan örnekler ve simülasyonlar yoluyla pratik uygulamalar.
- **Etkileşimli Tartışmalar:** Katılımcıların deneyimlerini paylaşacağı, siber güvenlikle ilgili güncel konuların tartışılacağı oturumlar.
- **Rol Oynama Senaryoları:** Katılımcıların çeşitli güvenlik senaryolarında rol alarak aktif katılım sağlaması ve pratik deneyim kazanması.
- **Ödevler ve Değerlendirme:** Eğitim süresince verilen ödevlerle katılımcıların öğrenimlerinin değerlendirilmesi.

HEDEF KİTLE

- **Kurum Çalışanları:** Temel bilgisayar kullanımı yapan tüm çalışanlar; güvenli bilgi işlem süreçlerini günlük işlerinde uygulamak ve öğrenmek isteyenler.
- **Sistem Yöneticileri ve IT Çalışanları:** Kurumun ağ güvenliği, veri koruması ve sistem yönetiminden sorumlu olan profesyoneller.
- **Yönetici ve Departman Liderleri:** Kurumun siber güvenlik politikalarını geliştirmek ve uygulamakla yükümlü olan yöneticiler.
- **Yeni Mezunlar ve Stajyerler:** Kariyerine siber güvenlik alanında adım atmak isteyen üniversite mezunları ve stajyerler.
- **Siber Güvenlik Uzmanları:** Yetkinliklerini artırmak ve güncel tehditlerle başa çıkma becerilerini geliştirmek isteyen profesyoneller.

KATILIMCILARDAN BEKLENTİLERİMİZ

- Katılımcıların temel bilgisayar bilgisine sahip olmaları, özellikle bilgi teknolojileri ile ilgili temel kavramlara dair bir anlayışlarının bulunması.
- Siber güvenlik konularında öğrenmeye açık olmaları ve güncel tehditler ile güvenlik önlemleri hakkında farkındalık oluşturmayı hedeflemeleri.
- Gruplar halinde etkin bir şekilde çalışabilmeleri ve etkileşimde bulunmaları.
- Eğitim sırasında düzenlenecek uygulamalara aktif katılım göstermeleri.

Eğitim Materyalleri (Eğitmenlere Özel)