KİMLİK AVI SALDIRISI ÖNLEME KONTROL LİSTESİ

Şirket çalışanlarınızın phishing saldırılarına karşı bilinçli olmasını sağlamak için kapsamlı bir eğitim programı sunuyoruz. Bu eğitim, phishing taktiklerinden e-posta güvenliğine, URL ve bağlantı korumasından kimlik doğrulama ve erişim kontrollerine kadar geniş bir bilgi yelpazesi sunmaktadır. Çalışanlarınızın dijital tehditlere karşı koruma bilincini artırmak, güvenlik protokollerine uyumlarını güçlendirmek ve şirketinizin verilerini korumak amacıyla özel olarak tasarlanmış bu eğitim, siber güvenliğinizi artırmak için önemli bir adım olacaktır.

KİMLİK AVI SALDIRISI ÖNLEME KONTROL LİSTESİ

KURUMSAL ÖZEL EĞİTİM

Bu konuyu istediğiniz gibi özelleştirebilirsiniz. Kullandığınız teknolojiye özel uygulamalar ile anlatılmasını, projenize uygun içerik haline getirilmesini ...

Vebende
Bilişim, Eğitim ve Danışmanlık

KİMLİK AVI SALDIRISI ÖNLEME KONTROL LİSTESİ

hishing saldırıları, kötü niyetli kişilerin, sahte e-postalar veya web siteleri aracılığıyla kişisel bilgileri çalmayı hedeflediği siber tehditlerdir. Genellikle bankalar, sosyal medya platformları veya tanınmış şirketleri taklit eden saldırganlar, kurbanları kandırarak şifre, kredi kartı bilgileri gibi hassas verileri ele geçirmeye çalışır.

Korunma Yöntemleri:

- E-posta Güvenliği: Şüpheli e-postaları açmayın ve asla kişisel bilgilerinizi isteyen e-postalara cevap vermeyin. URL'leri dikkatlice kontrol edin.
- Çift Faktörlü Kimlik Doğrulama (2FA): Özellikle banka ve sosyal medya hesaplarınızda 2FA kullanarak güvenliği artırın.
- Antivirüs Yazılımı: Kötü amaçlı yazılımlara karşı koruma sağlamak için güncel antivirüs yazılımları kullanın.
- Eğitim ve Farkındalık: Hem bireysel hem de kurumsal seviyede phishing saldırıları hakkında eğitimler düzenleyerek farkındalık oluşturun.

Phishing Türleri:

- Sahte E-postalar: Tanınmış kurumları taklit ederek şüpheli bağlantılarla kişisel bilgilerinizi çalmak.
- Sahte Web Siteleri: Gerçek web sitelerinin birebir kopyalarını kullanarak bilgilerinizi almak.
- Telefonla Phishing (Vishing): Telefonla kişisel bilgilerinizi istemek.

EĞİTİM HEDEFİ

Bu eğitim, çalışanlarınızı phishing (oltalama) saldırıları konusunda bilinçlendirerek, kurumun siber güvenliğini güçlendirmeyi amaçlamaktadır. Katılımcılar, phishing saldırılarının nasıl çalıştığını, bu saldırılardan nasıl korunabileceklerini ve güvenli dijital alışkanlıklar geliştirebileceklerini öğreneceklerdir.

EĞİTİM İÇERİĞİ

PHISHING TEHDİTLERİNE KARŞI FARKINDALIK

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

SİBER GÜVENLİK PROTOKOLLERİ

- Temel Siber Güvenlik Prosedürleri
  - Parola Güçlendirme: Parola oluşturma ve yönetim kuralları.
  - Güncellemeler ve Yamanlar: Yazılımların sürekli güncellenmesi ve zayıflıkların onarılması.
- Ağ Güvenliği Protokolleri
  - Firewall Kuralları: İnternet trafiğini kontrol etme ve izleme.
  - Güvenlik Günlüğü Tutma: Ağ aktivitelerinin kaydedilmesi ve analiz edilmesi.
- Veri Gizliliği Standartları
  - KVKK ve GDPR Uyumluluğu: Kişisel verilerin korunması ile ilgili düzenlemelere uyum sağlamak.

ACİL DURUM PLANI VE YANIT STRATEJİLERİ

- Siber Olaylara Müdahale Planı
  - Olay Tanımlama: Olayın tespiti ve sınıflandırılması süreçleri.
  - Müdahale Süreci: Belirlenen adımlar ve sorumluluklar.
- İletişim Stratejileri
  - İç ve Dış İletişim: Olay sonrası hem iç hem de dış paydaşlarla iletişim kurma yöntemleri.
- Olay Analizi ve Raporlama
  - Olay sonrası analiz ve gelişmiş raporların hazırlanması.

KİMLİK AVI SALDIRISI ÖNLEME KONTROL LİSTESİ

Giriş: Phishing (oltalama) saldırıları, kötü niyetli kişilerin, kurbanlarını kandırarak hassas bilgilerini çalmayı amaçladığı bir siber saldırı türüdür. E-posta, web sitesi, telefon veya sosyal medya platformları gibi çeşitli kanallar aracılığıyla yapılan bu saldırılar, kullanıcıları sahte mesajlar veya web siteleri ile kandırmayı hedefler. Phishing saldırıları, genellikle kullanıcı adı, şifre, kredi kartı bilgileri, kimlik bilgileri gibi değerli verilerin ele geçirilmesine neden olur.

Phishing Saldırısının Temel Özellikleri:
Sahte E-posta Gönderimleri: Phishing saldırılarının en yaygın türü, sahte e-posta göndermektir. Bu e-postalar genellikle tanınmış bir kurumu, banka, e-ticaret sitesi veya sosyal medya platformunu taklit eder. E-posta, genellikle acil bir işlem yapmanız gerektiğini belirten sahte uyarılar içerir ve kurbanı, sahte bir bağlantıya tıklamaya yönlendirir.
Sahte Web Siteleri: Phishing saldırıları, kurbanları kimlik bilgilerini girmeleri için kandırmak amacıyla gerçek web sitelerinin birebir kopyalarını oluşturur. Bu sahte siteler, tasarım açısından orijinal sitelere benzer, ancak URL genellikle küçük bir fark içerir.
Telefonla Phishing (Vishing): Telefonla yapılan oltalama saldırıları, genellikle bir bankadan veya tanınmış bir şirketten geliyormuş gibi davranarak kurbanlardan kişisel bilgilerini veya finansal bilgilerini almaya yönelik yapılır.
SMS Phishing (Smishing): Kurbanlara, sahte SMS mesajları gönderilir. Bu mesajlar genellikle bir aciliyet yaratır ve kurbanları bir bağlantıya tıklamaya veya bir numarayı aramaya zorlar.

Phishing saldırılarına karşı korunmak, bilinçli bir dijital vatandaş olmayı gerektirir. Güvenlik, dikkatli ve eğitimli kullanıcılar ile sağlanabilir.

EĞİTİM SÜRESİ

- 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.

EĞİTİM YÖNTEMİ

- Sunum ve Teorik Eğitim
  - Görsel İçerik: Phishing saldırıları ve korunma yöntemleri hakkında etkili ve görsel destekli sunumlar yapılır. Katılımcılara gerçek hayattan örnekler sunarak phishing saldırılarının nasıl çalıştığı ve nelere dikkat edilmesi gerektiği anlatılır.
- Etkileşimli Eğitim
  - Sahte E-posta Testleri: Katılımcılara sahte e-posta örnekleri sunulur ve bu e-postaların phishing olup olmadığını belirlemeleri istenir. Böylece katılımcılar gerçek zamanlı kararlar alarak dikkatli olma becerisi kazanır.
  - Canlı Senaryolar: Gerçek hayattan örneklerle, katılımcılar phishing saldırılarını tanıma ve doğru tepki verme konusunda etkileşimli senaryolarla test edilir.

HEDEF KİTLE

- IT ve Güvenlik Ekipleri
- Dijital İletişim ve Pazarlama Departmanları
- Yönetici ve Üst Düzey Yöneticiler
- Finans ve Muhasebe Departmanları
- İnsan Kaynakları ve İK Departmanları
- Tüm Çalışanlar

KATILIMCILARDAN BEKLENTİLERİMİZ

- Aktif Katılım
- Bilgi Paylaşımı ve Deneyim Paylaşımı
- Eğitim İçeriğini Uygulamak
- Eğitim Sonrası Bilgileri Geri Getirme ve Uygulama
- İleri Düzey Eğitim ve Sertifika Talepleri
- Geri Bildirim Sağlama

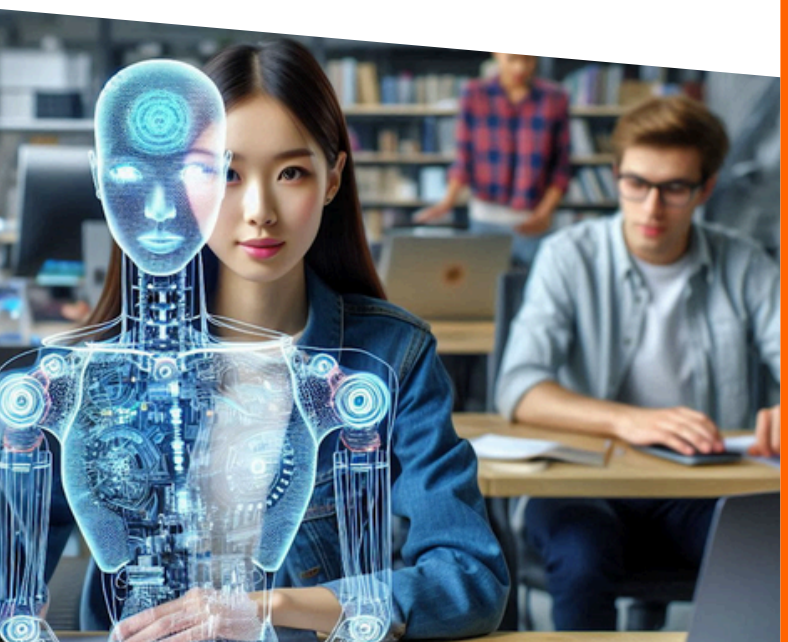
"

Kurumsal size özel eğitimler hazırlıyoruz. Her eğitim yeni bir heyecan.

Vebende A.Ş.

Kurumsal Terzi Usulü Butik Eğitimler.

Size özel hazırlanan seminer, danışmanlık, eğitim ve hizmetlerimizle yüksek verim elde edin. Paranızı boşa harcamayın. Zaman çok değerli.



Her Eğitim Yeni Bir Heyecan

2000 yılından günümüze devam eden eğitim heyecanı. Uluslararası tecrübe, proje geliştirme deneyimleri, danışmanlıklar ve arge mühendislik deneyimlerimizi ülkemize sunmak için yeni bir konsept tasarladık.
Sizi dinliyor, takımınıza uygun özel içerikler ile hazırlanmış eğitimler hazırlıyoruz. Her eğitim özel bir çalışma, içerik üretimi, uygulama örnekleri hazırlıkları, sunumlar hazırlamayı gerektiriyor. Aynı eğitimi yönetim kadrosuna farklı, teknik ve mimar ekiplerinize farklı içerikler ile hazırlıyoruz. Her eğitim yeni bir macera ve heyecan.

Bizimle İletişime Geçin

iletisim@vebende.com

www.vebende.com.tr

İzmir - Türkiye

Kurumsal
Eğitimler

www.vebende.com.tr

İletişime Geçin

Whatsapp 0542 5505704

iletisim@vebende.com

www.vebende.com.tr

Adalet Mah. Manas Bulvarı
No:39 İç Kapı N0: 3107 Bayraklı
İZMİR






Sürekli Güncellenen Eğitimlerimizi Sitemizden Takip Edin.

"

Kurumsal terzi usulu size özel eğitimler ve uluslararası deneyime sahip eğitmenler ile çalışmanın keyfi

"

Size Neler Sunuyoruz?

- Kitaptan okunan eğitimler sunmuyoruz. Sizin için özel hazırlanan içerikler ve uygulamalı eğitimler hazırlıyoruz.
- Her eğitim için sunumlar, materyaller, örnek senaryolar size özel hazırlıyoruz.
- Her eğitim için katılımcılara özel github repoları hazırlanıyor. Eğitimden sonra da katılımcılar hayat boyu kaynaklara ulaşmaya devam edebilsinler diye, **"katılımcılar ve eğitmenle birlikte yapılan tüm çalışmaları"** github repolarında saklıyoruz.

Misyonumuz

1. Ülkemizde dünyanın en güncel teknolojilerini kazandırmak. En güncel teknolojilerine hakim takımlarına katkı sağlamak.
2. Alışılmışın dışında en güncel teknolojileri deneyimli eğitmenler ve uygulamalar ile sunmak.
3. Siber güvenlik konusunda hassas çalışmalar sunarak, çağımızın büyük kabusu siber tehditler konusunda deneyimli bilgili takımların oluşmasına katkı sağlamak.