

TÜM KURUM ÇALIŞANLARINA SİBER GÜVENLİK

Şirket çalışanlarınızın siber güvenlik konusundaki farkındalığını artırmak için kapsamlı bir eğitim programı sunuyoruz. Bu eğitim, temel siber güvenlik kavramlarından ağ ve cihaz güvenliğine, veri koruma stratejilerinden kriz yönetimi ve siber saldırılara müdahale yöntemlerine kadar geniş bir yelpazede bilgi sunuyor. Çalışanlarınızın dijital dünyadaki tehditlere karşı bilinçli olmasını sağlamak, güvenlik protokollerine uyumlarını artırmak ve kurumsal verilerinizi korumak için özel olarak tasarlanmış bu eğitim, şirketinizin güvenliğini güçlendirmeye yönelik güçlü bir adım olacaktır.

TÜM KURUM ÇALIŞANLARINA SİBER GÜVENLİK

KURUMSAL ÖZEL EĞİTİM

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

TÜM KURUM ÇALIŞANLARINA SİBER GÜVENLİK

Siber güvenlik, artık sadece bilgi teknolojileri departmanlarının değil, tüm kurum çalışanlarının sorumluluğu altında olan kritik bir konudur. Gelişen dijital tehditler, kurumların en zayıf halkasını hedef alıyor yani insan faktörünü. Phishing saldırıları, sosyal mühendislik girişimleri, zararlı yazılımlar ve kimlik hırsızlığı gibi tehlikeler, farkındalığı düşük çalışanlar üzerinden kurumsal sistemlere sızmakta ve ciddi kayıplara yol açmaktadır.

Bu kapsamlı eğitim programı, kurum genelinde dijital güvenlik bilinci oluşturmayı, çalışanların tehditleri tanımasını ve doğru tepkiler geliştirmesini hedefler. Eğitim içeriği, karmaşık teknik detaylara boğulmadan, sade ve etkili bir şekilde aktarılmakta; katılımcıların günlük iş hayatında karşılaşılabilecekleri gerçek senaryolar üzerinden öğrenmeleri sağlanmaktadır. Katılımcılar, sahte e-posta ve bağlantıları ayırt etme, güvenli parola oluşturma, şüpheli dosyaları tanıma ve acil durumda ne yapılması gerektiği gibi konularda pratik bilgiler edinirler.

EĞİTİM HEDEFİ

Bu eğitim, kurum çalışanlarının temel siber güvenlik farkındalığını artırmayı, dijital güvenlik risklerini tanımayı ve bu risklere karşı doğru adımlar atmayı hedeflemektedir. Katılımcılar, siber tehditleri tanımlamayı, güvenli bilgi işlem pratiklerini uygulamayı ve olası güvenlik açıklarına karşı nasıl davranmaları gerektiğini öğreneceklerdir. Eğitim sonunda, siber güvenlik politikalarının neden önemli olduğunu anlayarak, güvenlik ihlalleri ve tehditlere karşı bilinçli bir şekilde hareket edebilecek seviyeye ulaşacaklardır.





SİBER GÜVENLİK TEMELLERİ

- Siber Güvenlik Nedir?
 - Tanım: Siber güvenlik, dijital sistemlerin, ağların, cihazların, verilerin ve uygulamaların korunması sürecidir.
 - Önemi: Artan dijitalleşme ile siber tehditler de çoğalmaktadır. Şirketlerin siber güvenlik önlemleri, iş sürekliliği ve itibarlarını korumak için hayati öneme sahiptir.
 - Temel Kavramlar:
 - Siber Saldırıları: Bilgisayar sistemlerine, ağlara veya cihazlara yapılan zararlı müdahaleler.
 - Güvenlik Açıkları: Sistemlerin savunmasız olduğu noktalar, bu açıklar siber saldırganlar tarafından kullanılır.
 - Veri İhlalleri: Yetkisiz kişilerin hassas bilgilere erişimi.
- Siber Tehdit Türleri
 - Virüsler: Sistemleri yavaşlatabilir veya dosyaları silebilir.
 - Trojanlar: Kullanıcıları kandırarak zararlı yazılımı sisteme sızdırır.
 - Fidye Yazılımları (Ransomware): Dosyaları şifreler ve para talep eder.
 - Oltalama (Phishing): Kişisel verileri çalmaya yönelik saldırılar.
 - DDoS Saldırıları: Web sitelerini veya servisleri aşırı trafikle felç etme.
- Sosyal Mühendislik Saldırıları
 - İnsan psikolojisini manipüle ederek güvenlik ihlali yapma yöntemleri.
 - Korunma Yöntemleri: Şüpheli iletişimlere dikkat etme, güvenli uygulama protokollerine sadık kalma.
- Güvenli Parola Yönetimi
 - Parola Oluşturma: Karmaşık ve uzun parolalar kullanma.
 - Parola Yöneticileri: Güvenli parola saklama ve yönetme yazılımları.
 - İki Faktörlü Kimlik Doğrulama (2FA): Ekstra bir güvenlik katmanı ekler.

- Ağ Güvenliğine Giriş
 - Kurum İçi Ağlar: Verilerin ve iletişimin güvenliği.
 - Ağ Saldırıları ve Önlemleri: Ağ tıkanıklığı ve veri ele geçirme risklerine karşı koruma.
 - Firewall ve Ağ Segmentasyonu: Ağları izole ederek güvenliği artırma.
- Wi-Fi Güvenliği
 - Güçlü şifreleme protokolleri kullanımı (WPA2, WPA3).
 - Açık Wi-Fi Ağları: Güvenli olmayan ağların riskleri.
- VPN Kullanımı
 - Sanal Özel Ağ (VPN): Kimlik ve verilerin şifrlenmesi.
- E-posta Güvenliği
 - Zararlı e-posta eklerine karşı dikkatli olunması.
 - E-posta şifreleme yöntemleri.

BİLGİ GÜVENLİĞİ VE VERİ KORUMA

- Bilgi Güvenliği Politikaları
 - Kurumsal Politikalara Uyumluluk: Güvenlik protokollerine sadık kalma.
 - Bilgi Sınıflandırma: Verilerin gizlilik seviyelerine göre sınıflandırılması.
- Veri Şifreleme
 - Şifreleme Türleri: Simetrik ve asimetrik şifreleme yöntemleri.
- Kişisel Verilerin Korunması (KVKK ve GDPR)
 - Verilerin toplanması, işlenmesi ve saklanmasıyla ilgili düzenlemeler.
- Veri Yedekleme ve Kurtarma
 - Yedekleme stratejileri ve kurtarma planları.

UYGULAMA VE CİHAZ GÜVENLİĞİ

- Mobil Cihaz Güvenliği
 - BYOD politikaları ve cihaz yönetimi.
- İşletim Sistemi Güvenliği
 - Windows, macOS ve Linux güvenliği.
- Güvenli Uygulama Kullanımı
 - Kurumsal yazılımların güvenli kullanımı.
- Zararlı Yazılımlardan Korunma
 - Antivirüs yazılımları ve zararlı yazılım tespit yöntemleri.

KRİZ YÖNETİMİ VE SİBER OLAYLARA MÜDAHALE

- Siber Güvenlik Olaylarına Müdahale
 - Olay yönetimi süreçleri ve kriz yönetimi adımları.
- Güvenlik İhlallerinin Bildirilmesi
 - Yetkililere bilgi verilmesi ve olay sonrası analiz.
- Siber Güvenlik Farkındalığının Artırılması
 - Kurumsal farkındalık eğitimleri ve sonuçların değerlendirilmesi.



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 içeriğe cevap verir. Katılımcılar bu araçlarla eğitimlerde sorulan sorulara ve taleplere uygun içeriğe 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.

TÜM KURUM ÇALIŞANLARINA SİBER GÜVENLİK

Eğitim, kurum çalışanlarının dijital güvenlik reflekslerini güçlendiren ve kurumsal riskleri azaltmaya yönelik bir önleyici güvenlik çözümüdür. Çevrim içi veya yüz yüze seçeneklerle sunulabilen program, tüm çalışanlar için uygundur ve sertifika ile tamamlanır. Kurumunuzda güçlü bir siber güvenlik kültürü inşa etmek istiyorsanız, bu eğitim önemli bir ilk adımdır.

KATILIMCILARDAN BEKLENTİLERİMİZ

Katılımcılardan, eğitime aktif ve dikkatli bir şekilde katılım göstermeleri beklenmektedir. Anlatılan konuların sadece teorik bilgi olarak değil, günlük iş hayatında uygulanabilir güvenlik alışkanlıkları olarak benimsenmesi hedeflenmektedir. Eğitim sürecinde sorular sormaları, kendi deneyimlerini paylaşımları ve sunulan örnek senaryolara katkı sunmaları önemlidir. Eğitimin sonunda edinilen bilgilerin sadece kişisel güvenlikte değil, kurumsal dijital güvenliğin gelişmesinde de etkili olması beklenir. Katılımcıların, şüpheli durumları doğru şekilde değerlendirmesi, olası tehditleri ilgili birimlere bildirme sorumluluğunu üstlenmesi ve kurum içindeki diğer çalışanlara da farkındalık kazandıracak şekilde örnek olması en değerli çıktılardan biridir. Ayrıca eğitim sonrası sağlanacak değerlendirme ve geri bildirim anketlerine katılarak sürecin gelişmesine katkı sunmaları beklenmektedir.

EĞİTİM YÖNTEMİ

Eğitim, katılımcıların konuya aktif şekilde dâhil olabileceği etkileşimli bir yapıda planlanmıştır. Teorik bilgilerin sade ve anlaşılır şekilde sunulmasının yanı sıra, gerçek hayattan örnekler ve vaka analizleriyle desteklenerek farkındalık düzeyinin artırılması hedeflenir.

Görsel materyaller, kısa videolar ve senaryo temelli anlatımlar sayesinde dikkat çekici ve akılda kalıcı bir öğrenme ortamı sunulur. Eğitimin sonunda yapılan kısa bilgi testleri ile öğrenilenlerin pekiştirilmesi sağlanır. Eğitim tercihe göre çevrim içi platformlar üzerinden ya da yüz yüze sınıf ortamında uygulanabilir şekilde esnek olarak sunulur.

HEDEF KİTLE

- **Bilgisayar başında çalışan yöneticiler:** Günlük iletişimlerini e-posta üzerinden sürdüren, dosya paylaşan ve kurumun dijital akışında aktif rol alan karar vericiler.
- **İdari personel:** Ofis içinde belge, sistem ve iletişim trafiğiyle uğraşırken, siber saldırıların en çok hedeflediği kullanıcı grubunda yer alan çalışanlar.
- **Saha ekipleri:** Mobil cihazlar üzerinden veri paylaşan, farklı ağlara bağlanan ve güvenlik açığı oluşturabilecek alışkanlıklara sahip olabilecek personeller.
- **Destek ve operasyon birimleri:** Sistemlerle doğrudan etkileşimde bulunmasalar bile, sosyal mühendislik saldırılarına maruz kalma riski taşıyan tüm çalışanlar.
- **Tüm çalışanlar:** E-posta açan, internete bağlanan, cihaz kullanan herkes bu zincirin bir halkasıdır. Eğitim, teknik düzeyi ne olursa olsun tüm personele yönelik olarak tasarlanmıştır.

"

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

