Kaspersky Security Awareness

İşletmenizin güvenliğini sağlayan bir siber güvenlik kültürü oluşturun

kaspersky geleceği yakalayın

İnsan hatası

en büyük tehditlerden biridir: Veri ihlallerinin ortalama %64-86'sı kötü niyetli olmayan insan eylemlerinden kaynaklanmaktadır[1]

4,4 milyon $:

kuruluş başına bir veri ihlalinin ortalama maliyeti[2]

Yönetmelikler güvenlik bilincini zorunlu kılıyor

Uyumluluk kapsamında: PCI DSS, ISO/IEC 27001, GDPR, NIS 2 ve diğer standartlar, hassas verilerin korunması için güvenlik bilinci programlarını zorunlu kılar veya şiddetle tavsiye eder

Güvenlik bilincine sahip bir kültür oluşturmak karşılığını verir

Kaspersky'nin araştırmasına göre, farkındalık eğitimini tamamlayan çalışanların %85'inden fazlası, uyanıklık ve dikkat düzeylerinde artış olduğunu belirtiyor; bu davranış değişikliği, olayların önlenmesine yardımcı oluyor.

%92

oranında kullanıcı Kaspersky Security Awareness'ı başkalarına tavsiye ediyor

3 milyon

çalışan eğitim programlarımızı başarılı bir şekilde tamamladı

160'dan fazla

ülkede kuruluşlar, çalışanlarını eğitim çözümlerimizle koruyor

İnsan kaynaklı siber riskleri azaltmaya yönelik etkili bir yaklaşım

Güçlü bir siber güvenlik bilinci ve pratik becerilerle desteklenen, kurum genelinde siber güvenlik bilinci kültürünü oluşturun. Bu, insan hatasından kaynaklanan olayların sayısını azaltmaya yardımcı olur. İnsan faktörünü ele almanın en iyi yolu, ilgili ve güncel içeriği en yeni öğrenme yöntemleri ve teknolojileriyle birleştiren yapılandırılmış bir eğitim programıdır.

Kaspersky Güvenlik Farkındalığı çözümleri

Kaspersky Security Awareness, dünyanın dört bir yanındaki her büyüklükteki işletmenin çalışanlarının siber okuryazarlığını artırmasına ve güvenliğin herkesin sorumluluğu olduğu bir kültürün oluşmasını sağlamasına olanak tanır. Davranışlarda sürdürülebilir değişikliklerin zaman alması nedeniyle, yaklaşımımız çeşitli araçlar ve destek materyalleriyle sürekli bir öğrenme döngüsü oluşturmayı içermektedir: Kaspersky Interactive Protection Simulation, Executive Training, Automated Security Awareness Platform ve Cybersecurity for IT Online.

Müşteriler neden Kaspersky Security Awareness'ı tercih ediyor?

Gerçek hayattaki tehditleri fark etme ve bunlara müdahale etme becerisi ve öz güven

Kaspersky'nin yaklaşık 30 yıllık siber güvenlik uzmanlığı ve gerçek zamanlı tehdit istihbaratından yararlanarak, son derece güncel siber güvenlik eğitim içerikleri hazırlıyoruz. Yeni tehditler ortaya çıktıkça içeriklerimizi güncelliyoruz ve çalışanlarınızın her zaman hazırlıklı olmasını sağlıyoruz.

Erişilebilir, etkileşimli öğrenme

Eğitim programımız, çalışanların dersleri günlük görevleriyle ilişkilendirmelerine yardımcı olan net ve mantıklı bir yapıya sahip etkileşimli öğrenme yöntemini kullanır; bu sayede konunun kavranması, bilginin kalıcı hale gelmesi ve pratikte uygulanabilirliği artırılır.

Kalıcı davranış değişikliği

Yöntemimiz, yeni becerileri pekiştirir, sürekli motivasyon sağlar ve öğrenmeyi kurumsal rutinlerin bir parçası haline getirmeye yardımcı olur. Sonuçta, güvenli uygulamaların artık ikinci bir doğa haline geldiği, kalıcı bir davranış değişikliği ortaya çıkıyor.

Her alanda katılım

Üst düzey, eyleme geçirilebilir içgörülere ihtiyaç duyan yöneticilerden, pratik rehberliğe ihtiyaç duyan saha çalışanlarına kadar, her hedef kitleye uygun içeriği doğru formatta sunuyoruz.

1 Kaspersky İnsan Faktörü 360 Raporu, Cybersecurity Ventures, Verizon Veri İhlali Raporları
2 2025 Veri İhlali Maliyet Raporu, IBM

Kaspersky Automated Security Awareness Platform İnsanlardan oluşan bir güvenlik duvarı oluşturmak

Kaspersky Automated Security Awareness Platform (ASAP), çalışanlara gerçek hayattaki saldırı vektörlerini fark edip engelleyebilmeleri için gerekli beceri ve bilgileri kazandıran, sürekli eğitim sunan bir çevrimiçi araçtır.

Dünya çapında uzmanlar tarafından geliştirilen Kaspersky ASAP, çalışanlarınızı destekler ve işinizi güçlendirir:

İnsan kaynaklı olayların sayısını ve bunun sonucunda ortaya çıkan maddi kayıpları ve itibar kaybını azaltır

Yasal gereklilikleri destekleyerek, mevzuata uyumsuzluktan kaynaklanan para cezası riskini en aza indirir

Farkındalık eğitimlerini yönetmek için gereken zaman ve çabayı azaltır ve BT ekiplerinin yükünü hafifletir

Kaspersky ASAP, sadece bir kimlik avı koruması aracından çok daha fazlasıdır. Bu eğitim, MITRE ATT&CK teknikleriyle uyumlu olup, çalışanların hangi insan kaynaklı saldırı vektörlerini önlemeye yardımcı olabileceğini göstermektedir. Örnek olarak şunları sayabiliriz:

MITRE tekniği	Tehdit	Beceri ve davranışsal sonuçlar
T1566 – Kimlik Avı	Kötü amaçlı e-postalar	Kimlik avı girişimlerini fark edin ve bildirin
T1585 – Hesaplar Oluşturma	Sahte hesaplar/profiller	Bilgileri paylaşmadan önce doğruluğunu kontrol edin
T1199 – Güvene Dayalı İlişki	İş ortağı güvenini suistimal etme	Olağandışı talepleri sorgulamayı öğrenin
T1091 – Çıkarılabilir Ortamlar Aracılığıyla Kopyalama	Çıkarılabilir ortam	USB belleklerdeki kötü amaçlı yazılımların tehlikesini anlayın
T1078 – Geçerli Hesaplar	Kimlik bilgilerinin çalınması	Sosyal mühendislik yoluyla erişim izni vermekten kaçının

%95

oranında eğitimli çalışan, artık kimlik avı saldırılarını tespit edebiliyor

20x

Çalışanlar düzenli olarak eğitildiğinde veri ihlalleri azalır[1]

ASAP kapsamında ele alınan başlıca konular arasında şunlar yer almaktadır (bunlarla sınırlı değildir):

- E-posta
- Parolalar ve hesaplar
- Web siteleri ve internet
- PC güvenliği
- Gizli veriler
- Kişisel veriler
- Fiziksel veri güvenliği
- GDPR
- Yapay zeka ve sinir ağları
- Üst düzey yöneticilere yönelik saldırılar
- Mobil cihazlar
- Tedarik zinciri saldırıları
- Sosyal medya ve mesajlaşma uygulamaları
- Endüstriyel siber güvenlik
- Banka kartı güvenliği ve PCI DSS
- Olaylara nasıl müdahale edilir
- Telefonla kimlik avı

Çalışanlarınızı, teknik araçların yanı sıra ek bir koruma katmanı oluşturmaları için güçlendirin.

Deneme sürümünü başlat

1 2025 Kaspersky Automated Security Awareness Platform Araştırması

Bilgiyi kalıcı kılmak ve becerileri uygulamaya geçirmek için etkili içerik ve yöntemler

Uzman odaklı

Neredeyse 30 yıllık siber güvenlik uzmanlığına dayanan ve çok sayıda konuyu kapsayan pratik ve temel siber güvenlik becerilerini içeren bir yetkinlik modeli.

Çeşitli içerikler

Etkileşimli modüller ve alıştırmalar, gerçek hayattan örnekler, testler, videolar ve çok senaryolu kimlik avı simülasyonları aracılığıyla bilginin kalıcı hale gelmesini destekler.

Geniş bir yelpazede özelleştirme seçenekleri

Logonuzu ve marka sertifikalarınızı ekleyin, dersleri kurum içi slaytlar, belgeler veya ilkelerle zenginleştirin, özel SCORM/PDF modülleri ekleyin ve test yapılarını düzenleyin.

İnsan odaklı

İnsanların bilgiyi nasıl algıladığı, hafızasında tuttuğu ve uyguladığına göre tasarlanmıştır

Nasıl çalışır?

Kuruluşunuzdaki herkesin siber güvenlik bilincine sahip olması gerekir, ancak bu bilginin kapsamı, kişinin görevine ve risk profiline göre değişiklik gösterir. İşte bu noktada, herkese uyan tek tip eğitim başarısız olur. Platformumuz, ekibinizin 500'den fazla pratik beceriyi geliştirmesine, çalışanları zahmetsizce gruplandırmasına ve aşağıdaki bileşenleri kullanarak sadece birkaç tıklamayla her katılımcıya uygun eğitimi atamasına yardımcı olur.

Ana yemek

Karmaşıklık düzeyine göre düzenlenmiş mikro dersler sayesinde konuyu derinlemesine öğrenin.

Ekspres kurs

Kısa ve son derece ilgi çekici sesli-görüntülü eğitimlerle siber güvenlik eğitimi uyumluluk gerekliliklerini hızla karşılayın veya bilgilerinizi tazeleyin.

Kimlik avı simülatörü

Eğitim öncesinde, sırasında ve sonrasında simüle edilmiş kimlik avı saldırıları düzenleyerek, çalışanların siber saldırılara karşı direnme becerilerini test edin.

Ders planı

Ezberlemeyi en üst düzeye çıkarmak için farklı türde etkinlikler içeren modüller

Her büyüklükteki kuruluş için yönetimi kolay bir çözüm

Kolay başlangıç

Çevrimiçi kayıt olun ve iki ay boyunca en fazla beş kullanıcı için demo erişimi kazanın. "Başlangıç kılavuzu" ve çevrimiçi destek içerir

Tam otomasyon

Eğitim modülleri, testler ve kimlik avı simülasyonları, eğitim grubu ayarlarına göre otomatik olarak atanır

Proaktif insan kaynaklı risk yönetimi

Kaspersky SIEM ve XDR ile sorunsuz entegrasyon ve üçüncü taraf uygulamalarla entegrasyon için API'ler, çalışan davranışlarına ilişkin eksiksiz bir görünüm sunar ve konsoldan doğrudan gerçek güvenlik olaylarına dayalı eğitimler atar

Çoklu kullanıcı desteği ve esnek yönetici rolleri

Şubeleri ve farklı coğrafi bölgelerde bulunan ekipleri olan kuruluşlar için idealdir; yönetimi yerel yöneticilere devrederken merkezi denetim imkanı sunar.

Önceden tanımlanmış özel kurallara dayalı otomatik kullanıcı gruplandırması

Rol, departman veya risk profiline göre düzenleyin

Net raporlama

Kontrol panelleri, her çalışanın ilerlemesi, gecikmeleri veya düşük performansına ilişkin ayrıntılı görünümler sunarak önemli verileri sağlar ve tek bir tıklamayla yönetim için gönderilmeye hazır bir PDF raporu sunar

Esnek dağıtım

SaaS platformu olarak veya şirket içi kurulum olarak sunulmaktadır

Sorunsuz kayıt

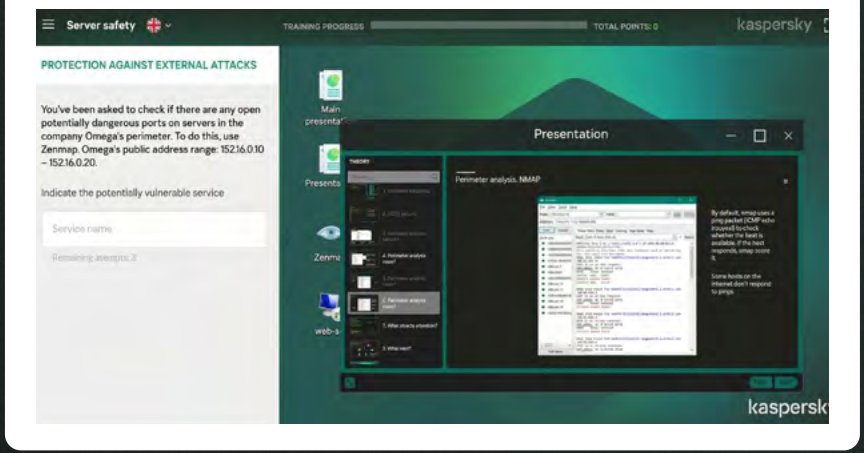
Active Directory ve SSO ile entegre olur

BT Çevrimiçi Siber Güvenliği

Cybersecurity for IT Online (CITO), hizmet masası uzmanlarına, sistem yöneticilerine ve uzman olmayan BT güvenlik ekibi üyelerine, günlük bilgisayar sorunları içinde gizli siber saldırıları tespit etme, ilgili verileri toplama ve siber güvenlik savunmasının ilk hattı olarak hareket etme konusunda pratik beceriler kazandıran etkileşimli bir eğitim programıdır.

Birinci aşama olay müdahalesi için pratik beceriler:

- Kötü amaçlı yazılımları, potansiyel olarak istenmeyen programları, güvenlik açıklarını ve kimlik avı saldırılarını tespit etmeyi, analiz etmeyi ve bunlara müdahale etmeyi öğrenin
- BT altyapısı güvenliğini güçlendirmek ve olayları etkin bir şekilde araştırmak için gerçek hayatta kullanılan araç ve teknikleri uygulayın
- Günlük analizi, dijital delil toplama ve tehdit araştırması becerilerini geliştirin
- Güçlendirme, ilke yapılandırması ve izleme yoluyla sunucuları ve Active Directory'yi güvenli hale getirmeyi öğrenin



Katılımcılar, özlü teorik bilgiler, pratik ipuçları ve her modülde gerçek hayattaki BT güvenlik araçları ile günlük görevlere odaklanan 4 ila 13 alıştırmayı bir araya getiren altı modül boyunca ilerler.

Kötü amaçlı yazılım	Potansiyel olarak istenmeyen programlar ve güvenlik açıkları	Sunucu güvenliği
Araştırma temelleri	Kimlik avı ve açık kaynak istihbaratı	Active Directory güvenliği

Kaspersky Yönetici Eğitimi

Yönetici kararlarının risk durumunu, mevzuata uygunluğu ve uzun vadeli kurumsal dayanıklılığı nasıl doğrudan etkilediğini göstererek, yukarıdan aşağıya doğru bir güvenlik kültürü oluşturun.

Kaspersky Yönetici Eğitimi, iş dünyasının liderleri ve üst düzey yöneticiler için düzenlenen canlı bir atölye çalışmasıdır. Bu etkinlikte, güncel tehdit ortamının işletmeniz için ne anlama geldiği, bir siber saldırı durumunda hangi önlemlerin alınması gerektiği ve daha pek çok konu ele alınmaktadır. Katılımcılar, temel siber güvenlik ilkelerinin ötesinde, güvenlik yatırımlarının finansal sürdürülebilirliği konusunda önemli bilgiler edinerek, üst düzey yöneticilerin güvenlik önlemlerini iş performansıyla ilişkilendirmelerine olanak tanır. KIPS ile bu eğitimi birleştirmek en uygunudur.

Siber güvenliğin iş dünyası açısından kritik öneme sahip unsurları, açık, anlaşılır ve teknik terimler içermeyen bir dille açıklanıyor:

- Siber güvenliği genel sistemin bir parçası olarak kavrayın
- Siber risklerin iş faaliyetlerini nasıl etkilediğini ve bunların nasıl yönetilebileceğini öğrenin
- Siber güvenlik yönetişiminde üst yönetimin rolünü anlamak

Kaspersky Interactive Protection Simulation (KIPS): Bir işletmenin gözünden siber güvenlik

KIPS, her türlü BT sistemi ve iş sürecinin kullanımıyla ilgili riskler ve zorluklar konusunda farkındalığı artırır. Bu, üst düzey yöneticiler, iş sistemleri uzmanları ve BT profesyonellerine yönelik iki saatlik, etkileşimli bir takım oyunudur. Sektöre özgü senaryolar, katılımcılara tedarik zinciri saldırıları, üçüncü taraf erişimlerinin kötüye kullanılması, sosyal mühendislik veya kötü amaçlı yazılımlar dahil olmak üzere Kaspersky uzmanları tarafından aktif saldırı kampanyalarında gözlemlenen modern saldırı tekniklerini gösterir. Zaman ve bütçe kısıtlamaları altında çalışan ekipler, iş performansını ve gelirini korumak için stratejiler geliştirmeli, güvenlik olaylarının etkisini öngörmeli ve bu olaylara etkin bir şekilde müdahale etmelidir.

- Karar vericiler arasında bir anlayış oluşturur
- Siber güvenlik risklerini görselleştirmeye ve bunları doğrudan gelir ve operasyonlarla ilişkilendirmeye yardımcı olur
- Ekipleri siber güvenlik konularına dahil eder ve güvenlik öncelikli bir kültürün oluşmasını sağlar

14 sektöre özel senaryo; bunlara sürekli yenileri ekleniyor

- Havalimanı
- Büyük kurum
- Banka
- Petrol ve Gaz
- Taşıma
- Enerji santrali
- Su arıtma tesisi
- Yerel kamu idareleri
- Petrokimya sanayii
- Petrol şirketi
- Küçük ve orta ölçekli işletmeler
- Telekom
- Teknik niteleme
- BT

KIPS Live

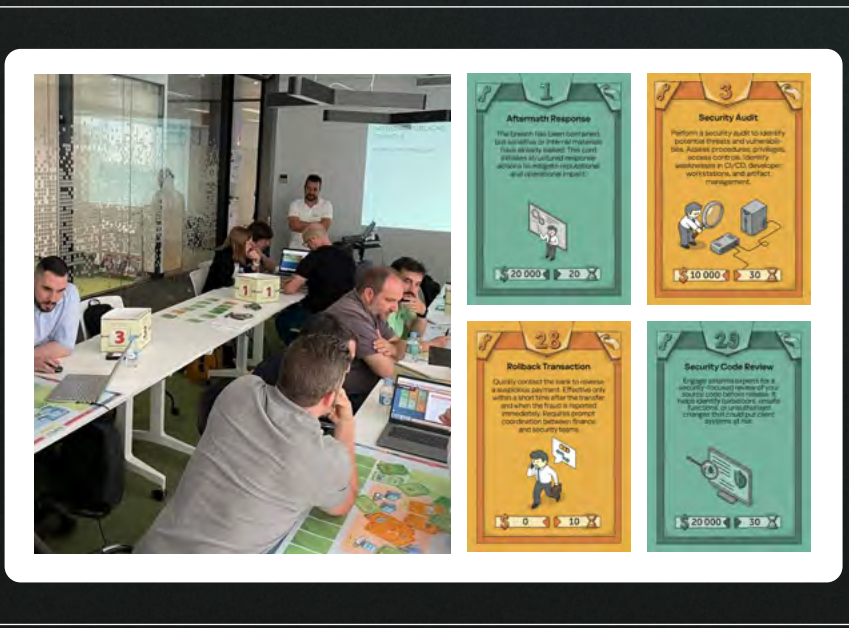
Tek başına bir etkinlik olarak ya da mevcut bir konferans, seminer veya kurumsal etkinliğin bir parçası olarak gerçekleştirilebilen eğlenceli bir etkinlik.

- En fazla 100 katılımcı, her takımda 4–5 kişi
- Yerinde kolaylaştırıcı ve eğitim asistanı

KIPS Online

Çevrimiçi sürüm, küresel kuruluşlar veya halka açık etkinlikler için idealdir. Ayrıca KIPS Live ile entegre edilerek, uzaktaki ekipler de yerinde düzenlenen bir etkinliğe dahil edilebilir.

- Herhangi bir yerden en fazla 300 takım (1000 katılımcı)



KIPS özelleştirme seçenekleri

- Ortak markalı veya müşteri markalı panolar, kartlar ve masa numaraları
- Kaspersky ile ortaklaşa geliştirilen, ağınızı, geçmişteki olayları veya sektörünüze özgü tehditleri simüle edebilen benzersiz bir senaryo

Siber güvenlik kültürü oluşturmak

Gerçek siber dayanıklılık sadece ilke ve teknolojilerle ilgili değildir; bu bir kültür meselesidir. Kültür ise insanların davranışları, liderlerin liderlik tarzları, süreçlerin nasıl tasarlandığı ve teknolojinin tüm bunları nasıl mümkün kıldığına göre şekillenir:

- İnsanlar ve davranışlar
- Liderlik ve işbirliği
- Operasyonel entegrasyon
- Güvenlik hazırlığı ve altyapısı

Sürekli bir bağlılık sayesinde sürdürülebilir bir siber güvenlik kültürü oluşturulur. Bu nedenle, Kaspersky Security Awareness çözümlerini kullanabileceğiniz beş temel adımdan oluşan sistematik bir yaklaşım geliştirdik.

Kuruluşunuzda siber güvenlik kültürü olgunluk seviyesi şu anda ne durumda?

0 Parçalı
Risk: Temel uygulamaların ve yapıların bulunmaması, yüksek düzeyde bir savunmasızlık yaratır. En ufak bir olay bile ciddi sonuçlara yol açabilir.

1 Farkında ve duyarlı
Risk: Yalnızca açıkça belirtilen kurallara uyulur. Standart dışı durumlarda, çalışanlar kendi muhakemelerine göre hareket ederler.

2 Yönetilen
Risk: Olay sayısı azalıyor, ancak sistem daha karmaşık senaryolara karşı hâlâ savunmasız durumda.

3 Entegre
Risk: Süreçler sorunsuz görünüyor, ancak siber kültür kendi kendini düzenleyen bir sistem olarak işlev görmezse, bir "gecikme riski" devam eder.

4 Esnek
Sonuç: Olayların sayısı ve önemi azalmaya devam ediyor. Kuruluş, sürekli değişen tehdit ortamına hızla uyum sağlayabilir.

"

Güvenlik, bir saldırı kampanyası olmaktan çıkıp bir kültür haline geldiğinde risk azalır ve sonuçlar da kendiliğinden gelir.

CISO

Müşteri Etkileşim Hizmetleri

Kaspersky ASAP ile insanları, süreçleri ve teknolojileri uyumlu hale getirerek siber dayanıklılık kültürünü oluşturmaya başlayın.

Şimdi deneyin

Kaspersky Security Awareness

Dikkatli olun.
Güvende kalın.

www.kaspersky.com.tr

#kaspersky
#cybersecuritytruetobusiness