kaspersky cybersecurity true to business

Kaspersky Security Awareness

İşletmenizin güvenliğini sağlayan bir siber güvenlik kültürü oluşturun



Güvenliğe önem veren bir kültür neden önemlidir?

İnsan hatası

Veri ihlallerinin %62–80'i; hatalar, ayrıcalıkların kötüye kullanılması ve sosyal mühendislik dâhil olmak üzere insan kaynaklı eylemlerden kaynaklanmaktadır.[1] [2]

4.99 milyon dolar

kuruluş başına bir veri ihlalinin ortalama maliyeti[3]

Kapsamlarına güvenlik farkındalığını dâhil eden regülasyonlar: PCI DSS, ISO/IEC 27001, GDPR, NIS 2 ve diğer standartlar, hassas verilerin korunması için güvenlik bilinci programlarını zorunlu kılar veya şiddetle tavsiye eder

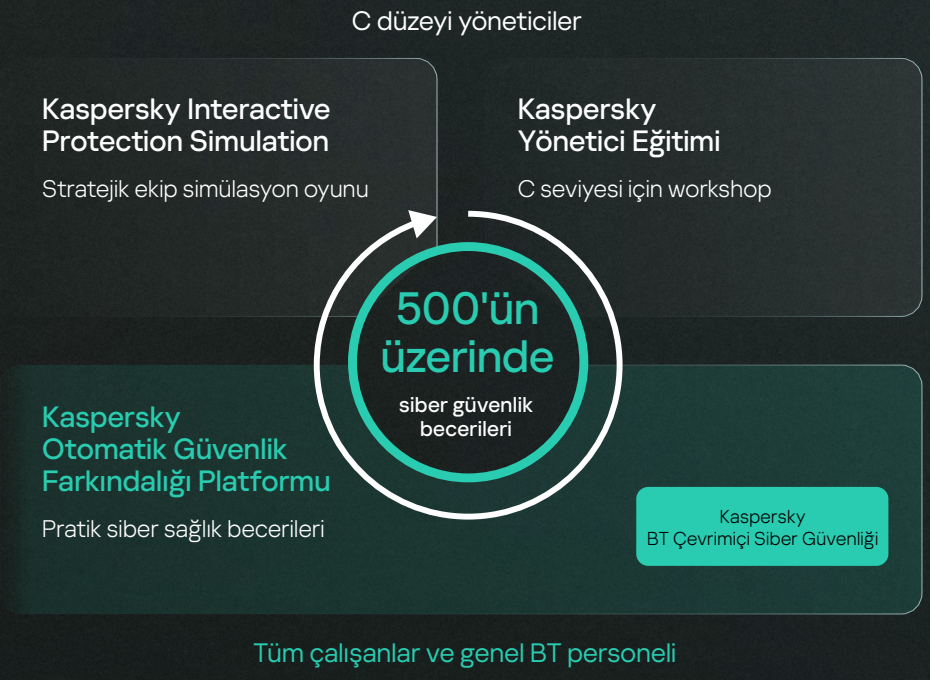
%85 Üstü

Farkındalık eğitimini tamamladıktan sonra farkındalık ve dikkat düzeylerinde artış olduğunu belirten çalışanların oranı; bu davranış değişikliği, olayların önlenmesine yardımcı oluyor[4]

Kaspersky Security Awareness ile insan kaynaklı siber riskleri azaltın

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 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.



%90

oranında kullanıcı Kaspersky Security Awareness'ı başkalarına[4] tavsiye ediyor

3 milyon

çalışan eğitim programlarımızı başarılı bir şekilde tamamladı

160'den fazla

ülkede kuruluşlar, çalışanlarını eğitim çözümlerimizle koruyor

Neden Kaspersky Security Awareness tercih edilmeli?

Neredeyse 30 yıldır siber güvenlik alanında uzmanlık

Kaspersky'nin küresel uzmanlığından yararlanarak, son derece güncel ve ihtiyaca uygun siber güvenlik eğitim içerikleri oluşturuyoruz. Yeni tehditler ortaya çıktıkça içeriklerimizi güncelliyoruz ve çalışanlarınızın her zaman hazırlıklı olmasını sağlıyoruz.

Kalıcı davranış değişikliği

Yöntemimiz, yeni becerileri pekiştirir, sürekli motivasyon sağlar ve öğrenmeyi kurumsal rutinlerin bir parçası haline getirmeye yardımcı olur.

Erişilebilir, etkileşimli öğrenme

Eğitim programımız, çalışanların dersleri günlük görevleriyle ilişkilendirmelerine yardımcı olan etkileşimli öğrenme yöntemini kullanır; bu sayede, bilginin kalıcı hale gelmesi ve pratikte uygulanabilirliği artırılır.

Her alanda katılım

Yöneticilerden saha çalışanlarına kadar her hedef kitleye, doğru içeriği doğru formatta sunuyoruz.

1 2026 Veri İhlali Soruşturmaları Raporu, Verizon
2 2026 Siber risk Anketi, Kaspersky
3 2026 Veri İhlali Maliyet Raporu, IBM
4 2024 Güvenlik Farkındalığı ve Eğitim Veri Kadranı, Info-Tech Research Group

Kaspersky Automated Security Awareness Platformu

Kaspersky Automated Security Awareness Platform (ASAP), çalışanlara gerçek hayattaki saldırıları 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 bunların yol açtığı finansal ve itibar kaybını azaltır



Uyumsuzluk nedeniyle uygulanabilecek para cezaları riskini

düzenleyici gerekliliklerin karşılanmasını destekleyerek en aza indirir



Farkındalık eğitimlerini yönetmek için gereken zaman ve çabayı

azaltarak 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 ATT&CK

MITRE tekniği	Tehdit	Beceri ve davranışsalkazanımlar
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
- Sosyal medya ve mesajlaşma uygulamaları
- Tedarik zinciri saldırıları
- Endüstriyel siber güvenlik
- Banka kartı güvenliği ve PCI DSS
- Olaylara nasıl müdahale edilir
- Telefonla kimlik avı

1 2025 Kaspersky Automated Security Awareness Platform Araştırması

Küresel uzmanlık ve esneklikle çalışanların güvenlik farkındalığını eğitin, test edin ve güçlendirin.

Kaspersky ASAP, her büyüklükte ve her seviyedeki güvenlik kültürüne sahip kuruluşların ihtiyaçlarına uygun üç farklı planla sunulmaktadır.

		Essential	Proactive	Advanced
		Küçük ekipler için ideal	Büyüyen işletmeler için ideal	Özel gereksinimleri ve olgun bir güvenlik kültürü bulunan kurumsal şirketler için idealdir
		Uyumluluk gerekliliklerini karşılamaya hazır güvenlik farkındalığı eğitimi	Proaktif güvenlik farkındalığı eğitimi ve ölçümleme	Özelleştirilmiş, yüksek etkili güvenlik farkındalığı eğitimi
Kimlik avı	Özelleştirilebilir, gerçekçi kimlik avı simülasyonlarıyla çalışanların siber saldırılara karşı hazırlık düzeyini test eder	●	●	●
Hızlı kurs	İnsan kaynaklı tehditlerle başa çıkmak için pratik beceriler kazandıran ve kuruluşunuzun mevzuata uygunluğunu sağlayan etkileşimli dersler	●	●	●
Temel kurs	Risk düzeylerine göre uyarlanmış, mikro öğrenme ve beceri pekiştirme yöntemlerini içeren, tam otomatik Güvenlik Farkındalığı eğitimi		●	●
İçerik özelleştirme	Özelleştirilebilir modüller, testler, kimlik avı sayfaları ve alan adları ve daha fazlası			●
Şirket içi dağıtım	Hassas veriler, entegrasyonlar ve mevzuata uyumluluk üzerinde tam kontrol sağlamak için kendi altyapınızda dağıtım seçeneği			●

Her büyüklükteki kuruluş için yönetimi kolay bir çözüm

Kolay başlangıç

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

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

Önceden tanımlanmış özel kurallara dayalı otomatik kullanıcı gruplandırması

Rol, departman veya risk profiline göre düzenleme

Esnek dağıtım

SaaS platformu olarak veya şirket içi kurulum olarak sunulmaktadır

Tam otomasyon

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

Çoklu kullanıcı desteği ve esnek yönetici rolleri

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

Anlaşılır ve yönetici dostu raporlar

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

Sorunsuz kayıt

Active Directory ve SSO ile entegre olur

Kaspersky Interactive Protection Simulation

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 ve kötü amaçlı yazılımlar dâhil 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 merciileri arasında
bir anlayış sağlar

Anlamaya yardımcı olur
Siber güvenlik risklerini görselleştirmeye ve bunları doğrudan gelir ve operasyonlarla ilişkilendirmeye yardımcı olur

Ekipleri siber güvenliğin parçası kılar
Ekipleri siber güvenlik konularına dâhil eder ve güvenlik öncelikli bir kültürün oluşmasını sağlar

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 dâhil 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

Sektöre özel 14 senaryo ve sürekli eklenen yeni içerikler

- BT
- Havalimanı
- Büyük şirket
- 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

Kaspersky
BT Çevrimiçi Siber Güvenliği

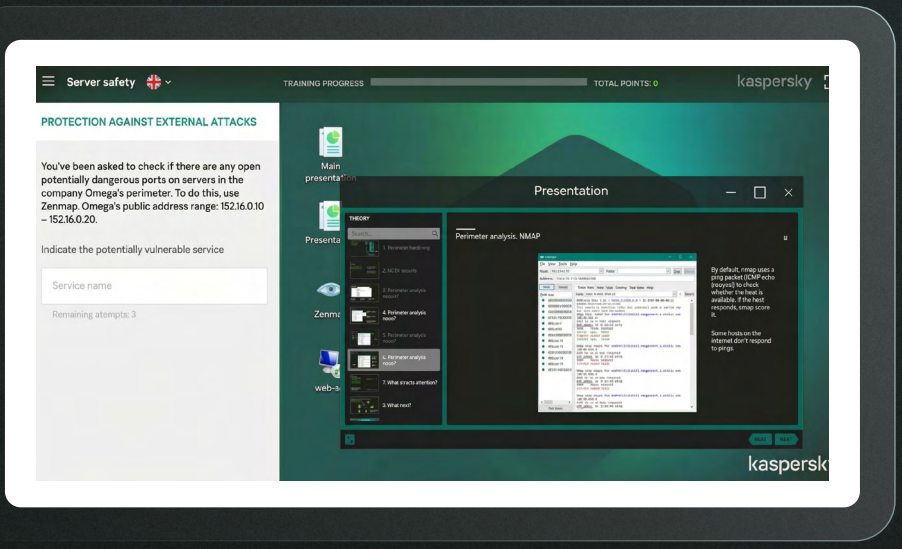
Cybersecurity for IT Online (CITO), hizmet masası uzmanları, sistem yöneticileri ve uzmanlık alanı siber güvenlik olmayan BT güvenlik ekibi üyeleri için tasarlanmış interaktif bir eğitim programıdır. Günlük bilgisayar olaylarının ardındaki gizli siber saldırıları tespit etme, ilgili verileri toplama ve siber savunmanın ilk hattı olarak hareket etme konusunda pratik beceriler kazandırır.

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

Pratik olay müdahalesi ve sistemleri güçlendirme becerileri:

- 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



Kaspersky Executive Training

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. 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:

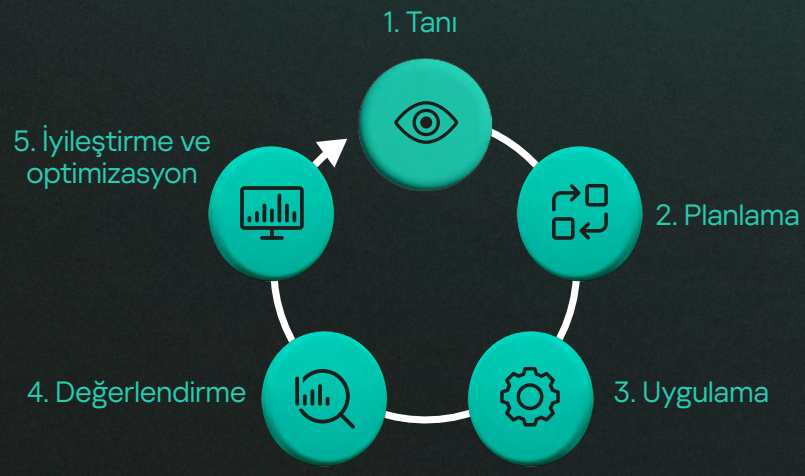
- Siber güvenliği genel sistemin bir parçası olarak kavrayın
- Siber risklerin iş faaliyetlerini nasıl etkilediğini ve bunların nasıl yönetilebileceğini öğrenin
- Siber güvenlik yönetişiminde üst yönetimin rolünü anlamak

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 zayıflık 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 eder. 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

Ücretsiz deneme sürümünüzü başlatıp güvenlik kültürü seviyenizi hemen öğrenin



Kaspersky Security Awareness

Dikkatli olun.
Güvende kalın.

www.kaspersky.com.tr

© 2026 AO Kaspersky Lab.
Tescilli ticari markalar ve hizmet markaları,
ilgili sahiplerine aittir.

#kaspersky
#truetobusiness