Her seviyeden çalışan için siber güvenlik becerileri

Kaspersky Güvenlik Farkındalığı

kaspersky GELECEĞİ YAKALAYIN

Daha fazla bilgi edinmek için
kaspersky.com.tr/awareness
adresini ziyaret edin

Kaspersky Güvenlik Farkındalığı

Kurumunuzda siber güvenlik kültürü inşa edin

Tüm siber olayların %80'inden fazlası insan hatasından kaynaklanır. Kuruluşunuz genelinde temel siber güvenlik becerilerini ve farkındalığını geliştirerek siber açıdan güvenli bir davranış kültürü inşa edebilir, böylece saldırılara açık yüzey ve müdahale etmeniz gereken olay sayısını azaltabilirsiniz. Siber güvenlikte 'insan faktörü' sorununu çözecek davranış değişikliklerini gerçekleştirmenin en iyi yolu, yetişkin eğitiminde en son teknik ve teknolojileri kullanarak konuyla en yakından ilgili ve güncel içeriği sunan bir eğitimdir.

İnsan faktörü – siber güvenliğin en savunmasız unsuru

Siber güvenlik çözümleri hızla gelişerek ve karmaşık tehditlere uyum sağlayarak siber güvenliğin en savunmasız unsuru olan insan faktörünü hedef alan siber suçluların hayatını daha da zorlaştırıyor.

Kurumların %55'i BT güvenlik politikalarının kendi çalışanları tarafından ihlal edildiğini bildirmektedir*

Küçük işletmelerin %43'ü çalışanların BT güvenlik politikası ihlallerinin güvenlik olaylarına neden olduğunu bildirmektedir**

Veri sızıntıları en yaygın güvenlik sorunudur ve çoğunlukla **çalışanlardan** (%22) ve saldırganlardan (%23) kaynaklanır.*

%30 oranında çalışan iş bilgisayarlarının oturum açma ve parola bilgilerini çalışma arkadaşlarıyla paylaştıklarını kabul ediyor***

%23 oranında kuruluş kurumsal veri depolaması için herhangi bir siber güvenlik kuralına veya ilkesine sahip değil***

Kaspersky Güvenlik Farkındalığı – BT güvenliği becerilerinde uzmanlaşmak için yeni bir yaklaşım

Kaspersky Güvenlik Farkındalığı, uzun yıllara dayalı uluslararası bir başarı geçmişine sahip, kanıtlanmış ve etkili bir çözümdür. Her büyüklükten işletme tarafından 75'ten fazla ülkede bir milyondan fazla çalışanı eğitmek için kullanılan çözüm, Kaspersky'nin siber güvenlik alanındaki 25 yılı aşkın deneyimini, yetişkin eğitimindeki kapsamlı deneyimiyle birleştiriyor.

İlgi uyandırıcı ve etkili eğitim çözümleri, personelinizin siber güvenlik farkındalığını arttırarak kuruluşunuzun genel siber güvenliğinin sağlanmasında kendilerine düşen payı gerçekleştirebilmelerini sağlar. Davranışlarda sürdürülebilir değişiklikler oluşturmak zaman aldığından yaklaşımımız, birden fazla bileşene sahip sürekli bir öğrenme döngüsü oluşturmayı içerir.

Sürekli öğrenme döngüsü

1 – Katılım/motivasyon
- Neden buna ihtiyacım var?
- Kavrama

2 – Başlangıç noktası
- Bilgi sahibi miyim?
- Hangilerini biliyorum ve boşluklar nerede?

3 – Öğrenme
- Mikro öğrenme
- Sürekli öğrenme
- Uyum sağlama

4 – Birleştirme
- Doğru anlamış mıyım?
- Bunu hatırlıyor muyum?
- Buna göre hareket ediyor muyum?

Temel program farklılıkları

İleri seviyede siber güvenlik uzmanlığı

25 yılı aşkın siber güvenlik deneyimimiz, ürünlerimizin temelini oluşturan siber güvenlik becerilerine dönüşüyor

Kuruluşunuzun tüm seviyelerindeki çalışanların davranışlarını değiştiren eğitimler

Oyunlaştırılmış eğitimimiz, eğlenceli eğitim yoluyla katılım ve motivasyon sağlarken öğrenme platformları, öğrenilen becerilerin süreç sırasında unutulmaması için siber güvenlik becerilerinin benimsenmesine yardımcı olur.

* "IT Security Economics 2022", Kaspersky

** "IT Security Economics 2021" Raporu, Kaspersky.

*** "Sorting out a Digital Clutter". Kaspersky Lab, 2019.

Etkili güvenlik farkındalığı için motivasyonu artırma

Çalışanlar hata yapar. Kuruluşlar para kaybeder...

52.887$
kurumsal işletme başına
Çalışanların uygun olmayan BT kaynaklarını kullanmasından kaynaklanan veri ihlallerinin ortalama finansal etkisi*

%30
oranında kötü amaçlı yazılım ihlali
sahte bağlantılar ve ekler içeren e-postalar yüzünden gerçekleşir**

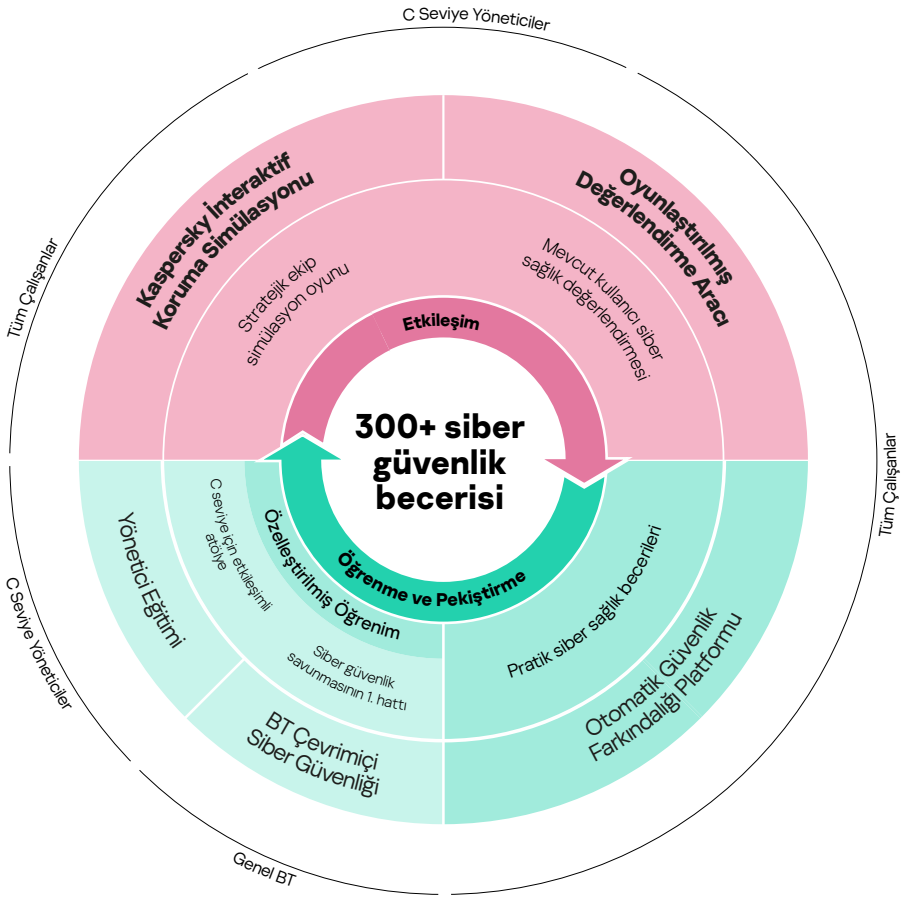
%79
oranında çalışan
risklerin farkında olmalarına rağmen geçtiğimiz bir yıl içerisinde en azından bir kez riskli aktivitede bulunduğunu kabul etmektedir***

164$
kayıt başına
2.200 ila 102.000 arasında kayıt içeren ihlaller için ortalama küresel maliyet****

1000'den fazla çalışana sahip şirketlerde çalışan
%42 oranında katılımcı
katıldıkları eğitim programlarının çoğunun yararsız olduğunu ve ilgilerini çekmediğini söyledi*****

Çalışanların davranışlarını değiştirmek, yaşayabileceğiniz en büyük siber güvenlik zorluğudur. İnsanlar genellikle beceri kazanmaya ve alışkanlıklarını değiştirmeye motive olmazlar, bu yüzden pek çok eğitim girişimi neredeyse boş bir formaliteye dönüşür. Etkili eğitim, insan doğasının özelliklerini ve kazanılan becerileri özümseme yeteneğini dikkate alan farklı bileşenlerden oluşur. Siber güvenlik uzmanları olarak Kaspersky, siber açıdan güvenli kullanıcı davranışının neye benzediğini bilir. İçgörülerimizi ve uzmanlığımızı kullanarak, müşterilerimizin çalışanlarını saldırılara karşı bağışık hâle getirirken onlara kısıtlamalar olmadan hareket etme özgürlüğü verecek öğrenme teknikleri ve yöntemleri ekledik.

Kuruluşlardaki farklı seviyeler için farklı eğitim formatları



* "IT Security Economics 2022", Kaspersky
** Veri İhlali Soruşturmaları Raporu, 2022
*** «Balancing Risk, Productivity, and Security», Delinea 2021
**** Veri İhlali Maliyeti, 2022. IBM
***** Capgemini "Dijital yetenek boşluğu"

Kaspersky Güvenlik Farkındalığı çözümleri

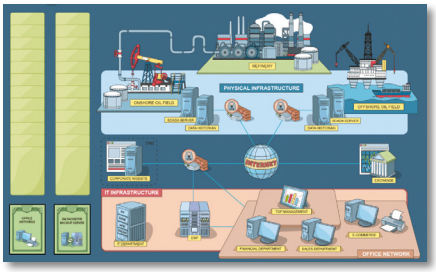
Katılım ve motivasyon

Çalışanlar her zaman zorunlu eğitim konusunda istekli değildir ve konu siber güvenlik olduğunda çoğu kişi bunun çok karmaşık veya sıkıcı olduğunu düşünür veya bunlarla hiçbir ilgisi olmadığına inanır. Öğrenme motivasyonu olmadan öğrenme sonucunun çok olumlu olması olası değildir. Eğitimden sorumlu kişiler için bir başka zorluk da, hataları şirkete herkesinki kadar pahalıya mal olsa da şirket yöneticilerini eğitime dâhil etmektir. Oyunlaştırma burada devreye girer çünkü çok ilgi çekicidir, personelinizi eğitime karşı ilk dirençlerinin üstesinden gelmeye teşvik etmenin en etkili yoludur.

CEO'ların **%76'sı** bir işi daha hızlı yapmak için güvenlik protokollerini atladıklarını, hız için güvenliği feda ettiklerini itiraf ediyor*.

Yöneticilerin **%62'si** kurumlarında BT güvenliğine ilişkin iletişimsizliğin en az bir siber güvenlik olayına yol açtığını kabul ediyor**

KIPS eğitimi üst düzey yöneticilerin, iş sistemleri uzmanlarının ve BT uzmanlarının her türlü BT sistemi ve sürecini kullanmaya ilişkin riskler ve zorluklarla ilgili farkındalığını artırmayı hedefler.



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

KIPS, karar makamları (kıdemli yöneticiler, BT ve siber güvenlik görevlileri) arasında anlayış oluşturan ve siber güvenlik algılarını değiştiren 2 saatlik etkileşimli bir takım oyunudur. Kötü amaçlı yazılımların ve diğer saldırıların işletme performansı ve geliri üzerindeki gerçek etkisine ilişkin bir yazılım simülasyonu sunar. Oyuncuları stratejik düşünmeye, bir saldırının sonuçlarını tahmin etmeye, zaman ve para kısıtlamaları dâhilinde buna göre yanıt vermeye zorlar. Her karar, tüm diğer iş süreçlerini de etkiler; temel amaç, işlerin sorunsuz şekilde yürümesini sağlamaktır. Oyunu en fazla gelirle bitiren, siber güvenlik sistemindeki tüm tuzakları bulup analiz eden ve uygun şekilde müdahale eden takım kazanır.

13 endüstriyel senaryo
(sürekli yeni eklemeler yapılmaktadır)

Her senaryo, siber güvenliğin iş sürekliliği ve kârlılık açısından rolünü ortaya koymakta, ortaya çıkan zorlukları, tehditleri ve kuruluşların siber güvenliklerini oluştururken yaptıkları tipik hataları vurgulamaktadır. Ayrıca siber tehditlere karşı istikrarlı operasyonların ve sürdürülebilirliğin korunmasına yardımcı olan satış ve güvenlik ekipleri arasındaki iş birliğini de teşvik eder.

KIPS iki şekilde sunulur

Çok popüler olan KIPS Çevrimiçi seçeneği, sahadaki yüz yüze rekabet avantajı sayesinde tarif edilemez bir heyecan ve coşku atmosferi yaratıyor. Bir kurum içerisinde siber güvenlik kültürünün oluşturulması ve benimsenmesi için harika bir araçtır.

KIPS Çevrimiçi versiyonunda, kullanıcılar bulundukları herhangi bir yerden çok sayıda katılımcıyla etkileşime geçebilirler. Küresel kuruluşlar veya halka açık etkinlikler için mükemmel olan KIPS Çevrimiçi, uzaktaki ekipleri sahadaki etkinliğe eklemek için KIPS Canlı ile birleştirilebilir.

- Herhangi bir konumdan aynı anda yaklaşık 300 takım (= 1000 katılımcı).
- Farklı takımlar, farklı dillerde oyun arayüzü seçebilirler.
- Müşteriler, kütüphaneden oyundaki saldırıların sayısını ve türlerini belirleyerek önceden yüklenmiş senaryoları kişiselleştirebilir.
- Çevrimiçi versiyonun bir diğer avantajı da oyuncuların tercihlerine ilişkin istatistikler, takımların belirli durumlardaki eylemlerine ilişkin veriler ve bir önceki oyuna göre oyuncu eylemlerinin bir karşılaştırmasını alabilmektir.

Ticari girişimler için KIPS

Lisans süresi boyunca istedikleri sıklıkta KIPS oynamalarına izin veren bir lisansa sahip olan müşteriler, önceden tanımlanmış ayarlarla oynayabilir veya kütüphaneden farklı saldırılar seçip birleştirerek oyun senaryosunu her oynadıklarında kişiselleştirebilirler. Bu işlevsellik oyunu her seferinde değiştirerek daha da ilginç hale getirir.

* https://www.forbes.com/sites/louiscolumbus/2020/05/29/cybersecuritysgreatest-insider-threat-is-in-thec-suite/?sh=466624f87626

** https://www.kaspersky.com/blog/speakfluent-infosec-2023/

Başlangıç noktası

İnsanlar genellikle yetersizlik düzeylerinin farkında değildir ve bu da onları özellikle savunmasız hâle getirir. Diğer eğitimlerin etkili olabilmesi için teste tabi tutulmaları ve siber güvenlik yeterlilik düzeyleri hakkında ayrıntılı ve net geri bildirim almaları gerekir. Bu, aşina olunan materyaller üzerinde zaman kaybedilmemesini de sağlar.

Oyunlaştırılmış Değerlendirme Aracı: çalışanların siber güvenlik becerilerini değerlendirmenin hızlı ve heyecan verici yolu

Kaspersky Oyunlaştırılmış Değerlendirme Aracı (GAT), çalışanlarınızın siber güvenlik bilgi düzeylerini hızlı bir şekilde tahmin etmenize olanak tanır. İlgi çekici interaktif yaklaşım, klasik değerlendirme araçlarında sıklıkla görülen sıkılma hâlini ortadan kaldırır. Çalışanların 15 dakika içinde siber güvenlikle ilgili 12 günlük durumu gözden geçirmeleri, karakterin eylemlerinin riskli olup olmadığını değerlendirmeleri ve müdahalelerindeki güven düzeyini ifade etmeleri gerekir.

Tamamlandıktan sonra kullanıcılar, siber güvenlik farkındalığı düzeylerini yansıtan bir puana sahip bir sertifika alırlar. Ayrıca açıklamalar ve faydalı ipuçları ile her alan hakkında geri bildirim alırlar.

GAT'nin oyunlaştırılmış yaklaşımı, çalışanları motive ederken aynı zamanda belirli siber güvenlik durumlarını çözmelerini sağlayarak konuyla ilgili bilgilerinde boşluklar olabileceğini de gösterir. Bu aynı zamanda BT/İK departmanlarının kuruluşlarındaki siber güvenlik farkındalığı düzeylerini daha iyi anlamaları için faydalıdır ve daha geniş bir eğitim kampanyasına giriş aşaması olarak işlev görebilir.

Öğrenme

Çevrimiçi öğrenme platformumuz, farkındalık programının temelini oluşturur. **300'den fazla siber güvenlik becerisi** ile tüm önemli BT güvenliği konularını kapsar.
Her ders çeşitli vakalar ve gerçek hayattan örnekler içerir, böylece çalışanlar günlük işlerinde başa çıkmak zorunda oldukları süreçlerle bağlantı kurabilir. Ayrıca bu becerileri ilk dersin hemen ardından kullanmaya başlayabilirler.

Kaspersky Otomatik Güvenlik Farkındalığı Platformu: her ölçekten kuruluş için verimlilik ve eğitim yönetimi kolaylığı

Kaspersky ASAP, çalışanların siber güvenlik becerilerini şekillendiren ve onları doğru şekilde davranmaya motive eden etkili ve kullanımı kolay bir çevrimiçi araçtır.

Eğitim tüm şirketlerin güvenlik farkındalığı gereksinimlerini karşılasa da, otomatikleştirilmiş yönetim öncelikle özel eğitim yönetimi kaynaklarına sahip olmayanlara hitap edecektir.

Temel avantajlar:

- **Tam otomasyon sayesinde basitlik:** Programın başlatılması, yapılandırılması ve izlenmesi çok kolaydır. Takip eden süreçteki yönetim tamamen otomatikleştirilmiştir ve yönetici müdahalesi gerektirmez. Platform kendiliğinden, her bir çalışan grubu için bir eğitim programı oluşturur ve farklı eğitim formatlarını karıştırarak otomatik olarak sunulan aralıklı öğrenme sağlar.

- **Her biri yöneticilerin işini kolaylaştıracak sayısız özellik.....:**Otomatikleştirilmiş platform yönetimi, AD (Active Directory) ile senkronizasyon, SSO (Tekli Oturum Açma), Open API (üçüncü taraf çözümleriyle etkileşim olanağı), kullanıcı dostu bir gösterge paneli, ilk ziyaret sırasında çevrimiçi katılım olanağı, SSS bölümü ve ipuçları – tüm bu özellikler, platform yönetimini kolay ve verimli kılar.

Kaspersky ASAP: çalışanların siber güvenlik becerilerini seviye seviye geliştiren, yönetimi kolay çevrimiçi araç

ASAP'de ele alınan konular:

- Parolalar ve Hesaplar
- E-posta
- Web Siteleri ve İnternet
- Sosyal Medya ve Mesajlaşma Uygulamaları
- Bilgisayar Güvenliği
- Mobil Cihazlar
- Gizli verilerin korunması
- GDPR
- Endüstriyel Siber Güvenlik
- Kişisel veriler
- Banka kartı güvenliği ve PCI DSS
- Doxing (bilgilerinizin ifşa edilmesi)
- Kripto para güvenliği
- Uzaktan çalışılan zamanlarda bilgi güvenliği
- 152-FZ sayılı Rusya Federal Yasası

ASAP Hızlandırılmış kurs

Eğitimin görsel-işitsel formatta kısa bir sürümü.

- Etkileşimli teori
- Videolar
- Testler

Kaspersky ASAP, çok dilli bir çözümdür.

ASAP, MSP'ler ve xSP'ler için idealdir: birden fazla işletme için eğitim hizmetleri tek bir hesap üzerinden yönetilebilir ve aylık lisans abonelikleri mevcuttur.

Kaspersky ASAP'ın tam işlevsel sürümünü asap.kaspersky.com adresinde deneyin kendi kurumsal güvenlik farkındalığı eğitim programınızı oluşturmanın ve yönetmenin ne kadar kolay olduğunu kendiniz görün!

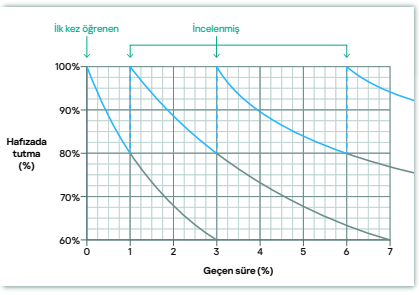
Birleştirme

Güçlendirme, öğrenme programının önemli bir parçasıdır ve öğrenme sırasında kazanılan bilgi ve becerileri pekiştirmek için gereklidir.

Öğrenilen becerileri alışkanlıklara dönüştürmenin en iyi yolu uygulamaya koymaktır. Aynı zamanda insanlar bazen hata yapar ve kişisel deneyimlerinden ders alırlar. Ancak konu siber güvenlik olduğunda, kendi hatalarınızdan ders çıkarmak çok pahalıya mal olabilir.

Oyunlaştırılmış eğitim yoluyla kendinize veya şirketinize herhangi bir zarar vermeden bir durumu "yaşayabilir" ve sonuçlarını deneyimleyebilirsiniz.

%70
oranında öğrenilen bilgi
geleneksel eğitim biçimlerinde bir gün içinde unutulur

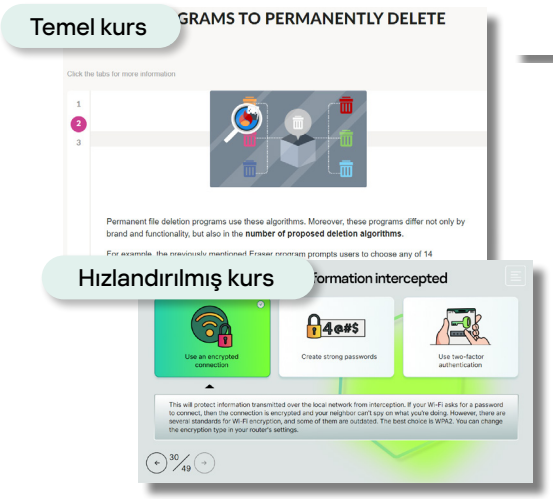


- **.....kullanıcıların işini kolaylaştıracak özellikler:** Anlaşılır ders yapısı, küçük boyutlu dersler, gerçek hayattan örnekler, kullanıcı dostu arayüz, e-posta hatırlatıcıları, gerektiğinde derslere geri dönme ve tekrar etme olanağı, PC veya mobil uyumlu arayüz – tüm bu özellikler, öğrenme sürecini keyifli, ilginç ve etkili hale getirir.
- **Ön tanımlı öğrenme etkisi:** Program içeriği, sürekli pekiştirme sayesinde artan aralıklı öğrenmeyi destekleyecek şekilde yapılandırılmıştır. Metodoloji, bilginin akılda tutulmasını ve sonraki becerilerin uygulanmasını sağlamak için insan hafızasının çalışma dinamiklerine göre tasarlanmıştır.
- **Kişiselleştirme:** Eğitim programının görünümü kolayca değiştirilebilir – yönetici ve öğrenci portalında ve platform e-postalarında Kaspersky logosunu şirketinizin logosuyla değiştirin, sertifikaları kişiselleştirin ve herhangi bir derse kişisel içerik ekleyin.
- **Esnek öğrenme**: Size uygun çalışan eğitimi seçeneğini belirleyin – Çalışanlarınıza, siber güvenlik eğitimiyle ilgili yönetmelik gerekliliklerini hızlı bir şekilde karşılamanıza veya çalışanlarınızın bilgilerini güncellemenize yardımcı olacak basit bir Hızlı kurs atayın veya siber güvenlik becerilerinin daha ayrıntılı ve kapsamlı geliştirilmesi için farklı karmaşıklık düzeylerine ayrılmış bir Temel kurs seçin.
- **Esnek lisanslama** (Hizmet Yönetimi Sağlayıcılar için): Kullanıcı başına lisanslama modeli 5'e kadar düşük sayıda lisansla başlayabilir ve birden fazla şirket tek bir hesaptan yönetilebilir.

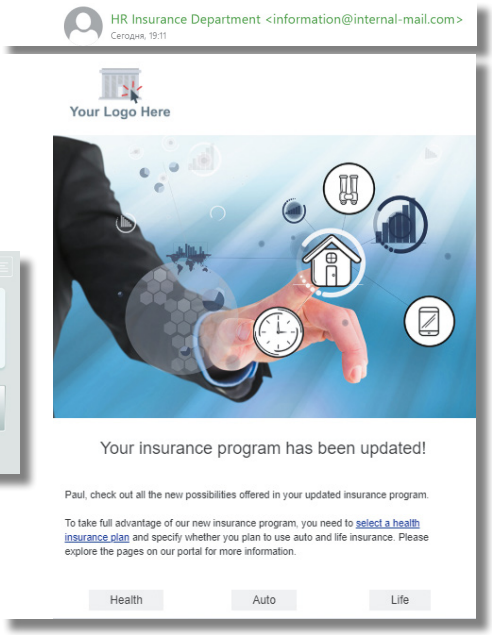
Simüle edilmiş kimlik avı kampanyaları

Kimlik avı saldırısı simülasyonları, çalışanların siber saldırılara direnme becerilerini test edip onlara yardım etmek ve şirket yönetiminin eğitimin faydalarını görmesini sağlamak için eğitim öncesinde, sırasında ve sonrasında kullanılabilir.

Etkileşimli dersler

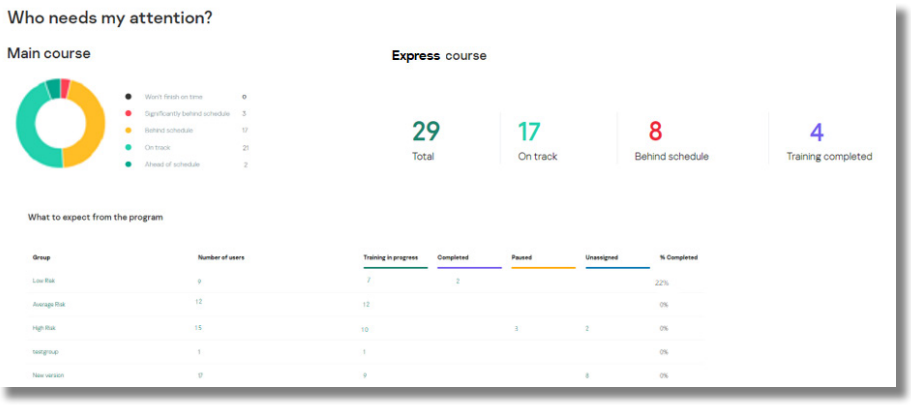


Kimlik avı saldırısı simülasyonları



Sonuçları takip etme

Panodan çalışanlarınız ilerlemesini takip edebilir, böylece tüm şirketin ve tüm grupların ilerlemesini tek bakışta değerlendirebilirsiniz. Bireysel seviyede de daha fazla ayrıntı edinebilirsiniz.



Özelleştirilmiş öğrenim

Genel BT uzmanları: Yardım masaları ve teknik alanda bilgili diğer personel, standart farkındalık programları onlar için yeterli olmadığından genellikle eğitimin dışında bırakılır. Şirketlerin de bu kişileri birer siber güvenlik uzmanına dönüştürmesine gerek yoktur. Böyle bir girişim çok pahalı, zaman alıcı ve gereksizdir.

Bu boşluğu dolduracak eğitimi duyurmaktan mutluluk duyuyoruz – uzman eğitimi kadar kapsamlı değildir, ancak sıradan çalışanlara yönelik eğitimlerden daha ileri düzeydir.

CITO eğitimi modülleri:

- Kötü amaçlı yazılım
- Potansiyel olarak istenmeyen programlar ve dosyalar
- Araştırma temelleri
- Kimlik avı olay müdahalesi
- Sunucu güvenliği
- Active Directory Güvenliği

CITO gönderim yöntemi:

Bulut veya SCORM formatı

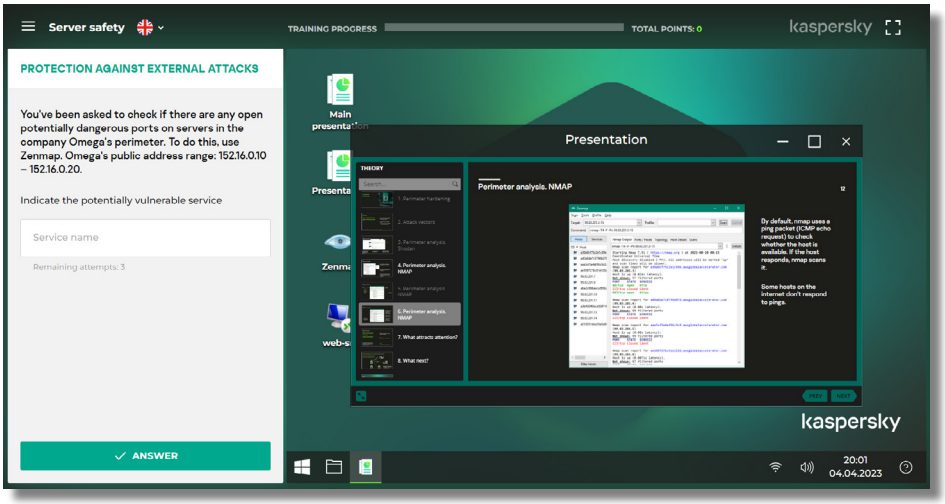
Cybersecurity for IT Online: Olay savunmasının ilk hattı

Cybersecurity for IT Online, BT ile ilgilenenlere yönelik etkileşimli bir eğitimdir. Güçlü siber güvenlik ve birinci seviye olay müdahalesi becerileri geliştirir.

Program, BT uzmanlarına görünüşte iyi huylu bir bilgisayar olayında olası bir saldırı senaryosunu tanımak üzere pratik beceriler kazandırır. Aynı zamanda tüm BT ekibi üyelerinin güvenlik savunmasının ilk hattı olarak rolünü güçlendirerek kötü amaçlı belirtileri bulmaya teşvik eder.

CITO ayrıca, BT uzmanlarınıza teorik, pratik ve alıştırmaya dayalı beceriler kazandırarak BT güvenliğine verilecek olay verilerini toplamalarına olanak sağlamak için BT güvenlik araçlarının ve yazılımlarının nasıl kullanılacağını ve araştırma temellerini öğretir.

Bu eğitim, başta hizmet masaları ve sistem yöneticileri olmak üzere kuruluşunuzdaki tüm BT uzmanları için önerilir. Uzman olmayan çoğu BT güvenliği ekip üyesi de bu kurstan yararlanabilir.



Yöneticiler için ideal bir çözüm

Üst düzey yöneticiler, siber suçlular için en ideal hedefler arasındadır; ancak eğitimciler için de üst düzey yöneticilere yönelik eğitimler oluşturmak gerçek bir zorluk teşkil eder. Ancak, üst düzey yöneticiler, siber güvenlik girişimlerine katılım ve destek sağlayıp bu alanı savunmadığı sürece bir kuruluşta siber güvenlik kültürü oluşturmak imkansızdır.

Siber güvenlik, proje yönetimi, finansal araçlar ve işletmenin operasyonel verimliliği ile birlikte gelir yaratmada önemli bir unsurdur. Bu, yöneticiler için oluşturduğumuz kursun odak noktasıdır.

Yönetici Eğitimi:

Yönetici eğitim programımızda işletme liderleri ve üst düzey yöneticiler, siber tehditleri ve bunlara karşı nasıl korunulacağını daha iyi anlamalarını sağlayan ve eğitmen liderliğinde sürdürülen interaktif bir kurs veya çevrimiçi dersler aracılığıyla siber güvenlikle ilgili temel bilgileri öğrenirler.

Kurs kapsamında özellikle siber güvenliğin finansal yönlerine ve buna yatırım yapmanın fizibilitesine önem verilerek C seviye yöneticilerinizin siber güvenlik ve iş verimliliği arasındaki bağlantıyı daha iyi anlamaları sağlanır. Yöneticileriniz, mevcut tehdit ortamının işletmeniz için ne anlama geldiğini, bir siber saldırı durumunda ne gibi önlemler almanız gerektiğini öğrenecekler ve bunlara ek olarak birçok ilginç, konuyla yakından ilgili ve faydalı bilgi edinecekler.

Bu kurstan daha da fazla yarar sağlamak için KIPS eğitimi ile birleştirilmesi önerilir. Yöneticilere yönelik eğitim, Güvenlik Farkındalığı yaklaşımınıza bağlı olarak KIPS'ten önce veya sonra alınabilir.

* Güncel modül listesini cito-training.com adresinde bulabilirsiniz

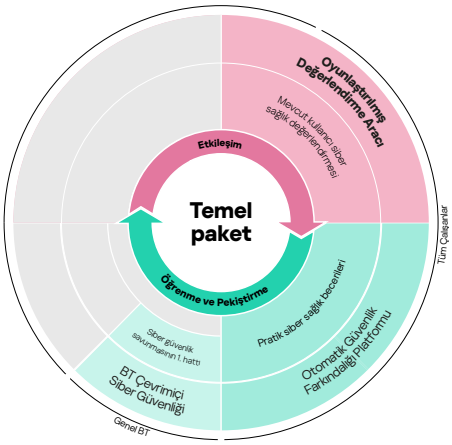
Kaspersky Güvenlik Farkındalığı: esnek eğitim yöntemleri

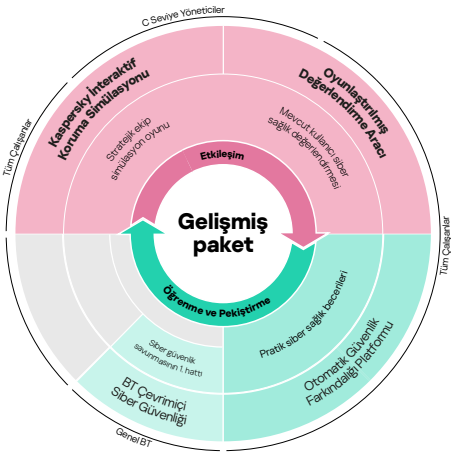
Kaspersky eğitim çözümleri, şirketinizin her seviyesini kapsar ve tek başına veya toplu olarak kullanılabilir. Ayrıca ihtiyaçlarınıza göre hazırlanmış paketleri kullanmaya başlamanızı da kolaylaştırıyoruz.

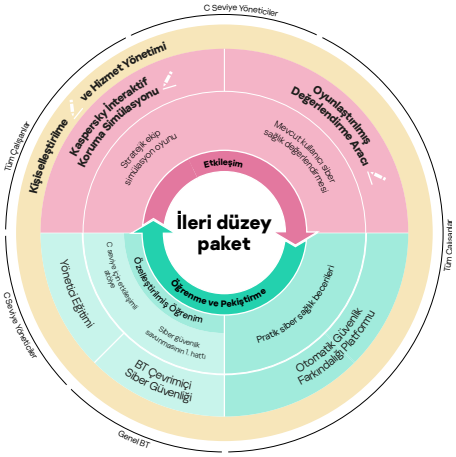
Çalışanların siber güvenlik farkındalığını artırmak için zahmetsiz bir seçenek – kurulumu kolay, yönetimi kolay.
Kurumsal işleyişinizi başarılı bir şekilde sürdürmenize ve genel siber güvenlik eğitimi açısından yasal düzenlemelerde belirtilen gereksinimleri veya üçüncü taraf gereksinimlerini karşılamanıza yardımcı olacak temel düzeyde bir güvenlik eğitimi sağlar.

Basit ve 'eksiksiz' bir eğitim çözümü kullanarak daha büyük kuruluşların iş sürekliliğini sürdürmesine yardımcı olur. Öğrenme döngüsünün her aşamasını kapsayarak her kuruluş seviyesini destekler ve davranışı değiştirir.

Kişiselleştirme ve hizmet yönetimi sayesinde maksimum siber güvenlik farkındalığı oluşturur. Böylece, yöneticilerin tehdit senaryoları hakkında yeterli bilgi sahibi olması, çalışanların otomatik siber güvenlik becerilerine sahip olması ve genel BT personelinin ilk savunma hattı olarak sizi desteklemesi sağlanır.







Kaspersky Güvenlik Farkındalığı eğitimi, başarıyı sağlamak için en son eğitim yöntemlerini ve gelişmiş teknikleri kullanır. Esnek yeni paketteki çözümler ihtiyaçlarınıza göre uyarlanabilir, dolayısıyla herkes için bir çözüm vardır. kaspersky.com.tr/awareness adresini ziyaret ederek daha fazla bilgi alın

Kaspersky Güvenlik Farkındalığı: kaspersky.com.tr/awareness
BT Güvenliği Haberleri: business.kaspersky.com

kaspersky.com.tr

kaspersky