KASPERSKY lab

# Employee Skills Training Platform

www.kaspersky.com.tr/demo-sa

#truecybersecurity

# Employee Skills Training Platform

Becerileri ve bilgileri arttırmak çok önemlidir. Bu nedenle tipik senaryolar ve durumlar üzerinde çalışmak ve potansiyel tehditlerin yanı sıra bunlarla nasıl mücadele edileceğini anlamak için bir Çevrimiçi Beceri Platformu'na erişim sağlamak temel gereksinimlerdendir. Çevrimiçi öğrenme, adayların alıştırma yapmasını ve interaktif bir öğrenme portalı üzerinden öğrenmesini sağlar.

**Platform, Kaspersky Security Awareness eğitim programlarının bir parçasıdır**

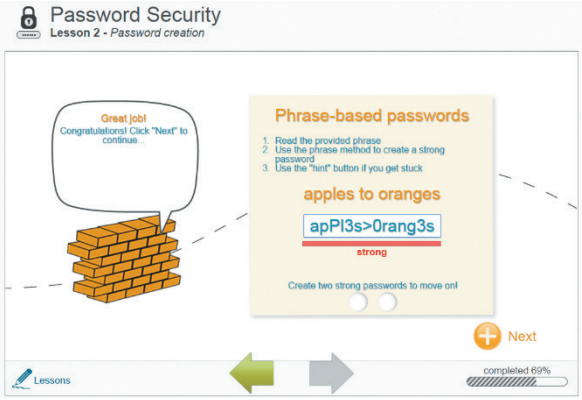
**Siber güvenlik için kolay ve etkili çözüm**

- **Hedeflerin belirlenmesi ve program seçimi:** KL global verilerine dayanarak hedef belirleme; dünya/sektör ortalaması ile karşılaştırma
- **Öğrenme yönetimi:** öğrenme otomasyonu; kendi kendine ayarlanabilen öğrenme yolu; harcanan zamanın hesaplanması
- **Raporlama ve analizler:** her zaman uygulanabilir raporlar; geliştirilebilecek alanların anında analizi
- **Program verimliliği ve değerlendirme:** gerçek oyunlaştırma, yarışmalar ve mücadele; aşırı yükü önleme

## Employee Skills Training platformunun önemli bileşenleri

### 1. İnteraktif eğitim modülleri:

- Eğlenceli ve kısa
- Zincirleme etkisi içeren alıştırmalara dayalı
- Otomatik kayıt belirli becerileri güçlendirir
- Tüm güvenlik alanlarını kapsayan 30+[1]modül




### 2. Bilgi Değerlendirmesi

Kullanıcının beceri, bilgi ve eğitim ihtiyaçlarının kapsamlı olarak belirlenmesi için. Çeşitli güvenlik alanlarını kapsar ve önceden tanımlanmış veya rastgele değerlendirmeleri, müşteri tarafından tanımlanan soruları ve özelleştirilebilir uzunluk seçeneklerini içerir.

### 3. Kimlik avı saldırıları simülasyonu

Çeşitli zorluk düzeylerindeki kimlik avı saldırısı e-postaları için kullanıma hazır özelleştirilebilir şablonlar. Çalışanlar kimlik avı e-postasını aldıklarında ve tıkladıklarında bir öğrenme fırsatı yakalar ve ilgili eğitim modülüne otomatik olarak atanırlar.

### 4. Analiz ve Raporlama

Saldırıya, Gruba, Cihaz Türüne, Tekrarlama Sayısına, Konuma göre sonuçlar.

Kaspersky Lab'in En İyi Uygulama Kılavuzu'nu (Best Practice Guide) temel alarak bu platformu kullanan Müşteri; güçlü, devamlı ve ölçülebilir bir siber güvenlik eğitim planı oluşturabilir ve uygulayabilir. Bu sayede güvenlik alanları, çalışanlar basit derslerden zor derslere ilerlerken tehdit ortamına ve çalışanların becerilerine göre değişebilir.

1 Mayıs 2018

**Değerlendirme**

Özelleştirilmiş değerlendirmelerimiz ve saldırı simülasyonlarımızın yanı sıra sahte kimlik avı ve USB saldırılarına maruz kalan çalışanlar için ipuçları ve yararlı tavsiyeler sağlayan "Öğrenme Fırsatları" aracılığıyla çalışanlarınızın bilgilerini ve kuruluşunuzun savunma düzeyini değerlendirin; Bu kısa alıştırmalar, gerçek saldırıların tehlikelerini açıklar ve çalışanları bir sonraki eğitime katılmaları için motive eder.

**Eğitim**

Çalışanlarınızı iş yerindeki ve dışarıdaki güvenlik tehditleriyle ilgili eğitmek için önemli olan interaktif eğitim modülleri menüsünden seçim yapın. 10 ila 15 dakika arasında tamamlanabilen modüller, kullanıcıların potansiyel riskleri ve kurumsal ve kişisel varlıkları nasıl koruyacağını anlamalarına yardımcı olur.

Otomatik Kayıt özelliğimiz, kimlik avı saldırıları simülasyonunda başarılı olamayan çalışanlara ve önceden tanımlanmış bilgi değerlendirme testlerinde istenen düzeyde yeterlilik göstermeyen kullanıcılara otomatik olarak eğitim atar.

**Pekiştirme**

Eğitiminizi pekiştirmek ve bilgi birikimini teşvik etmek için tasarlanan Güvenlik Farkındalığı Materyalleri ile mesajları iş yerine getirerek çalışanlara en iyi uygulamaları hatırlatın. Makaleleri paylaşın, posterleri ve görüntüleri gösterin ve katılımcıları güvenlik odaklı hediyelerle ödüllendirin.

**Ölçüm**

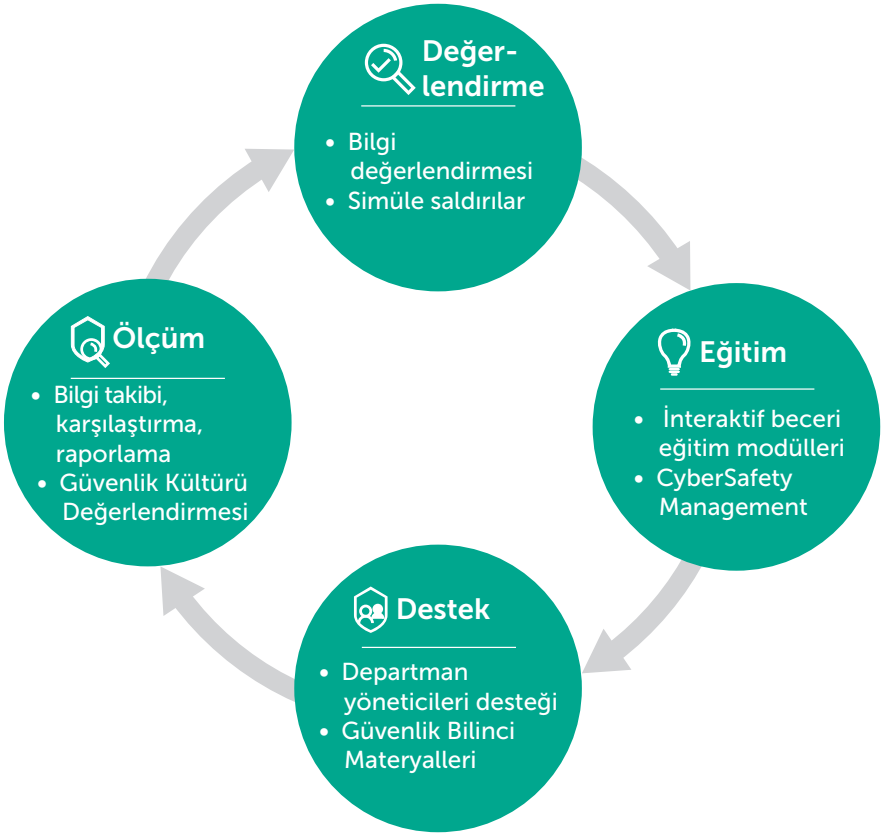
Kuruluşunuzun güçlü ve zayıf yönleri hakkında güçlü analizler toplayın, sonuçları değerlendirin ve dört adımlı döngüyü tekrarlamadan önce gelecekteki eğitimi planlayın.

# Metodoloji

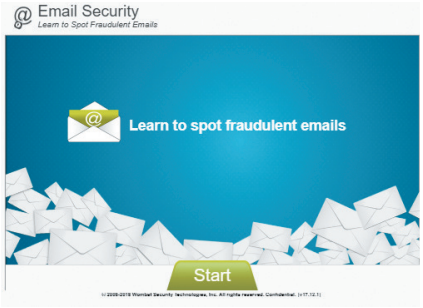
Müşterilerimiz, birçok alanda farklı avantajlardan faydalanmıştır. Bu avantajlara başarılı kimlik avı saldırılarının azalması (%90'a kadar), kötü amaçlı yazılım bulaşmalarının azalması (%95'e kadar), yardım masası çağrı hacminin azalması, çalışanların olayları daha çok bildirmesi ve güvenlik tutumunda genel bir iyileşme dahildir.

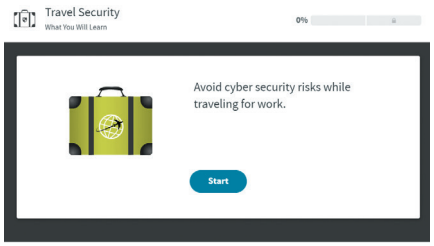
Bu sonuçlar, Sürekli Güvenlik Eğitim Metodolojisi ve siber güvenlik eğitim çözümleri uygulanarak elde edilir. Sürekli Güvenlik Eğitim Metodolojimiz dört temel adımı içerir: Değerlendir, Eğit, Pekiştir ve Ölç.

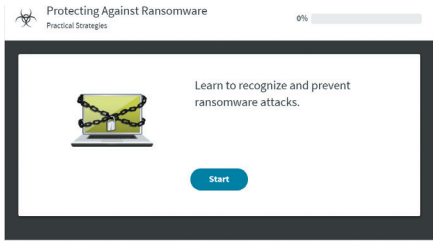
Bu bileşenler, bağımsız olarak kullanılabilmelerine rağmen en güçlü etki birlikte kullanıldıklarında elde edilir. Dört temel adımın birlikte kullanılması, güvenlik farkındalığına ve eğitimine 360 derecelik bir yaklaşımla bakılmasını sağlar. Bu adımları, bilgi güvenliği görevlileri için özel olarak geliştirilen ve programınızın kusursuz bir şekilde yürütülmesini sağlayan Security Education Platform'umuz üzerinden uygulayabilirsiniz.

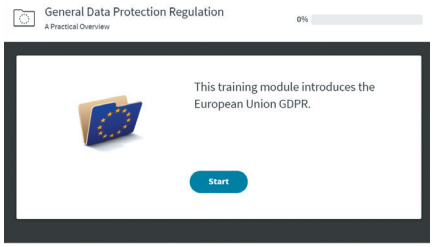



Çözümlerimiz sayesinde, güvenlik görevlileri eğitim kampanyalarını kolayca uygulayabilir, yönetebilir ve izleyebilir ve kapsamlı raporlama özellikleriyle başarıyı ölçebilir. Bu metodolojinin ilk adımlarında güvenlik görevlileri, kullanıcının bilgi düzeyini anlamak için Bilgi değerlendirmesini ve programın farkındalık düzeyini artırmak için farkındalık materyallerini kullanır. Güvenlik görevlileri, ilerleyen adımlarda kullanıcının saldırıya karşı savunmasızlığını değerlendirmek ve kullanıcıyı eğitimi tamamlamaya teşvik etmek için kimlik avı saldırısı simülasyonlarından faydalanır. Ortaya çıkan değerlendirme verileri, kritik eğitim konularına öncelik vermek için kullanılır. Ardından kullanıcıya, seçilen konulardaki interaktif yazılım eğitim modülleri atanır ve ilerleme ve tamamlama durumu izlenir. Otomatik Kayıt özelliği, gerekli doğru yanıt sayısına ulaşamayan kullanıcılara ilgili interaktif eğitim modüllerini otomatik olarak atayacaktır. Bu kullanıcı odaklı yaklaşım ile %90'lık bir eğitim tamamlama oranı elde edilebilir.




# 1. İnteraktif Eğitim Modülleri

## Mini Modüller

### Kötü Niyetli Çalışan Tehdidi Serisi (Mobil uyumlu)

- Kötü Niyetli Çalışan Tehdidine Genel Bakış: Kötü niyetli çalışan tehditlerini nasıl tanıyacağınızı ve bunlara karşı korunmak için temel en iyi uygulamaları nasıl öğreneceğinizi anlayın
- Kötü Amaçlı Çalışan Tehdidi: Gerçek dünya örnekleriyle öğrenin ve kötü amaçlı tehditleri azaltmaya yardımcı olan eylemleri keşfedin
- Kasıtsız Ortaya Çıkan Çalışan Tehditi: Çalışanların, istenmeyen tehditlere neden olan, tehditleri önleyen veya hafifleten günlük eylemlerini vurgulayan senaryoları inceleyin.

### E-postanızın Güvenliğini Sağlama – Temel Seri (Mobil uyumlu)

- Kimlik Avına Giriş (Mobil uyumlu): Şüpheli e-postaları tanımlama ve onlarla başa çıkma ile ilgili en iyi uygulamalara kısa ama açıklayıcı bir giriş yapar.
- Tehlikeli Bağlantılardan Kaçınma (Mobil uyumlu): Kullanıcılara, URL'nin gerçek hedefini bulma ve bir web sitesinin yasal veya tehlikeli olup olmadığını belirlemelerine yardımcı olabilecek genel görsel ipuçlarını incelemek için pratik yönergeler verir.
- Tehlikeli Eklerden Kaçınma (Mobil uyumlu): Kullanıcıların neden e-posta ekine şüphe ile yaklaşmaları gerektiğini ve bu tür mesajları nasıl idare edebileceklerini anlamalarına yardımcı olur.
- Veri Girişi Kimlik Avı (Mobil uyumlu) : Kötü amaçlı veri giriş formlarıyla ilgili tehlikeleri açıklar ve kullanıcıların kimlik bilgileri veya diğer hassas bilgiler için istek içeren e-postalara neden dikkat etmeleri gerektiğini anlamalarına yardımcı olur.

### E-postanızın Güvenliğini Sağlama – Gelişmiş Seri (Mobil uyumlu)

- E-posta Koruma Araçları: E-posta savunma araçlarıyla birlikte kendinizi kimlik avı dolandırıcılığından nasıl koruyacağınızı öğrenin.
- Mobil Cihazlarda E-posta Güvenliği: Mobil cihazlarda kimlik avı e-postalarını tanıma ve bunlardan kaçınma
- Hedef Odaklı Kimlik Avı Tehditleri: Hedef odaklı kimlik avı saldırılarını tanıma ve bunlardan kaçınma.

### Fidye Yazılımına Karşı Koruma (Mobil uyumlu)

- Bu mobil uyumlu mini modül, sağlık hizmetleri dahil tüm pazarlarda önemli ve artan bir tehdit olan fidye yazılımı hakkında kısa ama kapsamlı bir eğitim sunar.

### Seyahat Güvenliği (Mobil uyumlu)

- Bu mobil uyumlu mini modül, şirket cihazları ve verileri ile seyahate çıkan çalışanlar için önemlidir.

### USB Cihazı Güvenliği (Mobil uyumlu)

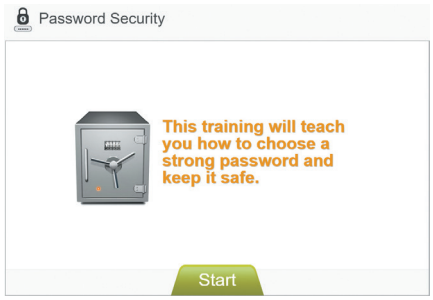
- Bu mobil uyumlu mini modül, çalışanlarınıza bilinmeyen USB sürücüleriyle ilgili tehlikeleri hızlı ve etkili bir şekilde öğretir ve kullanıcıların USB tabanlı cihazları kullanırken kişisel ve kurumsal verilerini ve sistemlerini nasıl koruyabileceklerini açıklar.

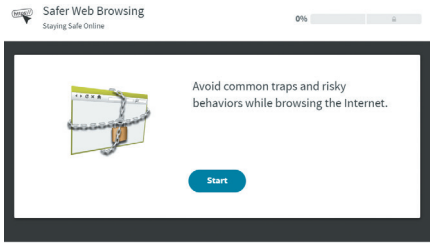
## Standart Modüller

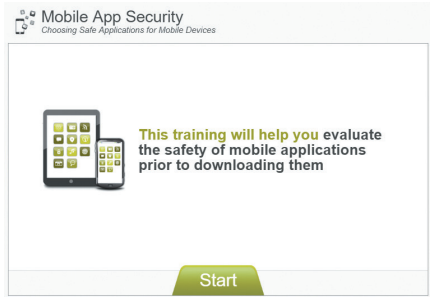
### Genel Veri Koruma Yönetmeliği (GDPR) (Mobil uyumlu)

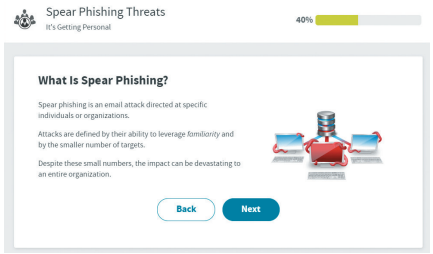
Genel Veri Koruma Yönetmeliği (GDPR), AB vatandaşları için veri koruma uygulamalarını geliştirmeyi ve AB genelindeki veri yönetmeliklerini basitleştirmeyi amaçlayan yeni bir Avrupa Birliği (AB) standartıdır.
Bu modül, aşağıdaki temel öğrenme alanlarını içerir:

- Kanun koyucular neden GDPR Yönetmeliğini geliştirdi
- Neden tüm çalışanların GDPR kapsamında bir görevi vardır
- GDPR kişisel verileri nasıl sınıflandırır
- GDPR ne tür kuruluşlar için geçerlidir
- Neler veri ihlali olarak kabul edilir
- Uyumsuzluk durumunda uygulanan cezalar
- Bireyler için veri izni, erişimi ve silme ile ilgili yeni bireysel gizlilik hakları
- Önemli veri güvenliği ve veri gizliliği kılavuzları
- Veri Koruma Görevlisinin görevleri ve sorumlulukları
- Uygunluğu artırmak ve riski azaltmak için dört önemli alan: hesap verilebilirlik; veri haritalandırma; veri sızıntılarını tespit etme ve raporlama; veri silme




### E-posta Güvenliği veya Anti-Phishing PHYLLIS™

- Kullanıcılar manipülatif içerileri, kötü niyetli ve gizli bağlantıları, tehlikeli ekleri, uygunsuz veri taleplerini ve diğer tehditleri tanımlamayı ve bunlardan kaçınmayı öğrenirler.
- Bu konuda iki farklı eğitim tarzı sunuyoruz: interaktif bir eğitim modülü ve karakter odaklı bir eğitim oyunu.

### URL Eğitimi veya Anti-Phishing PHIL™

- Çalışanlar URL'lerin nasıl oluşturulduğunu, URL uyarı işaretlerini ve kötü amaçlı bağlantıların nasıl tanımlanıp önleneceğini öğrenirler. Eğitim, manipüle edilmiş etki alanlarını, kısaltılmış URL'leri ve diğer genel ipuçlarını kapsar.

### Veri Koruma ve İmha (Mobil uyumlu)

- Çalışanlar, hassas verilerin kullanım ömrü boyunca güvenli bir şekilde yönetimi ve saklanması ile ilgili en iyi uygulamaların nasıl gerçekleştirilebileceğini öğrenir. Bu mobil uyumlu modül fiziksel dosyaların, belgelerin ve taşınabilir depolama ortamının yanı sıra elektronik cihazlar ve dosyalar için teknik önlemlerin nasıl yönetileceğini açıklar.

### Mobil Uygulama Güvenliği

- Kullanıcılar, uygulama bileşenlerini ve tehlikeli izinlerin etkilerini araştırmayı öğrenir ve bu eğitim, uygulamaları indirmeden önce güvenilirliklerini ve güvenliklerini anlamalarına yardımcı olabilir.

### Mobil Cihaz Güvenliği

- Kullanıcılar bu mobil uyumlu modülü kullanarak, fiziksel ve teknik korumaların önemini ve mobil iletişim ve bağlantıların güvenliğini geliştirmenin yollarını öğrenirler.

### Parola İlkesi (Mobil uyumlu)

- Bu modülde, parola oluşturma konusunda en iyi uygulamaları ve parolaları güvende tutmayı öğretiriz.

### Fiziksel Güvenlik

- Fiziksel güvenlik ihlallerini nasıl önleyeceğinizi ve düzelteceğinizi öğrenin ve insanların, yerlerin ve varlıkların güvenliğini sağlamaya yardımcı olacak en iyi uygulamaları edinin.

### Güvenli Sosyal Ağ İletişimi (Mobil uyumlu)

- Kullanıcılar nasıl güvenli bir şekilde paylaşım yapacağını ve sosyal ağ sitelerinde diğer kişilerle nasıl güvenli etkileşim kuracaklarını öğrenirler. Halka açık olan bu platformlardaki yaygın tuzaklardan ve hilelerden nasıl kaçınılacağını açıklarız.

### Daha Güvenli Web Taraması (Mobil uyumlu)

- Kullanıcılar, web'de gezinirken sıkça karşılaşılan tuzaklardan ve tehlikelerden nasıl kaçınacaklarını, tehlikeli olabilecek URL'leri nasıl tanıyacaklarını, kötü amaçlı yazılım ve virüslü indirmelerden nasıl kaçınacaklarını ve internet dolandırıcılıklarını nasıl tespit edeceklerini öğrenirler.

### Ofis Dışında Güvenlik (Mobil uyumlu)

- Çalışanlar, ofis dışında çalışırken verilerini, ağını ve ekipmanlarını güvende tutmak için en iyi uygulamaları öğrenirler.

### Güvenlik ile İlgili Temel Bilgiler (Mobil uyumlu)

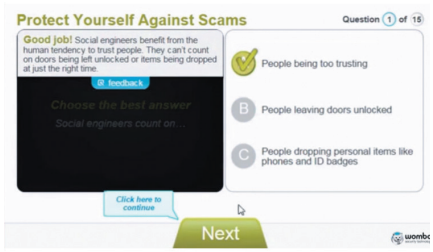
- Bu senaryo odaklı ve mobil uyumlu modül, kullanıcılara günlük işlerde ve kişisel etkinliklerde yaygın olarak karşılaşılan güvenlik sorunlarını gösterir.

### Yöneticiler için Güvenlik ile İlgili Temel Bilgiler (Mobil uyumlu)

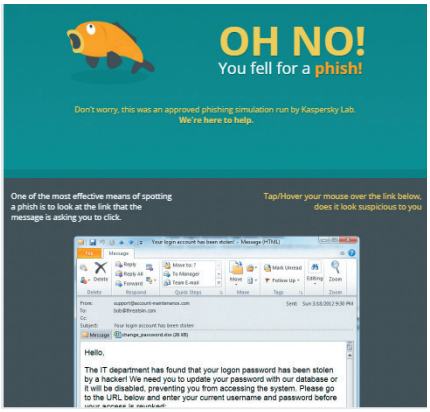
- Bu kapsamlı modül, yöneticilerin potansiyel tehditleri tanımalarına, iş ve kişisel yaşamlarında güvenlik davranışlarını geliştirmelerine ve kuruluşun her düzeyinde bir siber farkındalık kültürü oluşturmalarına yardımcı olur.

### Sosyal Mühendislik (Mobil uyumlu)

- Sosyal mühendislik dolandırıcıları, verileri çalmak, gizli ağlara erişmek ve diğer dolandırıcılıkları gerçekleştirmek amacıyla ilişkiler kurar ve insanların açık ve yardımsever olma eğiliminden yararlanırlar. Çalışanlar; insanların, alanların ve varlıkların güvenliğini sağlamayı ve ortak sosyal mühendislik tekniklerini tanımayı ve bunlardan kaçınmayı öğrenir.









### PCI DSS (Yalnızca ABD İngilizcesi) (Mobil uyumlu)

- Bu modül, çalışanlarınızın kredi kartı verilerini daha iyi yönetmesine; PCI DSS gereksinimlerini anlamasına; kayıtları ve hesapları güvenli bir şekilde yönetmesine ve güvenlik ihlallerini tanımalarına ve bu yönde harekete geçmelerine yardımcı olur.

### Kişisel Olarak Tanımlanabilir Bilgiler (PII)

- Çalışanlar, PII'yi tanımlamayı, PII'nin kullanımı, saklanması ve paylaşılması için en iyi uygulamaları ve bir PII ihlali durumunda yapılacakları öğrenirler.

### Koruma Kapsamındaki Sağlık Bilgileri (PHI) (yalnızca ABD için geçerlidir)

(Mobil uyumlu)

- Çalışanlar, PHI tanımlayıcıları hakkında bilgi edinir ve PHI'yi kullanmak, açıklamak, iletmek ve saklamak için pratik rehberlik alır.

### GDPR'nin Uygulanması

- Bu kurs ilk önce yönetmeliği tanıtır. GDPR için temel konseptleri keşfedin. Bu konseptlerin kuruluşunuzun işleyişini nasıl etkileyebileceğini düşünün. GDPR'de açıklanan konseptleri günlük durumlara ve kararlara uygulamayı öğrenin.

# 2. Bilgi Değerlendirmesi

İlk aşamadaki ve sürekli değerlendirme alıştırmaları için idealdir:

- kritik siber güvenlik konuları (kimlik avı dahil) hakkında çalışanlar için temel bir değerlendirme ölçütü oluşturma;
- mobil cihazlar ve mobil uygulamalar, veri yönetimi, fiziksel güvenlik ve daha fazlası ile ilgili güvenlik açıklarını değerlendirmek için kimlik avının ötesinde değerlendirme;
- kuruluş seviyesinden bireysel seviyeye kadar savunmasızlık alanlarının belirlenmesi;
- ilerlemeyi takip etme; halihazırda mevcut veya gelişmekte olan tehlikeli alanları belirleme.
- 2 çeşit önceden tanımlı değerlendirme sunuyoruz: belirli siber güvenlik alanlarını kapsayan değerlendirmeler veya geniş kapsamlı değerlendirmeler. Bunların dışında başka bir seçeneği de tercih edebilirsiniz:
- soru kitaplığımızı kullanarak kendi değerlendirmelerinizi oluşturmak
- kendi sorularınızı oluşturmak, yeni kategoriler tanımlamak ve değerlendirmelerde kullanmak

Değerlendirmede başarısız olanlara yönelik uygun modellerin otomatik olarak atanması için otomatik kayıt özelliği.

# 3. Kimlik avı saldırıları simülasyonu

Grup oluşturmanızı, kimlik avı e-postası simülasyonu oluşturmanızı ve doğrudan kullanıcılarınıza göndermenizi sağlar. Kullanıcılar kimlik avı simülasyonu bağlantısını tıklarsa, bir eki karşıdan yüklerse veya açılış sayfasına bilgi girerse, "anında" bir eğitim mesajı alır. Saldırı tuzağına düşen herkes, bir "öğrenme fırsatı" yakalar ve normal şartlarda kritik bir hata sayılabilecek bu hatayı yapan çalışanlar, yanlışlarını görerek eğitimin geri kalanında farklı bakış açılarına daha açık hale gelir.

## Kimlik avı saldırısı simülasyonu aracı:

- Kimlik avı e-postalarından oluşan güncel şablon kitaplığı
- Büyük bir sahte kimlik avı etki alanları listesi
- Öğrenme fırsatı kitaplığı (saldırıda başarısız olan kullanıcılar için giriş sayfaları)
- Kimlik avı saldırılarını kolayca oluşturma
- Kimlik avı e-postaları ve öğrenme fırsatları, tamamen özelleştirilebilirdir
- Saldırı simülasyonunun kapsamlı planlaması
- Siber güvenlik uzmanlarına ve yönetim kademesine yönelik olarak ayrı kullanım için dışa aktarılabilen detaylı raporlar.
- Otomatik kayıt özelliği

# 4. Analiz ve Raporlama

Çalışanların eğitimi devam ederken platform da aynı zamanda önemli ölçüm verilerini toplar ve takip eder. Platform, her çalışanın eğitim modülleri, sahte saldırılar ve bilgi değerlendirmeleri ile olan etkileşimini izler. Güvenlik görevlileri, yalnızca hangi görevlerin kimler tarafından tamamlandığını değil, aynı zamanda kullanıcıların hangi konseptte güçlü veya zayıf olduklarını ve zamanla nasıl geliştiklerini görebilir.

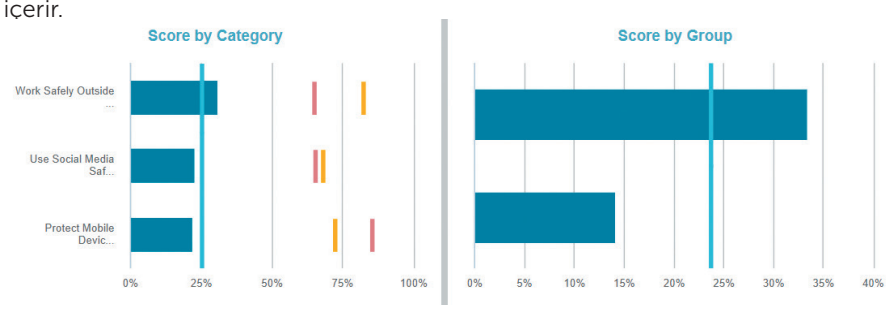
Tüm kullanıcı verileri, iş birimi, konum, departman, işe alınma tarihi vb. dahil yönetici tanımlı alanlar kullanılarak nitelendirilebilir, filtrelenebilir ve raporlanabilir.

Bilgi Değerlendirme raporu, kullanıcıların sektördeki diğer kişilere karşı nasıl performans gösterdiğini daha iyi anlamak için sektör değerlendirme verilerini içerir. Bu rapor, müşterilerin kurumsal riski daha iyi anlamalarına ve çalışanların siber güvenlik farkındalığı bilgilerinin, kendi sektöründeki ve dünyanın dört bir yanındaki diğer son kullanıcılarla karşılaştırıldığında ne durumda olduğunu bilerek eğitim çabalarını nereye yönelteceklerini görmelerine yardımcı olur.

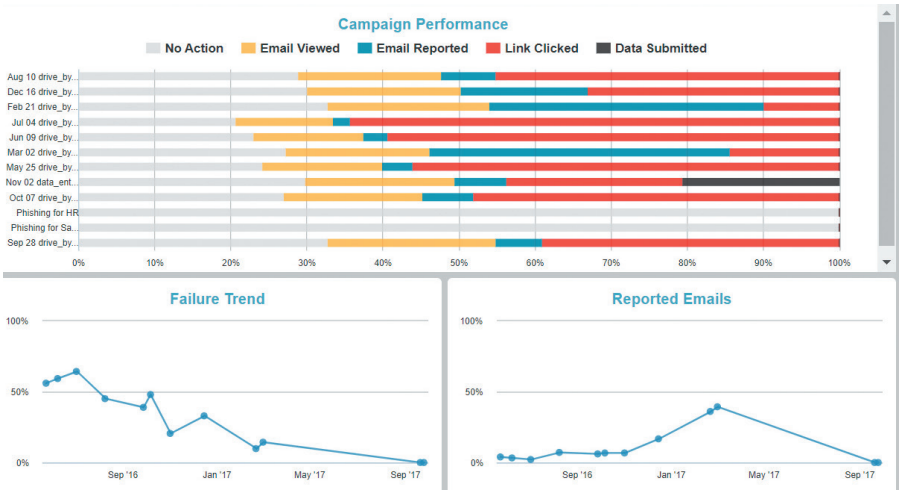
Kimlik avı simülasyonu raporu, kişisel verileri tüm müşteriler arasındaki ortalama başarısızlık oranıyla karşılaştırmanıza olanak sağlar

## Peformansınızı kıyaslama raporları ile karşılaştırın

Bilgi Değerlendirme raporu, kullanıcıların sektördeki diğer kişilere karşı nasıl performans gösterdiğini daha iyi anlamak için sektör değerlendirme verilerini içerir.




## Farkındalık Programındaki ilerlemenizi takip edin




CSV, Word, Excel veya PDF formatlarında, yöneticilerin istedikleri işletme analizlerini desteklemek için kolayca değiştirebilecekleri, döndürebilecekleri veya filtreleyebilecekleri raporlar oluşturulabilir.

# Desteklenen diller

Kaspersky Employee Skills Training Platform, tüm eğitim modüllerinde 33[2] dil setini destekler (yalnızca Amerikan İngilizcesi'nde kullanılabilen PHI modülü hariçtir).

Arapça, Çince (basitleştirilmiş ve geleneksel), Çekçe, Danca, Felemenkçe, İngilizce (Avustralya, İngiltere, ABD), Fince, Fransızca (Fransa ve Kanada), Almanca, İbranice, Hintçe, Macarca, Endonezyaca, İtalyanca, Japonca, Korece, Malayca , Norveççe, Lehçe, Portekizce, Romence, Rusça, İspanyolca (İspanya ve Latin Amerika), İsveççe, Tayca, Türkçe, Ukraynaca, Vietnamca.

Çeviriler hakkında not: İzlandaca ve Slovakça dilleri de sınırlı sayıda modül seçeneğinde mevcuttur.

# Kullanılabilir yapılandırmalar

## Uygulama seçenekleri

| Yapılandırma/dahil edilen özellikler | Kimlik Avı Koruması | Çok Konulu | Tam | Yalnızca Eğitim Modülleri |
|---|---|---|---|---|
| Bireysel modüller/dersler | 3 | Tümü (30+) | **Tümü** | Tümü |
| Kimlik avı saldırıları simülasyonu | Evet | Evet | **Evet** | - |
| Kimlik avı saldırılarından/ Değerlendirmelerden sonra Otomatik eğitim kaydı | Evet | Evet | **Evet** | - |
| Manuel Eğitim Atamaları | - | Evet | **Evet** | *) |
| CyberStrength bilgi değerlendirmesi | - | - | **Evet** | - |
| Ayrıntılı raporlar | Evet | Evet | **Evet** | *) |
| Sunma biçimi | Bulut | Bulut | **Bulut** | Şirket içinde**) |
| İçerik güncellemelerinin sunumu | Kısa Zamanda | Kısa Zamanda | **Kısa Zamanda** | Yıllık |
| Minimum kullanıcı sayısı | 250+ | 150+ | **50, 100+** | 250+ |
| Ne zaman kullanılması önerilir | Kimlik Avı ve Bilgi değerlendirme özelliklerinin çok önemli olduğu ve Kaspersky Lab tarafından sağlanan bulut veri depolama güvenliği tedbirlerinin yeterli olduğu durumlarda kullanılır. | | | Şirket içi veri depolamanın zorunlu olduğu durumlarda kullanılır. |

* Uygulanabilirlik ve tam işlevsellik, LMS işlevselliğine bağlıdır.

** Teslimat için müşterilerin SCORM 1.2 özellikleriyle uyumlu bir LMS'ye sahip olmaları gereklidir. Modern LMS'lerin çoğu buna uygundur.

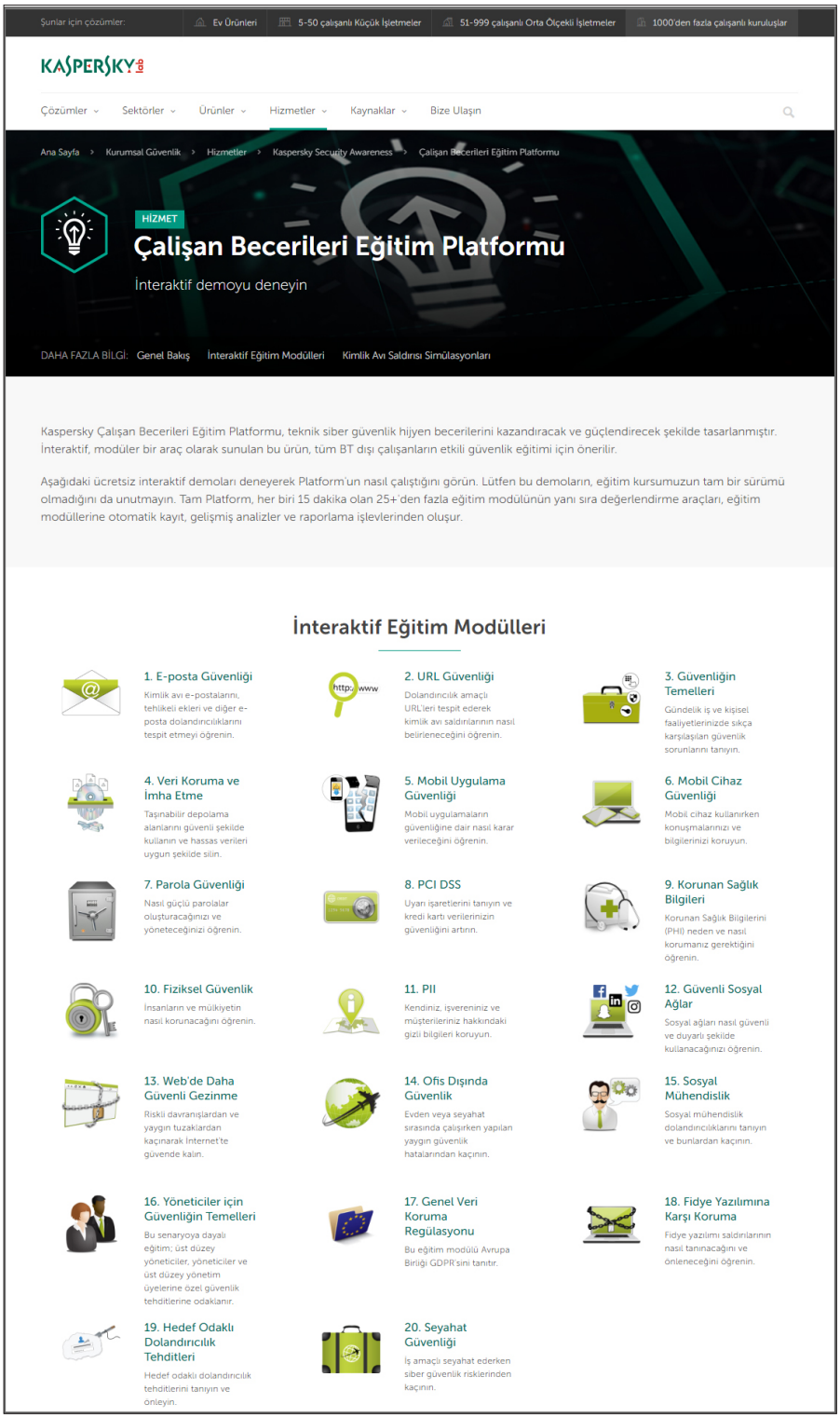
2 Mayıs 2018 itibariyle

# Platform demomuzu deneyin!

www.kaspersky.com.tr/demo-sa

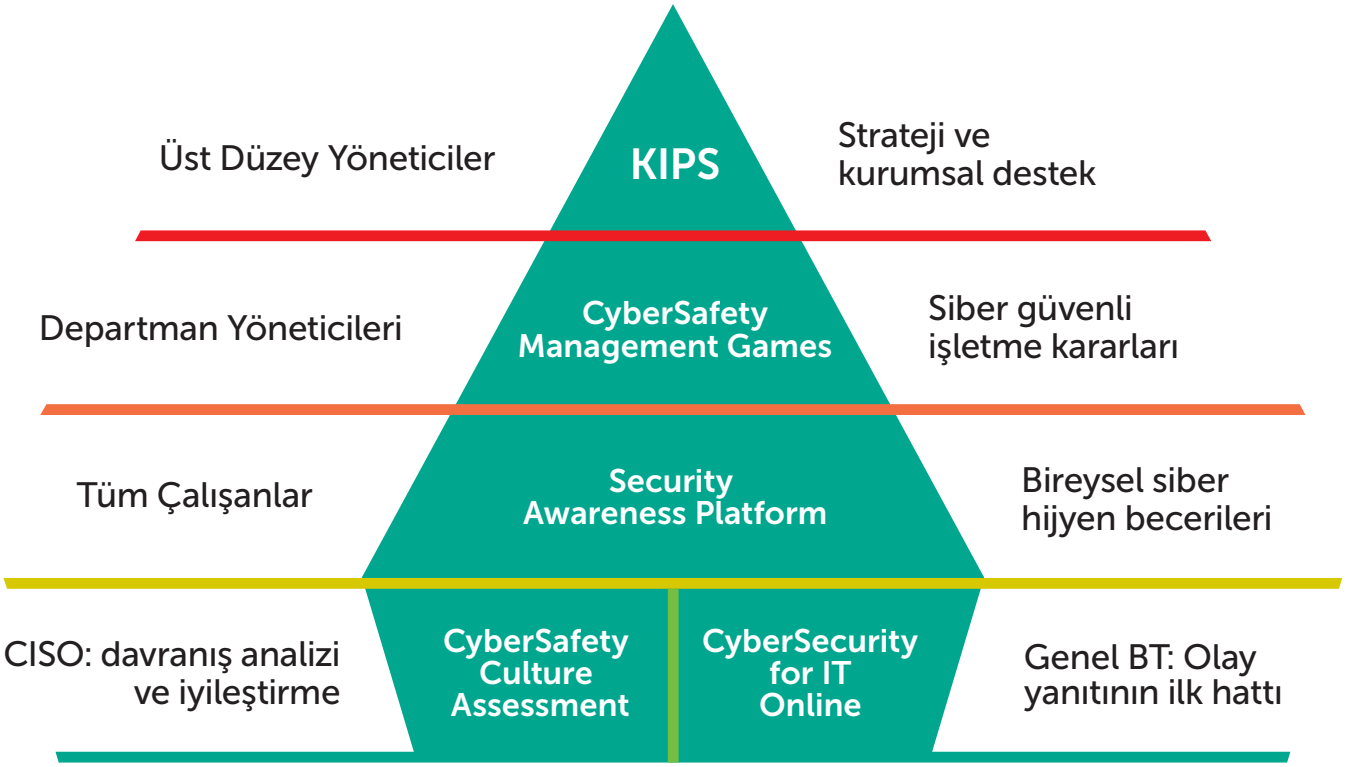
Eğitim modüllerinin ve kimlik avı saldırısı simülasyonlarının ücretsiz interaktif demosu (yerel web sitelerinde de mevcuttur)

Daha fazla bilgi için yerel Kaspersky Lab ofisi veya iş ortaklarımız ile iletişime geçin (yönetici özellikleri demosu, fiyatlandırma vb. bilgiler)



# Kaspersky® Security Awareness

Kaspersky Lab, modern eğitim teknikleri kullanan ve kurum yapısındaki her düzeye hitap eden bilgisayar tabanlı oyunlaştırılmış eğitim ürünleri ailesini piyasaya sürmüştür. Bu yaklaşım, ortak çalışmaya dayalı bir siber güvenlik kültürü oluşturarak kuruluşun tamamında kendi kendini yöneten bir siber güvenlik durumu yaratır.




**Hedeflerin belirlenmesi ve program seçimi**

Global verilere dayanan hedeflerin belirlenmesi

Dünya/endüstri ortalamalarına göre karşılaştırma

**Öğrenme yönetimi**

Öğrenme otomasyonu

Kendi kendine ayarlanan öğrenme yolu

Harcanan zamanın hesaplanması

**Raporlama ve analiz**

İstediğiniz zaman eyleme geçirilebilir raporlar

Gelişim potansiyelinin anında analizi

**Program verimliliği ve değerlendirme**

Gerçek oyunlaştırma

Rekabet ve meydan okuma

Aşırı yüklemenin önlenmesi

Maksimum
**%90**
Olayların toplam sayısında %90'a varan azalma

Minimum
**%50**
Olayların finansal etkisinde minimum %50 azalma

Maksimum
**%93**
%93'e varan oranda günlük çalışmalar için bilginin uygulanma olasılığı

Daha fazla
**30 kat**
Güvenlik farkındalığına yapılan yatırımlar için 30 kattan fazla yatırım getirisi

İnanılmaz
**%86**
Katılımcıların %86'sı deneyimi önermeye istekli

**www.kaspersky.com.tr**



Kaspersky Lab
Kurumsal Siber Güvenlik: **www.kaspersky.com.tr/enterprise**
Kaspersky Security Awareness: **www.kaspersky.com.tr/awareness**
Ürün tanıtımı: **www.kaspersky.com.tr/demo-sa**