

# CyberSafety Management Games

Bölüm Yöneticilerinin Siber Açıdan Güvenli Karar Almalarının  
Teşvik Edilmesi İçin Kapsamlı Eğitim ve Motivasyonel  
Deneyimler

[www.kaspersky.com.tr](http://www.kaspersky.com.tr)  
#truecybersecurity



# CyberSafety Management Games

## Kimlere Eğitim Verilebilir?

### Tüm Şirkette Siber Açından Güvenli Bir Çalışma Ortamını Sağlamaya Yönelik Bir Güç Olarak Bölüm Yöneticileri

Şirketlerde tipik siber güvenlik durumu (çok kötü olmayan durumlar için):

#### Kuruluş düzeyi

- Özel BT Güvenliği departmanı.
- Genel sorunları tanıma.
- Yüksek düzeyde siber güvenlik stratejisinin uygulanması.



#### Çalışan düzeyi

- Yılda bir kez siber güvenlikle ilgili uyumluluk eğitimi.
- Bazı ofis alanlarında siber güvenlik ipucu sayfaları.



Tüm kuruluşlar, siber tehditlerle mücadele etmek için BT güvenlik yapıları ve eğitim zorunluluğu gibi adımlar atmaktadır. Ancak bu yeterli midir?

- Eğitimde kazanılan bilgiler çalışanın davranışlarını gerçekten yönlendirir mi? Yoksa çalışanı yönlendiren başka bir şey midir?
- Güvenliği sağlamak için iş verimliliğinden ödün verilmeli midir?
- Güvenlikten sorumlu çalışanlar siber güvenlik mücadelelerinde seslerini herkese duyurabilmek için sayılarının çok az olduğunu düşünüyor mu?

Bu sorunlar, yalnızca bölüm yöneticileri, verimlilikten **taviz vermeden kurumların siber açıdan daha güvenli olmalarını sağlamak için görevlendirildiğinde çözülebilir.** Çalışanlarla günlük etkileşim içinde olan ve iş kararlarını alanlar yalnızca bölüm yöneticileridir. Çözüm, siber güvenliği günlük karar alma sürecinin zorunlu bir parçası haline getirmekte saklıdır.

Normalde, yönetimin siber güvenliğe katılmasını sağlamak Güvenlik ekibinin en zorlu görevlerindedir.

Bu nedenle Kaspersky Lab, bölüm yöneticilerini/orta düzey yöneticileri siber güvenlik destekçisi ve savunucusu haline getirmeyi amaçlayan özel bir eğitim programı geliştirmiştir.

#### Kuruluş düzeyi

- Özel ve iyi iletişim kuran BT Güvenliği departmanı.
- Uygulanabilir siber güvenlik stratejisi.
- Siber güvenlik ilkeleriyle uyumlu iş süreci.



#### Bölüm yöneticileri düzeyi

- Günlük çalışma hayatında siber güvenlik ilkelerinin etkili kullanımını sağlama.
- Çalışanlar için destek, gözetim ve rehberlik.



#### Çalışan düzeyi

- Sürekli siber güvenlik eğitimi.
- Öğrenme yolunda düzenli ve zaman açısından etkin değerlendirmeler ve otomatik düzenlemeler.



# Eğitim Sonucu

## Bölüm Müdürleri Siber Hijyeni Artırma Konusunda Etkileyici Güç Olmak Neler Kazanır?

Kaspersky CyberSafety Management Games, yöneticilere kendi bölümlerinde güvenli çalışma ortamını sağlamak için gereken **yeterliliği, bilgileri ve bakış açısını** kazandırır.

### Anlama

**Siber güvenlik önlemlerinin, önemli ancak karmaşık olmayan eylemler olarak içselleştirilmesi**

Yöneticiler şunları elde eder:

- "güvenlik meselesini neden önemsemeleri gerektiği" konusunda fikir edinme,
- siber suçluların bakış açısından nasıl göründüklerini anlama,
- tehditlerden kaçınmak ve onları önlemek için siber tehditlerin ve ihtimallerin farklı bir açıdan anlaşılması.

### İzleme

**Günlük çalışma sürecine siber güvenlik açısından bakma**

Yöneticiler şunları elde eder:

- güvenli ve güvenli olmayan davranışları ayırt edebilmeyi,
- Tehdit olasılığı olan durumlara dikkat etmek ve çalışanları güvenliğe yönlendirebilmek için tipik iş yerlerinde yaşanan günlük olayları "tarama".

### Siber Açıdan Güvenli Karar Verme

**İş süreçlerinin ayrılmaz bir parçası olarak siber güvenlik konuları**

Yöneticiler şunları elde eder:

- güvenlik önlemleri ve iş verimliliği arasında en iyi dengeyi seçme,
- iş projelerini, her aşamada ve dahil olan her ekip için siber risk düzeyini hesaplayarak, planlama ve uygulama,
- her projenin her adımında siber açıdan güvenli kararlar almak için ne kadar zaman ve bütçe ayrılması gerektiğini hesaplama,
- Güvenlik ekibiyle verimli bir şekilde iş birliği yapma.

Yöneticiler, güvenlik önlemlerinin karmaşık ve zaman alıcı olmak zorunda olmadığını anlar. Ayrıca kurumsal ve kişisel açıdan büyük kayıplara neden olabilecek durumlardan kaçınılmasına katkı sağlarlar.

### Güçlendirme ve Örnek Olma

**Örnek liderlik ve çalışanlara faydalı tavsiyeler**

Yöneticiler şunları elde eder:

- siber güvenlik konuları hakkındaki soruları doğru cevaplama veya emin olmadıkları konular hakkında yeterli geri bildirim verme (ör. soru soran kişiyi BT güvenlik uzmanlarına yönlendirme veya daha ayrıntılı bilgi vermelerini isteme),
- siber güvenlik değerlerine ve prosedürlerine bağlılığı muhafaza etme ve bu değerlerden şüphe duyulmasını önleme,
- personeli siber güvenlik tekniklerini aktif olarak öğrenmeye ve günlük hayatlarında kullanmaya teşvik etme
- son olarak, yöneticiler siber güvenlikle ilgili kendi motivasyonlarını artırmanın yanı sıra siber güvenliğin iş hedeflerini, kişisel önceliklerini ve zaman dengesini etkilemeyeceğini öğrenir.

## 10 farklı Güvenlik alanındaki tehditler:

Anitvirüs/Uygulamalar, Veri sızıntıları, Mobil, Web, E-posta, Mağdur davranışları, Sosyal mühendislik, Güvenlik uyarıları, Çevik olma becerisi, İlke ihlali

## Eğitmeni Eğit Yöntemi Kullanılabilir

Müşteri, CyberSafety Management Games çözümünü birden fazla departmandaki veya sahadaki daha fazla sayıda çalışanı, yöneticiyi ve uzmanı eğitmek için kullanmak isterse lisansı satın almak, şirket içi eğitimleri eğitmek ve eğitim oturumlarını (şirket içinde veya çevrimiçi) müşterinin düzenine ve rahatlığına göre sürdürmek daha mantıklı olabilir. Kaspersky Lab, bunun için aşağıdaki özelliklere sahip bir lisans sunar:

- CyberSafety Management Games eğitim programını şirket içinde kullanma hakkı,
- Eğitim materyalleri ve bunları kullanma/çoğaltma hakkı,
- CyberSafety Management Games yazılım sunucusu için oturum açma/parola,
- Program liderleri için eğitimci kılavuzu ve uygulama eğitimi,
- Bakım ve destek (yazılım ve eğitim içeriği için güncellemeler ve destek),
- Senaryonun isteğe bağlı olarak özelleştirilmesi (ek ücret uygulanır).

# Eğitim Biçimi

## Kısa Eğitim Modülleriyle Bilgisayar Tabanlı Programı Birleştirme

CyberSafety Management Games, yöneticilerin odak noktasını ve önceliklerini düzenlemenin yanı sıra onları işle ilgili durum simülasyonlarının büyüklüğü, karmaşıklığı ve güvenilirliğiyle test etmek için özel olarak tasarlanmıştır.

Bu eğitim, oyunları ve kapsamlı güvenlik konularını birleştiren **amaca yönelik CyberSafety Management Games yazılımı** tarafından desteklenmektedir. Eğitim için kolay yönetilebilir bir eğitim sürecini desteklemek amacıyla örnekler, açıklamalar ve alıştırmalar yazılımın içinde yer alır.

Bu sayede eğitim bir güvenlik uzmanı tarafından değil bir işletme eğitmeni tarafından yürütülebilir (güvenlikle ilgili tüm içerikler, yazılıma dahildir).

Katılımcıların halihazırda siber güvenlik konusunda bazı "üst düzey becerilere" sahip olduğu varsayılır. Tercihen Kaspersky Employee Skills Training Platform çözümünün birkaç modülünü geçmiş olmaları beklenir. Katılımcılar bu becerilere sahip değilse CyberSafety Management Games, kısa bir teorik girişle desteklenebilir.

## Standart Eğitim Programı

Önerilen eğitim programı, 3 modülden oluşur ve kısa teknik açıklamalar ve öğrenciler tarafından yapılan hatalar hakkında değerlendirmelerle desteklenir. Modüller, müşterinin tercihiyle eklenilebilir veya kaldırılabilir.

Program ve ayarlar, özel ihtiyaçlarınıza göre ayarlanabilir (ücret karşılığında). Ancak müşterilerimizin çoğu, her şirketin ve her yöneticinin karşılaştığı yerleri ve durumları içeren standart müfredattan memnun kalmaktadır.



## 1. Oturum. "Virüslü bilgisayarlara değil, kötü insanlara dikkat edin"

2 saat

### 1. Siber tehditleri belirleme: "Açık ofis"

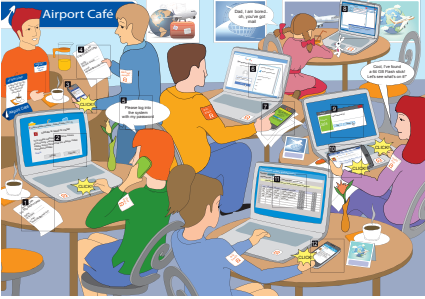
#### 2. Risk azaltma:

- Şüpheli ve normal bağlantıların karşılaştırılması
- Zayıf parolalar.  
Alıştırma "Ezberlenebilir güçlü parolalar ve parola aileleri oluşturma"
- Şüpheli ve normal eklerin karşılaştırılması
- Gizli bilgilere yetkisiz erişim.  
Alıştırma "Riski azaltmak için ne yapabilirim?"
- Gizli bilgilerin uygunsuz şekilde yayılması
- Gizli verilerin şirket dışına çıkarılması.  
Alıştırma "İş durumunu ve ilgili riskleri değerlendirme"
- Sahipsiz flash bellekler.  
Alıştırma "Riski azaltmak için ne yapabilirim?"
- İmzasız yazılımlar yükleme
- Kimlik avı e-postaları.  
Alıştırma "Sahte e-postaları belirleme"

### 3. Alıştırma "Suçlularla tanışın"

#### 4. Oturum sonucu

- **Unutmayın:** "Virüslü bilgisayarlara değil, kötü insanlara dikkat edin"
- **Yapın:** "Her zaman dijital dünyada yaptıklarınızı kimlerin kötüye kullanabileceğini düşünün"



## 2. Oturum. "Saldırıya maruz kalmanız için hedef alınmanız gerekmez"

2 saat

#### 1. Siber tehditleri belirleme: "Hareket halinde"

#### 2. Risk azaltma Alıştırmaları

- E-postaların ifşa edilmesi: kişisel/kurumsal
- Güvenlik güncellemelerinin ihmal edilmesi
- Sosyal ağlarda paylaşım yapma, bilgi sızıntısına denktir.
- Parolanın başkalarıyla paylaşılması.  
Alıştırma "İş durumunu ve ilgili riskleri değerlendirme"
- Kurumsal akıllı telefonlara uygulama yükleme
- Kilitlenmemiş PC.  
Alıştırma "Riski azaltmak için ne yapabilirim?"
- Şüpheli bağlantı.  
Alıştırma "Şüpheli URL eğitimi"
- Kamuya açık bir alanda gizli bilgilerin kullanılması
- Halka açık Wi-Fi aracılığıyla zayıf kimlik doğrulama

#### 3. Alıştırma "Mağdur profili"

#### 4. Oturum sonucu

- **Unutmayın:** "Saldırıya maruz kalmanız için hedef alınmanız gerekmez"
- **Yapın:** "Diğerlerinden daha zor bir hedef olun"



## 3. Oturum. "Siber Güvenlik herkesin sorumluluğudur"

2 saat

#### 1. Siber tehditleri belirleme: "Konferans odası"

#### 2. Risk azaltma Alıştırmaları

- Parolaların yeniden kullanımı ve saklanması
- Gizli bilgilerin yanlışlıkla ifşa edilmesi.  
Alıştırma "Riski azaltmak için ne yapabilirim?"
- DLP uyarıları
- Sosyal mühendislik saldırısı.  
Alıştırma "Sosyal mühendislik saldırılarını tanıma"
- BT Güvenliği'ni ihmal etme

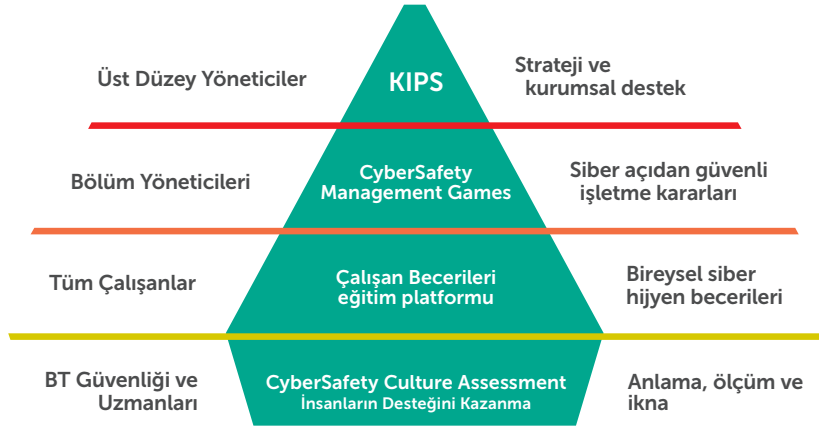


- Gizli bilgilerin şirket dışına gönderilmesi.  
Alıştırma "İş durumunu ve ilgili riskleri değerlendirme"
- Kötü amaçlı web siteleri
- Verilerin şirket dışına çıkarılması
- Gizli bilgilere yetkisiz erişim
- Eski antivirüs yazılımı
- İş amaçlarımıza güvenli bir şekilde ulaşma.  
Alıştırma "BT güvenlik departmanı ile diyalog"
- 3. Alıştırma "İşin bir parçası olarak güvenliği planlama"
- 4. Oturum sonucu
  - **Unutmayın:** "Siber Güvenlik herkesin sorumluluğudur"
  - **Yapın:** "BT Güvenlik ekibinizle işbirliği yapın"

## Kaspersky Güvenlik Farkındalığı Eğitimi Ürünleri

Siber Güvenlik Kültür Değerlendirmesi, Siber Güvenlik Kültürü metodolojisine dayalı Kaspersky Güvenlik Farkındalığı portföyünün bir parçasıdır. Siber Güvenlik Kültürü, bireyin davranışlarını bireysel veya şirket düzeyinde yönlendiren bir dizi değer ve tutumdan oluşur.

Müşterilerimize, bir dizi farkındalık eğitim programı aracılığıyla güvenlik ve İK ekiplerinin yönetimi altında bir Siber Güvenlik Kültürü geliştirme konusunda yardımcı oluruz. Eğitim programları, oyunlaştırma yöntemini kullanır ve kuruluş yapısındaki tüm seviyelere hitap eder.



## Kapsamlı Ancak Basit ve Anlaşılır

- Çok çeşitli güvenlik konuları
- Tanıdık ortamlar
- İlgi çekici eğitim süreçleri
- Pratik alışırmalar
- BT dışındaki çalışanlara uygun dil kullanımı

## Kurumsal Avantajlar

**%93**

günlük işlerde siber güvenlik bilgilerini kullanma olasılığı %93'tür

**%90**

%90'a kadar daha az siber güvenlik olayı sağlar.

**%50-60**

siber risk para hacmini %50-60 oranında düşürür

**30x**

Güvenlik Farkındalığı için yapılan yatırımlardan 30 kat yatırım getirisi sağlar





**[www.kaspersky.com.tr](http://www.kaspersky.com.tr)**

© 2017 AO Kaspersky Lab. Tüm hakları saklıdır. Tescilli ticari markalar ve hizmet markaları ilgili sahiplerinin mülkiyetindedir.

Kaspersky Lab

Kurumsal Güvenlik: [www.kaspersky.com.tr/enterprise](http://www.kaspersky.com.tr/enterprise)

Kaspersky Güvenlik Farkındalığı: [www.kaspersky.com.tr/awareness](http://www.kaspersky.com.tr/awareness)

Ürün tanıtımı: [www.kaspersky.com.tr/demo-sa](http://www.kaspersky.com.tr/demo-sa)