



Australian Government



Şimdi Harekete Geçin.
Güvende Kalın.

İnternette güvende kalmanın yolları

Kolay Okunur sürüm



Bu rehber nasıl kullanılır



Biz Avustralya Hükümeti'yiz.

Bu rehberi biz hazırladık.



Bazı kelimeleri **kalın** yazdık.

Bu kelimelerin ne anlama geldiğini açıkladık.

Bu kelimelerin listesini sayfa 28'de bulabilirsiniz.



Güvendiğiniz birinden;

- bu rehberi okumak ve
- daha fazla bilgi edinmek için yardım alabilirsiniz.



Bu, bir diğer rehberin Kolay Okunur sürümüdür.

İçeriğinde yalnızca en önemli bilgileri bulundurur.



Diğer rehberi internet sitemizde bulabilirsiniz.

www.actnowstaysecure.gov.au

Bu rehberin içerisinde neler bulunur?

Bu rehber hakkında	4
Hesaplarınızı güvende tutun	6
Bilgilerinizi korumak için ayarlarınızı kontrol edin	10
Cihazlarınızı koruyun	16
Dolandırıcılıklar	20
Sessiz kalmayın	25
Kelime listesi	28
Bize ulaşın	30

Bu rehber hakkında



Hepimizin, internette nasıl güvende kalabileceğimizi düşünmesi gerekir.

Buna **siber** güvenlik denir.



Siber kelimesi, konunun internetle ilgili olduğu anlamına gelir.



Bu rehber, internette güvende kalabilmek için alabileceğiniz birtakım önlemlerden bahseder.

Örneğin, **siber suçlardan** korunmak için.



Siber suçlar, suçluların internet üzerinden işlediği suçlardır.

Örneğin, interneti kullanarak:

- kişisel bilgilerinizi çalabilir
- çevrim içi hesap ve profillerinizi ele geçirebilirler.

Siber suçlar her cihazı hedef alabilir.



Buna řu cihazlar dâhildir:

- bilgisayarınız
- akıllı telefonunuz
- akıllı saatiniz.



Kendinizi siber suçlardan korumak için
alabileceğiniz bazı önlemler bulunmaktadır.



Bu önlemleri sonraki sayfalarda bulabilirsiniz.

Hesaplarınızı gvende tutun



evrim ii hesaplarınızı korumak iin neler yapabileceğiniz hakkında dşnmelisiniz.

Gl ve farklı parolalar kullanın



Parola daha gl bir Őfre trdr.

Başkalarının tahmin etmesi olduka zordur.



Gl ve farklı parola kullanmak hesaplarınızı korumanın en iyi yollarından biridir.



Her bir evrim ii hesabınız iin farklı bir parola kullanmalısınız.



Güçlü parolalarda şu özellikler bulunur:

- 4 ya da daha fazla rastgele seçilmiş kelime
- 15 ya da daha fazla harf veya numara.



Büyük harfler de kullanabilirsiniz.



Ayrıca, şu gibi semboller de kullanabilirsiniz;

- tire
- dolar işareti
- e-posta adreslerinde kullanılan @ işareti.



Parolalarınızda herhangi bir kişisel bilgi kullanmamalısınız.



Örneğin;

- doğum tarihiniz
- aile bireyleri veya evcil hayvanlarınızın isimleri.

Hesaplarınıza erişim için ilave güvenlik adımları ekleyin



Hesaplarınızı **çok faktörlü kimlik doğrulama (MFA)** ile koruyabilirsiniz.

MFA, hesaplarınıza giriş yaparken her seferinde 2 veya daha fazla farklı yöntem kullanmanız demektir.



Örneğin, önce parolanızı girmeniz gerekebilir.

Ardından, telefonunuza gelen bir kodu girersiniz.

Ŗu seeneklerden birini tercih etmeniz
gerekebilir:



- Telefonunuza kod reten bir uygulama
yklemek



- kodun size e-posta aracılıėıyla gnderilmesi



- kodun size kısa mesaj olarak gnderilmesi.



MFA, bařkalarının evrim ii hesaplarınıza eriřim
saėlamasını zorlařtırır.

Parolanızı ğrenseler bile. hesaplarınıza
eriřemezler.

Bilgilerinizi korumak için ayarlarınızı kontrol edin



Ayarlarınızın, sizin çevrim içi bilgilerinizi koruyup korumadığını kontrol edebilirsiniz.



Bu, aşağıdakiler üzerindeki ayarları içerir:

- çevrim içi hesaplarınız
- cihazlarınız
- uygulamalarınız



İsterseniz;

- ayarlarınızı değiştirebilirsiniz
- hangi uygulamaların bilgilerinizi kullanabileceğini seçebilirsiniz.

Cihazınızın ayarlarına erişmek için;



- dişli çark (ayarlar) simgesini bulabilir
ya da
- cihazınızın arama çubuğuna 'settings
(ayarlar)' yazabilirsiniz.



Bir uygulama veya çevrim içi hesaptaki ayarlara,
menüyü açarak erişebilirsiniz.

Genellikle menüler 3 düz çizgi ile gösterilir.



Bu ayarlardan bazıları şu bilgilerin paylaşımına
olanak sağlar;

- kim olduğunuz
- bulunduğunuz yer
- yaşadığınız yer.



Bu bilgileri çevrim içi ortamda paylaşmak sizi siber suçlara maruz bırakabilir.



Siber suçlular, sizin bilgilerinizi kullanarak siz imiş gibi davranabilirler.

Örneğin, şu bilgileri kullanabilirler;



- yaşadığınız yer



- aile bireylerinizin isimleri



- evcil hayvanlarınızın isimleri.



Hesaplarınızı, sosyal medya profillerinizi yalnızca tanıdığınız kişilerin görebileceği şekilde ayarlayabilirsiniz.

Örneğin, Facebook hesabınız.



Bu ayarlara genellikle gizlilik ayarları denir.



Konum ayarlarınızı da kontrol edebilirsiniz.

Konum ayarları cihazınızın bulunduğu yeri gösterir.



Konum ayarlarınızı açmak ve kapatmak mümkündür.

Ayrıca, hangi uygulamaların konumunuza erişebileceğini seçebilirsiniz.



Bunu aşağıdakiler için yapabilirsiniz:

- çevrim içi hesaplarınız
- cihazlarınız
- uygulamalarınız.

Bazı uygulamalar Őunlar iŐin sizden izin isteyebilir:



- kameranızı kullanmak



- fotoĐraflarınızı g rmek.



Yalnızca aŐına olduĐunuz uygulamaların kameranıza ve fotoĐraflarınıza eriŐmesine izin vermelisiniz.

Cihazlarınızı koruyun



İnternette güvende kalabilmeniz için cihazlarınızı nasıl koruyacağınız hakkında düşünmelisiniz.

Örneğin, telefonunuz veya akıllı saatiniz.



Bu, internete bağlanan cihazlar için önemli bir konu.

Cihazlarınızı güncelleyin



Cihazlarınızı güncelleyerek çevrim içi ortamda güvende tutabilirsiniz.

Örneğin, telefonunuz ve dizüstü bilgisayarınız.



Cihazınız buna yazılım güncellemesi adını veriyor olabilir.



Güncellemeler cihazın kendini siber suçlara karşı korumasını sağlar.



Bir cihazı kendi kendini güncelleyecek şekilde ayarlayabilirsiniz.



Cihazlarınızı nasıl güncelleyebileceğinizle ilgili daha fazla bilgiyi internet sitemizde öğrenebilirsiniz.

[www.actnowstaysecure.gov.au/
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)

Halka açık Wi-Fi ağıları



Halka açık Wi-Fi kullanırken dikkatli olmalısınız.



Halka açık Wi-Fi, halka açık alanlarda kullanabildiğiniz ücretsiz ve kablosuz internet ağılarına denir.



Örneğin şu alanlarda;

- kafeler
- havalimanları
- oteller.



Halka açık Wi-Fi kullanırken internet sitelerine hangi bilgileri girdiğinize dikkat etmelisiniz.



Örneğin;

- banka bilgileriniz
- e-posta hesaplarınız
- sosyal medya profilleriniz.



Bazı siber suçlular halka açık Wi-Fi kullanarak;

- internette ne yaptığınızı görebilir
- bilgilerinizi çalabilirler.

Bunun sebebi;



- bu ağların herkese açık olması ve



- cihazlarınızı korumanın daha zor olmasıdır.



İnternet sitemizde, halka açık Wi-Fi kullanırken nasıl güvende kalabileceğinizi öğrenebilirsiniz.

[www.actnowstaysecure.gov.au/
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)

Dolandırıcılıklar



Bir kişinin sizi:

- kandırmaya
- paranızı almaya çalışmasına

dolandırıcılık denir.



Dolandırıcılık yapan kimseye **dolandırıcı** denir.

Dolandırıcılar size şu kanallarla kandırmaya çalışır:



- kısa mesaj veya sesli arama
- e-posta
- sosyal medya
- bir internet sitesi.



Onlar arkadaşça görünebilirler.

Fakat sizi kandırarak sizden bilgilerinizi alabilirler.

Bu bilgileri kullanarak:



- çevrim içi hesaplarınıza erişebilir



- kendilerini siz imiş gibi gösterebilir



- paranızı çalabilirler.

Dolandırıcılar ayrıca:



- sizi kandırmak için sahte hesaplar oluşturabilir



- tıklamanız için bağlantı veya reklam paylaşabilirler.

Dolandırıcılık nasıl anlaşılır

Bir dolandırıcıyı şuradan anlayabilirsiniz:



- sizden acilen bir şey yapmanızı istiyorsa



- size yüklüce bir para teklif ediyorsa



- sizden para talep ediyorsa



- sizden bir bağlantıya tıklamanızı istiyorsa.



Ayrıca dolandırıcılar, bildiğiniz ve güvendiğiniz bir kurumu taklit edebilir.

Örneğin, bankanız.



Dolandırıcılar bunu kişisel bilgilerinizi onlarla paylaşmanız için yapar.



Birinin dolandırıcı olduğunu düşünüyorsanız onlarla konuşmayı bırakmalısınız.



Kişinin gerçekten söylediği kişi olup olmadığını kontrol etmelisiniz.

Kendi bulduğunuz ve güvendiğiniz iletişim bilgilerini kullanarak o kişi veya kurumla iletişime geçebilirsiniz.



Bir şeylerin yanlış olduğunu hissederseniz hemen kendinizi korumak için harekete geçin.

Dolandırıcılıkların ihbarı



Scamwatch Avustralyalılara řu konularda yardımcı olur;

- dolandırıcılıkları anlama
- dolandırıcılıkları ihbar etme.



Scamwatch ayrıca dolandırıcılığa maruz kalan Avustralyalılara destek sunar.



Scamwatch internet sitesi üzerinden dolandırıcılıkları ihbar edebilirsiniz.

www.scamwatch.gov.au/report-a-scam

Sessiz kalmayın



Başkalarının internette kendilerini koruyabilmeleri için sessiz kalmamalısınız.

Buna şunlar dahildir:



- siber suçları ihbar etme



- bildiklerinizi aile ve arkadaşlarınızla paylaşma.



Sesinizi nasıl duyurabileceğinizi sonraki sayfalarda açıklayacağız.

Siber suçları ihbar edin

Siber suçların ihbarı devlete řu konularda yardımcı olur:



- siber suçluların bireyleri nasıl hedef aldığını anlama



- daha fazla insanı koruma.



Siber suçları ReportCyber internet sitesi üzerinden ihbar edebilirsiniz.

www.cyber.gov.au/report

Aile ve arkadaşlarınızla internette gvende kalmaya dair konuřun



İnternette gvende kalmaya dair nerilerinizi aile ve arkadaşlarınızla paylařmalısınız.

Siz de onlardan ğrenebilirsiniz.



İnternette gvende kalmaya dair bildiklerinizi paylařarak kendinizi ve evrenizdeki insanları koruyabilirsiniz.



Eğér bařkalarıyla aynı cihazları kullanıyorsanız, bu konu ayrıca nemlidir.

Kelime listesi

Aşağıdaki liste, bu rehberde geçen **kalın** yazılmış sözcüklerin anlamlarını içerir.



Siber

Siber kelimesi, konunun internetle ilgili olduğu anlamına gelir.

Siber suç



Siber suçlar, suçluların interneti kullanarak işlediği suçlardır.

Örneğin, interneti kullanarak;

- kişisel bilgilerinizi çalabilir
- çevrim içi hesaplarınızı ele geçirebilirler.



Konum ayarları

Konum ayarları cihazınızın bulunduğu yeri gösterir.



Çok faktörlü kimlik doğrulama (MFA)

MFA, hesaplarınıza giriş yaparken her seferinde 2 veya daha fazla farklı yöntem kullanmanız demektir.



Parola

Parola daha güçlü bir şifre türüdür.

Başkalarının tahmin etmesi oldukça zordur.



Halka açık Wi-Fi

Halka açık Wi-Fi, halka açık alanlarda kullanabileceğiniz ücretsiz internet bağlantılarına denir.



Bir kişinin sizi:

- kandırmaya
- paranızı almaya çalışmasına

dolandırıcılık denir.



Dolandırıcı

Dolandırıcılık yapan kimseye dolandırıcı denir.

Bize ulaşın



Avustralya Siber Güvenlik Yardım Hattı'nı arayabilirsiniz.

1300 292 371



İnternet sitemizi ziyaret edebilirsiniz.

www.actnowstaysecure.gov.au



Siber suçları ReportCyber internet sitesi üzerinden ihbar edebilirsiniz.

www.cyber.gov.au/report



Information Access Group, bu Kolay Okunur belgeyi stok fotoğraflar ve özel görseller kullanarak oluşturmuştur. Görseller izin alınmadan yeniden kullanılamaz. Görsellerle ilgili sorularınız için bakınız:

www.informationaccessgroup.com. İş referans numarası: 6342.