



**Şimdi Harekete Geçin.
Güvende Kalın.**

actnowstaysecure.gov.au

Çevrimiçi olarak neleri riske atıyorsunuz?

Teknoloji hızla ilerledikçe ve çevrimiçi olarak daha fazla zaman geçirdikçe, Avustralyalılar siber saldırılara karşı savunmasız kalmaya devam ediyor.

Act Now. Stay Secure. (Hemen Harekete Geçin. Güvende Kalın.) kampanyası, Avustralyalıları çevrimiçi ortamda kendilerini korumaları için herkesin uygulayabileceği basit siber güvenlik önlemleri konusunda eğitmektedir.

Şimdi Harekete Geçin. Güvende Kalın.

Çevrimiçi ortamda nasıl güvende kalınır

Her hesabınızda özgün ve güçlü bir parola kullanın

Çevrimiçi hesaplarınızın her biri için özgün ve güçlü bir parola kullanmak, çevrimiçi ortamda güvende kalmak için atabileceğiniz en etkili adımlardan biridir.

Parola ifadesi, daha güvenli bir şifre türüdür. Bu, rastgele bir dizi sözcüklerden oluşur. Bunları sizin hatırlamanız daha kolaydır ancak siber suçluların tahmin etmesi daha zordur.

Parolanızın güçlü ve özgün olmasını sağlamak için şu öğeleri içerdiğinden emin olun:

- ✓ Dört veya daha fazla rastgele sözcük içersin
- ✓ en az 15 karakterden oluşsun
- ✓ her hesap için farklı olsun
- ✓ soyadı, doğum tarihi veya adres gibi kimik belirleyici bilgiler içermesin
- ✓ web sitesi veya platform tarafından gerekli kılınıyorsa sembol, büyük harf veya sayılar içersin.

Özgün parolalarınızı oluşturmak ve saklamak için bir parola yöneticisi kullanmayı dikkate alın.

Cihazlarınızı güvenliğini sağlamak için tüm yazılım güncellemelerini yükleyin

İnternete bağlı tüm cihazlarınıza (örneğin telefon, dizüstü bilgisayar veya akıllı saat) yazılım güncellemelerini düzenli olarak yüklemek, çevrim içi ortamda güvende kalmanız için kritik öneme sahiptir.

Yazılım güncellemeleri, cihazlarınızın güvenliğindeki zayıflıkları veya boşlukları giderir. Güncellemeleri düzenli olarak yüklemek cihazlarınızı güvende tutar ve siber suçluların bu cihazlara erişmesini zorlaştırır.

Otomatik güncellemeleri açık tutun ve güncelleme uyarısı aldığınızda bunları yüklediğinizden emin olun.

Her zaman çok faktörlü kimlik doğrulamayı açık tutun

Tüm çevrim içi hesaplarınıza ek bir güvenlik katmanı eklemek mümkünse, çok faktörlü kimlik doğrulamayı açın.

Çok faktörlü kimlik doğrulama, hesabınıza giriş yapabilmek için iki veya daha fazla doğrulama yöntemi gerektirir. Örneğin, şifrenizi veya parola ifadenizi girdikten sonra, bir doğrulama uygulaması, e-posta veya kısa mesaj yoluyla size gönderilen bir kodu girmeniz istenebilir.

Çok faktörlü kimlik doğrulama, diğer kimlik doğrulama yöntemlerinizden biri (örneğin bir parola ifadesi) ele geçirilse bile hesabınızı korumaya devam eder.



**Şimdi Harekete Geçin.
Güvende Kalın.**

actnowstaysecure.gov.au

Çevrimiçi ortamda güvende kalmanın başka yollarını mı arıyorsunuz?

Siber güvenliğinizi artırmanın daha fazla yolunu mu arıyorsunuz? Çevrimiçi ortamda kendinizi korumak için atabileceğiniz diğer bazı adımlar şöyledir.

Halka açık Wi-Fi kullanırken dikkatli olun

Halka açık Wi-Fi ağlarını kullanırken, bağlantı güvenli olmadığı için hassas veya kişisel bilgilerinize girmeyin. Buna sosyal medya hesapları, e-posta ya da çevrimiçi bankacılık işlemlerinizi dahildir. Girdiğiniz herhangi bir bilgi, siber suçlular tarafından ele geçirilebilir.

Gizlilik ve konum ayarlarınızı düzenli olarak kontrol edin ve güncelleyin

Kişisel veya kimliğinizi belirleyen bilgileri yanlışlıkla halkla paylaşmadığınızdan emin olmak için gizlilik ve konum ayarlarınızı sık sık kontrol etmeniz önemlidir.

Kontrol etmeniz gereken ayarlar arasında, sosyal medya hesaplarındaki gizlilik ayarları ve uygulamalarınız ile cihazlarındaki coğrafi konum izleme ayarları yer alır.

Aile ve arkadaşlarınız ile siber bakımdan güvende kalma hakkında konuşun

Eğitim ve farkındalık, hem sizin hem de aile ve arkadaşlarınızın çevrimiçi ortamda güvende kalması için kritik öneme sahiptir. Bu, özellikle internete bağlı cihazları ortak kullanmanız durumunda önemlidir. Bu konuyu çevrenizle konuşmak, siber güvenliği gündemde tutar ve onların çevrimiçi ortamda kendilerini nasıl koruyacakları konusunda en güncel bilgileri almalarını sağlar.

Dolandırıcılıkları nasıl tespit edeceğinizi öğrenin

Dolandırıcılar, insanları kandırarak onlardan para almaya veya kişisel bilgilerini elde etmeye çalışırlar.

Kiminle muhatap olduğunuzdan emin değilseniz, asla kimseye para ya da kişisel bilgi vermeyin. Kişi ya da kurumun kimliğini doğrulamak için, resmi bir web sitesi veya uygulamadan kendiniz bulacağınız iletişim bilgilerini kullanarak kontrol edin.

Siber saldırıları ve olayları bildirin

Dolandırıcılıkları veya siber olayları yetkililere bildirmek, hükümetin yeni eğilimleri belirlemesi, toplumu uyarması ve sizin karşılaştığınız siber saldırının etkilerinden kurtulmanıza destek olması açısından büyük önem taşır.

Kendinizi koruyacak basit adımları öğrenmek için bakınız actnowstaysecure.gov.au



**Şimdi Harekete Geçin.
Güvende Kalın.**

actnowstaysecure.gov.au