National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

# Çevrimiçi ortamda güvenliğinizi korumak

**Siber güvenlik benim için neden önemli?**

İnternet ve sosyal medya, bilgi paylaşmamıza ve arkadaşlarımızla ve ailemizle iletişimde kalmamıza yardımcı olan harika platformlardır.

Ancak suçlular ve diğer yasadışı örgütler de bunları paranızı, bilgilerinizi ele geçirmek veya sizi korkutmak için kullanırlar.

Bu kişiler dünyanın her yerinden faaliyet gösterebilirler, çoğu dili akıcı bir şekilde konuşabilirler ve ikna edici sahte web siteleri oluşturabilirler. E-posta, sosyal medya ve kısa mesaj yoluyla sizinle iletişime geçerler ve net düşünmenizi engellemek için sizi korkutmaya veya kaygılandırmaya çalışırlar.

Bütün bunlar, hazırlıklı olmanız ve onların kullandığı hilelerin her zaman farkında olmanız gerektiği anlamına gelir.

**Çevrimiçi ortamda karşılaşabileceğim bazı yaygın meseleler nelerdir?**

Bunlar gördüğümüz en yaygın durumlardan bazıları.

- Şüpheli bir e-posta veya kısa mesaj alırsınız ve sizden bir bağlantıya tıklamanızı ister.
    - Bu bağlantılar genellikle şifre veya finansal bilgilerinizi çalmak için tasarlanmış sahte web sitelerine yönlendirir.
- Kişisel bilgilerinizi isteyen şüpheli bir çağrı alırsınız.
    - Yukarıda belirtildiği gibi arayan kişi kendisini bankanızdanmış gibi tanıtacak ve sizden bilgi isteyecektir.
- Otorite sahibi biriymiş gibi davranan ve size bir şeyler yaptırmaya çalışan birinden iletişim alırsınız.
    - Genellikle bu kişi bir tür tehditte bulunur.
- Birisi çevrimiçi hesaplarınızdan bir veya daha fazlasına erişir (örneğin: e-posta veya sosyal medya).
    - Birisi çevrimiçi hesabınıza girerse bilgilerinizi çalabilir, ödemeleri yönlendirebilir ve potansiyel olarak sizmiş gibi davranarak arkadaşlarınızı veya ailenizi hedef alabilir.
- Kredi kartı bilgileriniz çalınır veya sahte bir satış veya yatırım ile paranız dolandırılır.
    - Dolandırıcılar, iyi bir alışveriş imkanı göreceğinizi ve düşünmeden ödeme yapmak isteyeceğinizi umarlar.  Ya da belki gerçek bir web sitesi bir veri ihlaline yakalanır ve bilgileriniz çevrimiçi olarak sızdırılır.

Burada bununla ilgili daha fazla senaryo bulabilirsiniz:
Şimdi yardım alın - Çevrimiçi Bilgilerinize Sahip Çıkın

**Çevrimiçi ortamda nasıl güvende kalırım?**

- Uzun ve benzersiz şifreler
    - Bir şifre ne kadar uzunsa o kadar güçlüdür.
    - Dört rastgele kelimeyi bir araya getirerek (örneğin: TriangleRhinoOperationShoes) ve gerekirse sayılar, büyük harfler ve semboller ekleyerek (örneğin: Triangle&"Rhino"Operation2Shoes) 16 karakterden uzun akılda kalıcı bir parola oluşturun.
    - Daha da önemlisi, şifrelerinizi tekrarlamayın. Bir suçlu şifrelerinizden birini ele geçirirse, bunu diğer hesaplarınızda da deneyecektir.
    - İyi şifreler oluşturun - Çevrimiçi Bilgilerinize Sahip Çıkın
- İki faktörlü kimlik doğrulamayı açın.
    - Bu, bir web sitesine giriş yapmak için gereken ekstra bir bilgidir; genellikle telefonunuza gönderilen bir koddur.
    - Bu yöntem inanılmaz derecede güçlüdür ve hesabınıza erişmeye yönelik girişimlerin çoğunu durdurabilir.
    - Desteklendiği takdirde bir 'kimlik doğrulama uygulaması' kullanmanızı öneririz.
    - İki faktörlü kimlik doğrulamayı (2FA) ayarlayın - Çevrimiçi Bilgilerinize Sahip Çıkın
- Çevrimiçi ortamda gizliliğinizi koruyun
    - Sosyal medyada güvende kalmak için en iyi seçenek gizlilik ayarlarınızı açık tutmaktır.
    - Bu, siber suçlular da dahil olmak üzere rastgele kişilerin paylaşımlarınızı görmesini veya size mesaj göndermesini engelleyecektir.
    - Çevrimiçi gizliliğinizi koruyun - Çevrimiçi Bilgilerinize Sahip Çıkın
- Her şeyi güncel tutun.
    - Telefonunuzu, bilgisayarınızı veya yazılımınızı güncellediğinizde, güvenlikte olabilecek açıkları da kapatmış olursunuz.
    - Suçlular sürekli olarak sisteme girmenin yollarını arıyorlar ve güncellemeler bu açıkları kapatıyor.
    - Güncellemelerinizi ihmal etmeyin - Çevrimiçi Bilgilerinize Sahip Çıkın
- Her zaman dikkatli olun
    - En iyi tavsiye, bu tür dolandırıcılıkların bilincinde olmanız ve suçluların sizinle herhangi bir çevrimiçi platformda iletişime geçmeye çalışması durumunda dikkatli olmanızdır.
    - Bir şeyler yanlış görünüyorsa, sizinle iletişime geçen kişiyle iletişim kurmayın. Özellikle arkadaşça görünseler bile para isterlerse dikkatli olun.

- Garip bağlantılar ve e-posta adreslerine dikkat edin (örneğin: bankanız size bir gmail hesabından e-posta göndermeyecektir).
- Şüpheniz varsa, doğrudan kuruluşla iletişime geçin ve size gönderilen hiçbir bağlantıyı veya telefon numarasını takip etmeyin.

**Dolandırılırsam veya daha kötü bir şey olursa ne yapmalıyım?**

Yardım için gidebileceğiniz birçok yer var. Bu kuruluşların tümü, siz onay vermedikçe bilgilerinizi başkalarıyla paylaşmazlar.

- Siber olayları CERT NZ portalı aracılığıyla NCSC'ye bildirebilirsiniz. Size yardımcı olabilir veya başka bir kurumla iletişime geçirebiliriz:
  Bir olayı bildirin | CERT NZ
- Paranızı kaybettiyseniz hemen bankanızla iletişime geçmelisiniz.
- Dolandırıcılık amaçlı telefon mesajları, İçişleri Bakanlığı tarafından yürütülen bir hizmet olan 7726'ya ücretsiz olarak iletilebilir.