Kuruluşunuzu çevrimiçi ortamda güvende tutmak

Siber güvenlik, toplumsal gruplar ve kuruluşlar için neden önemlidir?

Bu sayfada, topluluğunuzu, grubunuzu veya kuruluşunuzu siber güvenlik tehditlerinden korumak için alabileceğiniz tavsiyeler ve atabileceğiniz bazı adımlar yer almaktadır. Bireylerin kendilerini çevrimiçi ortamda güvende tutmaları için de ayrı bir kılavuz bulunmaktadır.

Bu tavsiyeler en yaygın ve ciddi tehditler baz alınarak hazırlanmıştır.

- Güncellemeler – güvenlikteki herhangi bir açığı kapatmak için cihazlarınızdaki yazılımı güncel tutun.
    - Topluluk grubunuzun veya kuruluşunuzun cihazlarını güncel tutun. Buna telefonlar, bilgisayarlar, WiFi yönlendiricileri ve akıllı cihazlar da dahil olmak üzere internete bağlanan diğer her şey dahildir.
    - Mümkün olduğunca otomatik güncellemeleri kullanın.
- İki faktörlü kimlik doğrulama (2FA) – bir şifre ve telefonunuzdaki bir uygulamadan gelen kod gibi bir adım daha isteyerek hesaplarınıza ekstra güvenlik ekler.
    - Not: Buna çok faktörlü kimlik doğrulama (MFA), iki adımlı doğrulama (2SV) ve daha birçok ad da verilmektedir.
    - Toplumsal grubunuzun veya kuruluşunuzun tüm hesaplarında 2FA'yı açın.
    - Mümkünse, kandırılıp vermenizin mümkün olmayacağı, kimlik avına dayanıklı bir 2FA biçimi kullanmayı deneyin. Bu fiziksel bir güvenlik anahtarı veya parmak izi ya da yüz kimliği gibi bir şey olabilir.
- Çevrimiçi hesaplarınızı takip edin; eski üyelerin topluluk grubundan veya organizasyondan ayrıldıktan sonra hesaplarına erişimlerini sürdürmediğinden emin olun.
    - Aynı hesaba birden fazla kişi erişiyorsa, hepsinin farklı oturum açma bilgilerine sahip olduğundan ve hepsinde 2FA'nın açık olduğundan emin olun.
    - Tüm kullanıcı hesaplarının bir listesini tutun ve personel ayrılması gibi durumlarda ihtiyaç duyulmayanları devre dışı bırakın.
    - Üyelerinize verdiğiniz tüm cihazların bir kaydını tutun ve söz konusu kişi organizasyondan ayrıldığında geri almayı ve fabrika ayarlarına döndürmeyi unutmayın. Ayrıca binaya erişim için fiziksel kodları değiştirmeniz gerekebilir.
- Çevrimiçi hesaplarınıza kimlerin erişebildiğini kontrol edin; topluluk grubunuzdaki veya kuruluşunuzdaki kişiler yalnızca ihtiyaç duydukları şeylere erişebilmelidir.
    - Bir kişinin hesabının hacklenmesi durumunda bu adımlar saldırganın verebileceği zararı sınırlar.
    - Gereksiz izinleri düzenli olarak kontrol edin ve kaldırın.

    - Birden fazla kişinin kullandığı tek bir "yönetici" hesabınız varsa, bu hesaptaki olağan dışı etkinlikleri kontrol edin. Özellikle günlük işler için bu tür hesaplara sahip olmayı sınırlandırmaya çalışın.
    - Bu kurallar, yönlendiriciler gibi cihazlara yönelik yönetici erişimi için de geçerlidir.
- Eğer sizin adınıza IT hizmetleri yürütecek birini işe aldıysanız, hizmet sağlayıcılarla yaptığınız sözleşmeleri gözden geçirin.
    - Topluluk grubunuzun veya kuruluşunuzun ihtiyaçlarını karşılamak için siber güvenlik korumalarının mevcut olduğundan emin olun.
- Tüm hesaplarınızın ve sistemlerinizin birlikte nasıl çalıştığını bilin; bağlantıları anlamak, bir saldırganın nereden içeri girebileceğini bilmenize yardımcı olur.
    - Sistemleriniz arasındaki bağlantıları (örneğin e-posta, bulut depolama ve muhasebe platformları) gözden geçirin.
    - Ekstra çevrimiçi güvenlik için Sanal Özel Ağ (VPN) kullanmayı düşünün. VPN kullanmak, çevrimiçi etkinliğinizi sizi takip etmeye çalışan herkesten gizler. Özellikle topluluk grubunuz veya organizasyonunuzdaki herhangi bir üyenin uzaktan bağlanması durumunda bu durum oldukça iyi bir seçenektir.
- İnsanlarınızın 'siber akıllı' olmasını sağlayın; toplum grubunuzdaki veya örgütünüzdeki insanların, sistemlerinizden daha fazla hedef alınma olasılığı vardır.
    - Tüm personeli temel siber güvenlik konusunda eğitin. Çevrimiçi Ortamınıza Sahip çıkın Çevrimiçi Ortamınıza Sahip Çıkın | NCSC web sitesi, çevrimiçi ortamda güvenliğinizi sağlamanıza ve dolandırıcılıkları tespit etmenize yardımcı olacak çok çeşitli tavsiyeler ve ipuçları sunar.
    - Onlara bunun hem kişisel hesapları hem de kuruluşunuz için kullandıkları hesaplar açısından önemli olduğunu hatırlatın.
    - Bireylerin çevrimiçi ortamda kendilerini güvende tutabilmeleri için de bir rehberimiz var.
- Olası bir olay için plan yapın – bir olay meydana geldiğinde insanların paniğe kapılmasını önlemek için bir müdahale planına sahip olmak önemlidir.
    - Olay müdahale planı, bir olay sırasında kimin ne yapacağını ana hatlarıyla belirtir. Şablonlar burada mevcuttur Olay Yönetimi | NCSC
    - Telefon, bilgisayar veya diğer sistemlerin arızalanması durumunda ne yapacağınıza dair bir plan ekleyin. Bu planı güncel tutun.
    - Gerekli herkesin iletişim bilgilerini saklayın ve onlarla iletişim kurmanın ana yolunun (e-posta gibi) bozulması durumları için yedekleyin.
    - Ulaşamamanız durumunda kullanmak üzere planı sisteminizin dışında bir yerde saklayın.