GÜVENLİ GÜNLER BÜLTENİ

Bilgisayar kullanıcılarına yönelik hazırlanır. Her ayın 15'i çıkar. Diğer sayılara erişmek ve sonraki mesajların direk posta kutunuza gelmesi için guvenligunler.com adresini ziyaret ediniz.

TEMMUZ 2019

***YILIN YORGUNLUĞUNU ATMAK**, kafanızı boşaltmak, rutin yaşamınıza kısa bir mola vermek ve enerji depolamak için aylardır beklediğiniz tatile çıkmanıza çok az kaldı. Ancak tam da bu noktada şunu unutmayın, siber saldırganlar tatil yapmaz.*

Bu nedenle tatil döneminde de güvenlikle ilgili tedbirleri elden bırakmamalı, hatta tatile çıkmadan, tatil sırasında ve sonrasında güvenliğe ilişkin ekstra kontroller yapmalısınız.

TATİLE GİTMEDEN ÖNCE

» **Paylaşımlara Dikkat**
Hırsızlara "Şu tarihler arasında evim boş olacak" der misiniz? Bu şekilde sorulduğunda hepinizin cevabı koca bir "HAYIR" tabii ki. Ancak farkında olmadan bunu yapıyor olabilirsiniz.

Sosyal medya üzerinden yaptığınız biletinize ya da rezervasyonunuza ait ekran görüntüsü gibi paylaşımlarla sadece tatile gideceğinizi değil, ne zaman ve nereye gideceğinizi de paylaşmış oluyorsunuz. Üstelik ne zaman evde olmayacağınızı da...

» **Yedeklerinizi Alın**
Veri kaybı yaşamamak için cihazlarınızdaki bilgilerin yedeklerini almak zaten düzenli olarak yapmanız gereken bir işlem. Ancak çalınma, fiziksel olarak zarar görme gibi

risklerin daha da arttığı tatil dönemi öncesinde mutlaka ve mutlaka yanınıza aldığınız telefon, dizüstü bilgisayar, tablet gibi cihazlarınızdaki bilgileri yedeklemelisiniz.

» **Güncel Antivirüs Yazılımı**
Tatilde ortak kablosuz ağlardan bulaşabilecek virüsler ya da internetinizin olmaması nedeniyle antivirüs programınızı güncelleyememe ihtimaline karşı tatile çıkmadan önce mutlaka antivirüs programınızı güncelleyin.

TATİL SIRASINDA

» **Kablosuz İnternete Bağlanma**
Günümüzde bir otele, restorana ya da kafeye girdiğimizde sorduğumuz ilk sorulardan biri "Kablosuz bağlantınız var mı?" olmaktadır. Özellikle birkaç gün kalacağımız otellerde çeşitli riskleri göz ardı ederek ortak ağlara bağlanıyoruz. Ancak bu işlemin yol açabileceği riskler vardır ve bunlardan bazıları şöyle sıralanabilir:

- Ağa bağlı diğer kişilerin ağ trafiğinize (yani gönderdiğiniz e-postaya, mesaja, kart bilgilerinize vb.) erişebilmesi
- Ağa bağlı diğer kişilerin cihazınıza erişebilmesi
- Cihazınızdaki hassas ve kişisel bilgilerin çalınması

Ortak kullanıma açık kablosuz ağlara bağlıyken herhangi bir satın alma işlemi yapmamanızı, bankacılık bilgilerini girdiğiniz uygulamalara erişmemenizi ve kuşkusuz şifrelerinizi ya da kimsenin bilmesini istemediğiniz diğer bilgileri göndermemenizi şiddetle tavsiye ederim.

» **Kiralık Araçla Kurulan Bağlantılar**
Tatil sırasında kiralamış olduğunuz araçlarda telefonunuzdan müzik dinlemek isteyebilirsiniz. Ancak bu masum istek sonucu, araçların USB ve Bluetooth eşleştirme özelliği ile telefon rehberi gibi kişisel bilgilerinizi fark etmeden paylaşmış da olabilirsiniz. Eğer kiralık araçlarda cihazlarınız ile böyle bir bağlantı kurarsanız, aracı teslim etmeden önce ayarlardan cihazınızı kaldırdığınızdan mutlaka emin olun.

» **Otomatik E-postalar**
Tatil sırasında gelen e-postaları, e-postalarınıza erişiminizin kısıtlı olduğunu ve insanların acil durumlar için kiminle iletişime geçmeleri gerektiğini söyleyen otomatik e-posta ile yanıtlıyor olabilirsiniz. Ne var ki bu aşamada tıpkı biletinizin ekran görüntüsünü paylaştığınız durumdaki gibi bir siber saldırının kurbanı haline gelebilirsiniz. Çünkü durumunuz hakkında verdiğiniz her bilgi, saldırganların elini güçlendirerek sizi bir sosyal mühendislik saldırısı ile karşı karşıya bırakabilir. Dolayısıyla, otomatik e-posta özelliğini aktifleştirirken bir kez daha düşünün. Kullanmanız gerekli ise, kurum içi – kurum dışı otomatik yanıtlarını ayırarak, alıcı profillerine göre içeriklerini belirleyin.

» **Konum Paylaşma**
Tatilcilerin bulundukları yerlerden konum paylaşımı yapmaları oldukça yaygındır. Bulunduğunuz yeri işaret ederek (tabii bu durumda bulunmadığınız yeri de) bir suçlunun otel odanızda ya da evinizde olmadığınızı saptamasını kolaylaştırabilir ve kişisel eşyalarınızı bu alanlarda fiziksel saldırılara açık hale getirebilirsiniz. Bu tehditlerden kaçınmak için bulunduğunuz yerle ilgili çevrimiçi yayınladığınız bilgileri sınırlandırın. Bu tip bildirimlerin sadece konum paylaşımı yapılan uygulamalar (örn. Swarm) üzerinden değil, amacı fotoğraf paylaşmak olan uygulamalarda (örn. Instagram) paylaştığınız görselin konum kısmını doldurarak da yapılabileceğini unutmayın.

TATİL DÖNÜŞÜ

» **Cihazlarınızı Tarayın**
Tatil dönüşü tüm cihazlarınızı güncel bir antivirüs yazılımı aracılığıyla taramadan geçirin.

» **Yazılım Güncellemelerini Kontrol Edin**
Tatil dönüşünde cihazlarınızdaki yazılımların güncelliğini kontrol edin ve yeni sürümleri varsa güncelleyin.

REFERANSLAR

» https://us.norton.com/internetsecurity-mobile-8-cyber-security-tips-for-business-travelers.html

» https://opendatasecurity.io/7-cyber-security-tips-for-holidays/

YAZAR HAKKINDA

MERVE ÇANKAYA EYİOL 2011 yılında Kocaeli Üniversitesi Bilgisayar Mühendisliği Bölümü'nden mezun olmuştur. Sakarya Üniversitesi bünyesinde İşletme Yüksek Lisans (MBA) derecesine sahip olup, yine aynı üniversitede Yönetim Bilişim Sistemleri (MIS) doktora programına devam etmektedir. Kardemir A.Ş.'de Sistem Analizi ve Denetimi Başmühendisi olarak IT süreç yönetimi, ISO 27001 Bilgi Güvenliği Yönetim Sistemi, kurumsal risk yönetimi ve IT uyum konularında çalışmalar yürütmektedir.

linkedin.com/in/merve-cankaya-eyiol/