

Evden Güvenli Çalışmanın 5 Önemli Adımı

Evden çalışmanın bazılarınız için yeni bir durum olabileceğini, hatta yeni ortamınıza alışmakta zorluk yaşayabileceğinizin farkındayız. Bir amacımız da evinizden mümkün olduğunca güvenli bir şekilde çalışabilmenize yardımcı olmaktır. Aşağıda, güvenli çalışmanın beş basit adımını göreceksiniz. Bunların en güzel tarafı, işinizi güvenceye almanın yanı sıra evinizde siber güvenlik sağlayarak hem sizi hem de ailenizi koruyacak olmasıdır.



Siz: En önemlisi şu ki, teknoloji tek başına sizi koruyamaz. En iyi savunma sizsiniz. Saldırganlar artık biliyorlar ki amaçlarına ulaşmanın en iyi yolu bilgisayarınızı ya da diğer cihazlarınızı değil, doğrudan sizi hedef almak. Parolanızı, işle ilgili verileri veya bilgisayarınızın kontrolünü ele geçirmek istediklerinde genellikle bir aciliyet hissi yaratıp sizi kandırarak bunları vermenizi sağlamaya çalışıyorlar. Örneğin

Microsoft teknik desteğinden arıyormuş gibi yapıp bilgisayarınıza virüs girdiğini söyleyebiliyorlar. Bir paketin teslim edilemediğini söyleyen bir e-posta göndererek tehlikeli bir bağlantıya tıklamanızı sağlayabiliyorlar. Bir sosyal mühendislik saldırısına işaret eden en genel belirtiler şunlardır:

- Saldırganın korku, göz dağı, kriz durumu veya zaman baskısı gibi inanılmaz bir acil durum hissi yaratmaya çalışması. Siber saldırgan banka, kamu kurumu veya uluslararası kuruluşlar gibi güvenilir kurumlardan geliyormuş gibi görünen ikna edici mesajlar oluşturabilirler.
- Güvenlik politikala veya prosedürlerini göz ardı etmeniz için baskı kurarlar veya gerçek olamayacak kadar iyi tekliflerde bulunurlar (bir çekilişi kazanmanız gibi).
- Bir arkadaşınızdan veya iş arkadaşınızdan geliyormuş gibi görünen ama üslubunda veya dilinde bir gariplik olan mesajlar gönderirler.

Nihayetinde bu saldırılara karşı en iyi savunma sizsiniz.

2 Home Network

EvAğı: Neredeyse tüm ev ağları, kablosuz (genellikle Wi-Fi denir) bir ağı dayandır. Bu, cihazlarınızın İnternet'e kablosuz bağlanmasını mümkün kılan sistemdir. Çoğu evin kablosuz ağı, modemle veya ayrı bir kablosuz erişim noktasıyla kontrol edilir. Bunların ikisi de aynı şekilde, ev cihazlarının bağlandığı kablosuz sinyaller yayarak çalışır. Yani kablosuz ağınıza güvenceye almak, evinizi güvenceye almanın önemli bir parçasıdır. Bunun için aşağıdaki tedbirleri almanızı öneririz:

- Kablosuz ağınıza kontrol eden cihazın varsayılan yönetici parolasını değiştirin. Yönetici hesabı, kablosuz ağınıza ayarlarını yapılandırabilmenizi sağlayan hesaptır.
- Sadece güvendiğiniz kişilerin, ev ağına bağlanabildiğinden emin olun. Güçlü bir güvenlik oluşturarak bunu sağlayabilirsiniz. Güçlü bir ağ güvenliği oluşturduğunuzda, kablosuz ağına bağlanmak için bir parola kullanılması gerekecektir ve ağ üzerinden yapılan çevrim içi faaliyetler şifrelenecektir.
- Kablosuz ağına bağlanmak için kullanılan parolanın güçlü bir parola olduğundan ve yönetici parolasından farklı olduğundan emin olun. Unutmayın, cihazlar parolayı kaydedip hatırlayacaktır ve bu nedenle her cihaz için parolayı sadece bir defa girmeniz yeterli olacaktır.

Bu işlemleri nasıl yapacağınızdan emin değil misiniz? İnternet Hizmet Sağlayıcınıza sorun, web sitesini ziyaret edin, kablosuz erişim noktanızla birlikte gelen belgeleri okuyun ya da satıcının web sitesini inceleyin.

3 Passwords

Parolalar: Bir site sizden parola oluşturmanızı isterse güçlü bir parola oluşturun. Parolada ne kadar çok karakter varsa o kadar güçlü olacaktır. Güçlü bir parola oluşturmanın en basit yolu bir kelime grubu kullanmaktır. Kelime grupları, "arı ballı viski" gibi birden fazla kelimeden oluşur. Parola olarak benzersiz bir kelime grubu kullanmak, her cihaz veya hesap için farklı bir kelime grubu kullanmaktır. Bu sayede, bunlardan biri ele geçirilse bile diğerleri güvende olacaktır. Her parolanızı hatırlayamıyor musunuz?

Tüm parolalarınızı şifrelenmiş bir biçimde saklayan (ve daha birçok önemli özelliği olan) bir parola yöneticisi kullanın. Son olarak, mümkünse iki adımlı (veya iki faktörlü ya da çok faktörlü) doğrulamayı etkinleştirin. Bu özellik, parolanızın yanı sıra cep telefonunuza gönderilecek veya bir uygulama tarafından oluşturulacak bir kodu kullanmanızı gerektirerek ilave bir güvenlik katmanı ekler.

İki adımlı doğrulama, muhtemelen çevrim içi hesaplarınızı korumak için atabileceğiniz en önemli adımdır ve sandığınızdan çok daha kolaydır.



Güncellemeler: Tüm bilgisayarlarınızın, mobil cihazlarınızın, programlarınızın ve uygulamalarınızın son sürümüne güncellenmiş olduğundan emin olun. Siber saldırganlar, sürekli olarak cihazlarınızın kullandığı yazılımlarda yeni açıklar aramaktadır. Bu açıkları bulduklarında bunlardan faydalanmak ve cihazlarınızı ele geçirmek için özel programlar kullanırlar. Aynı şekilde, bu cihazların yazılımlarını yapan şirketler de güncellemeler yayınlayarak bu açıkları kapatmaktadır. Bu güncellemeleri bilgisayar ve mobil cihazlarınıza en kısa sürede yükleyerek bu cihazlarınızın güvenliğini güçlendirmiş olursunuz. Cihazlarınızı daima güncel tutmak için varsa otomatik güncellemeleri etkinleştirin. Bu, iş cihazlarınızın yanı sıra İnternet'e bağlanan televizyonlar, bebek monitörleri, güvenlik kameraları, ev modemleri, oyun konsolları ve hatta arabanız gibi ağa bağlı olan neredeyse her teknoloji için de geçerlidir.



Çocuklar / Misafirler: Ofisteyken çocukların, misafirlerin veya diğer aile üyelerinin iş bilgisayarınızı veya diğer iş cihazlarınızı kullanması gibi bir derdiniz yoktur. Aileniz veya arkadaşlarınızın yanlışlıkla cihazdaki bilgileri silmeleri, değiştirmeleri ve hatta cihaza virüs bulaştırmaları mümkündür. Bu nedenle, iş cihazlarınızı kullanmamaları gerektiğini onlara mutlaka anlatın.