Herkes İçin Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

Parolalar

Giriş

Parolalarınızı her gün, e-posta hesabınıza erişmekten çevrimiçi bankacılığa kadar, e-ticaretten akıllı telefonunuza erişmeye kadar bir çok noktada kullanırsınız. Oysa, parolalarınız sizin en zayıf noktalarınızdan biridir : birisi parolanızı öğrenirse ya da tahmin edebilirse hesaplarınıza sizin yerinize girebilir, kimliğinizi çalabilir, paranızı transfer edebilir, e-postalarınızı okuyabilir veya kişisel bilgilerinize erişebilir. İşte bu nedenle güçlü parolalar, kendinizi korumanız için önemli ve gereklidir. Bu sayıda, kolay hatırlanabilir güçlü parolaların nasıl oluşturulabileceğini öğreneceksiniz.

Konuk Yazar

My-Ngoc Nguyen (Me-Nop Wynn şeklinde okunuyor) sertifikalı SANS eğitmeni ve Secured IT Solutions şirketinde CEO/Baş Danışmandır. Sertifikasyonları ve 14+ yıldır farklı endüstrilerde ve sektörlerde siber güvenlik programları geliştirme, iyileştirme ve yönetme tecrübesi bulunmaktadır. Twitter: **@MenopN** LinkedIn: My-Ngoc "Menop" Nguyen.

Parolalar

Siber saldırganların, parolaları tahmin etmek veya “brute force (kaba kuvvet)” saldırıları yaparak ele geçirmek için geliştirdiği karmaşık metodların zorluğuyla karşı karşıyayız. Bu şu demektir; parolalarınız eğer güçlü değilse veya kolay tahmin edilebiliyorsa, saldırganlar tarafından ele geçirilebilir. Kendinizi bu sonuçtan korumanın önemli adımlarından birisi, güçlü parolalar kullanmaktır. Ancak, uzun ve karmaşık parolaları hatırlamak zor olabilir. Böyle bir durumda size, rastgele kelimelerden oluşan basit cümlelerden oluşan parolaları kullanmanızı öneriyoruz. Parolanız ne kadar fazla karakter içeriyorsa, parolanız o kadar güçlü olacaktır. Bu durumun avantajı sizin için kolay hatırlanabilecek bu parolaların siber saldırganlar tarafından ele geçirilmesinin zorlaşmasıdır. İşte size iki farklı örnek;

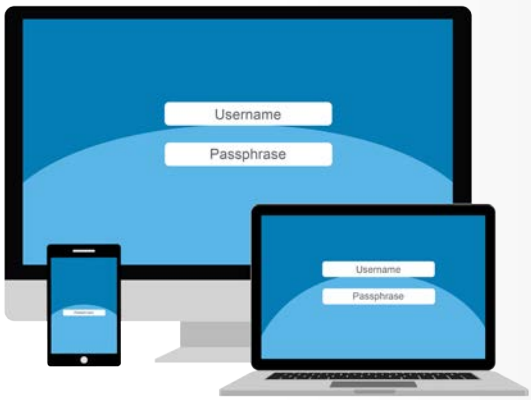
Sürdürmek-Kolaylık-Yasaklamak
Çay Saati 1:23

Örnekteki parolaları güçlü yapan birçok karakterden oluşmalarının yanı sıra büyük harf, küçük harf, sayı ve özel karakterler kullanılmış olmasıdır (boşluklar ve noktalama işaretleri de özel karakterdir). Aynı zamanda bu parolaları hatırlaması ve yazması da kolaydır. Parolalarınızı daha da güçlü yapmak isterseniz ‘a’ harfi yerine ‘@’, ‘o’ harfi yerine sıfır (0) rakamı kullanılması gibi harf yerine sayı veya özel karakterler de kullanabilirsiniz. Ayrıca, eğer bir web sitesinde veya yazılımda parola karakter sayısı için bir sınırlandırma varsa, izin verilen maksimum parola karakter sayısını kullanınız.

Parolalar

Parola Güvenliği

Parola kullanırken dikkatli olmalısınız. Art niyetli kişiler, kullandığınız parolayı kolayca ele geçirebilir veya kopyalayabilir durumdaysa parola kullanmanın bir yararı olmayacaktır.



Cümleler şeklinde oluşturacağınız parolalar, güçlü parola oluşturma ve hatırlamanın kolay yoludur.

1. Her cihazınız veya hesabınız için farklı parolalar kullandığınızdan emin olun. Örneğin, işte veya banka hesabınızda kullandığınız parolayı Facebook, Youtube veya Twitter gibi kişisel hesaplarınızda kullanmayın. Böylece, eğer bir hesabınız ele geçirilirse diğer hesaplarınız güvende olacaktır. Hatırlamanız gereken çok fazla parola varsa -ki bu çok yaygındır-, parola yönetim programı kullanmayı düşünebilirsiniz. Parola yönetim programı, bütün parolalarınızı güvenli bir şekilde saklayan özel bir programdır. Bu yolla hatırlamanız gereken parolalar sadece bilgisayarınızın ve parola yönetim programınızınki olacaktır.
2. Kullandığınız herhangi bir parolayı veya parola oluştururken kullandığınız stratejiyi iş arkadaşlarınız dahil kimseyle paylaşmayın. Parolanın kişiye özel olduğunu ve bu özel bilginin birisi tarafından bilinmesi durumunda daha fazla güvende olmayacağını unutmayın. Parola, eğer istemeyerek paylaşıldıysa veya ele geçirildiğine inanılıyorsa, hızlı bir şekilde değiştirilmelidir. Bunun tek istisnası, acil bir durumda kullanılmak üzere kişisel hesaplarınıza ait parolalarınızı çok güvendiğiniz bir aile üyesiyle paylaşmanız olabilir. Bu konuda bir yaklaşım kişisel parolalarınızın (iş hesaplarınızla ilgili olmadığından emin olarak) yazmak ve güvenli bir lokasyonda muhafaza etmek ve güvendiğiniz aile üyeniz ile o lokasyonu paylaşmak olabilir. Böylece size bir şey olursa veya acil bir durumda kalırsanız, sevdikleriniz sizce kritik olan kişisel hesaplarınıza erişebilir.
3. Otel, kütüphane gibi yerlerde bulunan genel kullanıma açık bilgisayarlarda iş veya banka hesabınızla ilgili herhangi bir işlem yapmayın. Çünkü bu bilgisayarlar herkes tarafından kullanabilir ve klavye hareketlerinizi kaydeden zararlı yazılımlar bulaşmış olabilir. İş veya banka hesaplarınızla ilgili işlemleri sadece güvenilir bilgisayar ve mobil cihazlar üzerinden yapın.
4. Güvenlik sorularına cevap vermeniz gereken internet sitelerinde dikkatli olun. Bu sorular kullandığınız parolayı unuttuğunuzda ve sıfırlamak istediğinizde kullanılır. Problem, bu soruların cevaplarının internet üzerinde veya sizin Facebook sayfanızda bulunabilme ihtimalinden kaynaklanmaktadır. Bu sorulara cevap verirken, cevapların genele açık ortamda kolayca bulunmadığından veya sizin oluşturduğunuz hayali bir bilgi olduğundan emin olun. Güvenlik sorularının cevaplarını hatırlayamıyor musunuz ? Bir film karakteri seçebilir ve yanıtlarınızı bu karakter üzerinden oluşturabilirsiniz mesela. Başka bir seçenek de parola yönetim programları kullanmak olabilir, zira birçoğu bu tarz ek bilgilerin saklanmasında da yardımcı olabilir.

Parolalar

5. Birçok çevrimiçi hesap iki adımlı doğrulama olarak da bilinen iki faktörlü doğrulama seçeneği sunar. Bu seçenek ile oturum açabilmeniz için parola kullanmanızın yanı sıra telefonunuza gönderilen kod gibi ek bir bileşene daha ihtiyacınız vardır. İki faktörlü doğrulama seçeneği, parolanın tek başına kullanımından çok daha güvenlidir. Mümkün olan her durumda bu seçeneği aktif hale getirin ve daha güçlü doğrulama/yetkilendirme kullanın.
6. Mobil cihazlar, güvenlik için genelde PIN kullanır. PIN'in de bir parola olduğunu unutmayın. Kullandığınız PIN ne kadar uzunsa, o kadar güvenlidir. Ayrıca, birçok mobil cihaz, PIN yerine parola kullanımına ya da parmak izi gibi biometrik doğrulamaya da izin vermektedir.
7. Son olarak, bir hesabı artık kullanmayacaksınız, kapattığınızdan, sildiğinizden veya pasif hale getirdiğinizden emin olun.

Daha Fazla Bilgi İçin

Aylık OUCH! güvenlik farkındalığı bültenine üye olun, OUCH! arşivlerine erişin ve securingthehuman.sans.org/ouch/archives adresini ziyaret ederek SANS güvenlik farkındalığı çözümleri hakkında daha fazla bilgi edinin.

Türkçe Çevirisi

Selma Süloğlu, ODTÜ Bilgisayar Mühendisliğinde doktorasını tamamlamış olup SOSoft Bilişim Teknolojilerinde biyometrik güvenlik sistemleri üzerinde çalışmaktadır.

Sema Yüce (https://tr.linkedin.com/in/semayuce), Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, finans, telekomünikasyon, sigortacılık, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, uyum, BT yönetişim/strateji, risk yönetimi, iş sürekliliği, hizmet yönetimi, altyapı hizmetleri, yazılım geliştirme ve program/proje yönetimi alanlarında yönetici ve danışman olarak 19 yılı aşkın süre görev yapmış olup, Nisan 2016 itibarıyla Trust ISC (www.trustisc.com) adıyla uzmanlık alanlarında hizmet vermekte olduğu kendi danışmanlık şirketini kurmuştur.

Kaynaklar

Parola Yönetim Programları: https://securingthehuman.sans.org/ouch/2015#october2015

İki Adımlı Doğrulama: https://securingthehuman.sans.org/ouch/2015#september2015

Girişinizi Kapatın: https://lockdownyourlogin.com

SANS SEC301 – Siber güvenliğe giriş eğitimi (5 gün): https://sans.org/sec301

Yayın Kurulu : Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley