Bilgisayar Kullanıcıları için Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...



# Parolalar

## Giriş

Parolaları her gün, e-posta hesabınıza erişmekten çevrimiçi bankacılığa kadar, çevrimiçi alışverişten akıllı telefonunuza erişmeye kadar bir çok noktada kullanırsınız. Oysa, parolalar sizin en zayıf noktalarınızdan biridir. Birisi sizin parolanızı öğrenirse kimliğinizi çalabilir, paranızı transfer edebilir veya kişisel bilgilerinize erişebilir. Güçlü parolalar, kendinizi korumanız için önemli ve gereklidir. Bu sayıda, kolay hatırlanabilir güçlü parolaların nasıl oluşturulabileceğini öğreneceksiniz.


## Konuk Yazar

Guy Bruneau, IPSS Inc. bünyesinde kıdemli güvenlik danışmanı, SANS eğitmeni ve ISC sorumlusudur. Guy, daha önce 'SANS Cyber Guardian' programından sorumluydu ve şu anda SANS GSE (GIAC Security Expert) üzerinde çalışmaktadır. Guy'ı, Twitter'da **@GuyBruneau** hesabından ve **handlers.sans.org/gbruneau** ağ sayfasından takip edebilirsiniz.


## Parolalar

Siber saldırganların, parolaları tahmin etmek veya "brute force (kaba kuvvet)" saldırıları yapmak için geliştirdiği karmaşık metodların zorluğuyla karşı karşıyayız, ve saldırganlar gün geçtikte sürekli olarak bu konuda daha iyi olmakta. Bu şu demektir; parolalarınız eğer güçsüzse veya kolay tahmin edilebilir durumdaysa saldırganlar tarafından ele geçirilebilir. Kendinizi bu durumdan korumanın önemli adımlarından birisi, güçlü parolaların kullanılmasıdır. Parolanız ne kadar fazla karakter içeriyorsa, parolanız o kadar güçlü ve zor tahmin edilebilir. Ancak, uzun ve karmaşık parolaları hatırlamak zor olabilir. Böyle bir durumda size, basit tümcecik veya kolay hatırlanan fakat zor ele geçirilen cümlelerden oluşan parolaları kullanmanızı öneriyoruz. İşte bir örnek;

*Kral Julian nerede?*

Örnekteki parolayı güçlü yapan 19 karakter olmasının yanı sıra büyük harf ve özel karakter kullanılmış olmasıdır (boşluklar ve noktalama işaretleri de özel karakterdir). 'a' harfi yerine '@', 'o' harfi yerine sıfır (0) rakamı kullanılması gibi harf yerine sayı veya özel karakter kullanımı, parolayı daha güçlü hale getirecektir. Ayrıca, eğer bir ağ sitesinde veya yazılımda parola karakter sayısı için bir sınırlandırma varsa, izin verilen maksimum parola karakter sayısını kullanınız.

## Parola güvenliği

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

# Parolalar

1. Her cihazınız veya hesabınız için farklı parolalar kullandığınızdan emin olun. Örneğin, işte veya banka hesabınızda kullandığınız parolayı Facebook, Youtube veya Twitter gibi özel 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.


*Parola kullanımı kimliğinizi ve bilgilerinizi korumak için en etkili adımlardan birisidir.*

3. Kolay tahmin edilebilir ve sık kullanılan parola kullanmaktan kaçının. Örneğin, “Sakla samanı gelir zamanı” yaygın bilinen bir deyim olduğundan iyi bir parola değildir.

4. 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.

5. Kişisel sorulara 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 bulunabilmesi durumundan kaynaklanmaktadır. Bu sorulara cevap verirken, cevapların genele açık ortamda kolayca bulunmadığından veya sizin oluşturduğunuz hayali bir bilgi olduğundan emin olun. Parola yönetim programları, bu bilgilerin saklanmasında da yardımcı olabilir.

6. 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 artı bir şeye daha ihtiyacınız vardır. İki faktörlü doğrulama seçeneği, yalnızca parola kullanımından daha güvenlidir. Mümkünse, her zaman bu seçenek kullanılmalıdır.

## Parolalar

7. 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 izin vermektedir.

8. 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 http://www.securingthehuman.org 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, Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, telekomünikasyon, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, iş sürekliliği, risk yönetimi, altyapı hizmetleri, yazılım geliştirme ve proje yönetimi alanlarında yönetici ve danışman olarak 15 yılı aşkın süredir görev yapmaktadır.

Mustafa Emrah Ünsür, Güvenlik Araştırmacısı olarak araştırmaları, makaleleri ve çevirileri vardır. Beyaz Şapkalı Hacker olarak kendisi tarafından kodlanan ve kodlanmakta olan 'exploit'ler ve 'tool'lar bulunmaktadır. Ayrıca, Sızma Testi Uzmanı olarak özel şirketlere ve devlet kurumlarına Zafiyet ve Sızma Testi yapmış ve yapmaya devam etmektedir.

## Kaynaklar

| | |
|---|---|
| İki aşamalı doğrulama: | http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201308_tr.pdf |
| Şifre yöneticileri: | http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_tr.pdf |
| Sosyal Mühendislik: | http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_tr.pdf |
| Common Security Terms: | http://www.securingthehuman.org/ouch/2014#december2014 |
| Verizon DBIR 2014: | http://www.securingthehuman.org/resources/security-terms |



Yayın Kurulu : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis