

Saldırıya Uğramış (Hacked) Hesaplar Güvenlik Önerileri

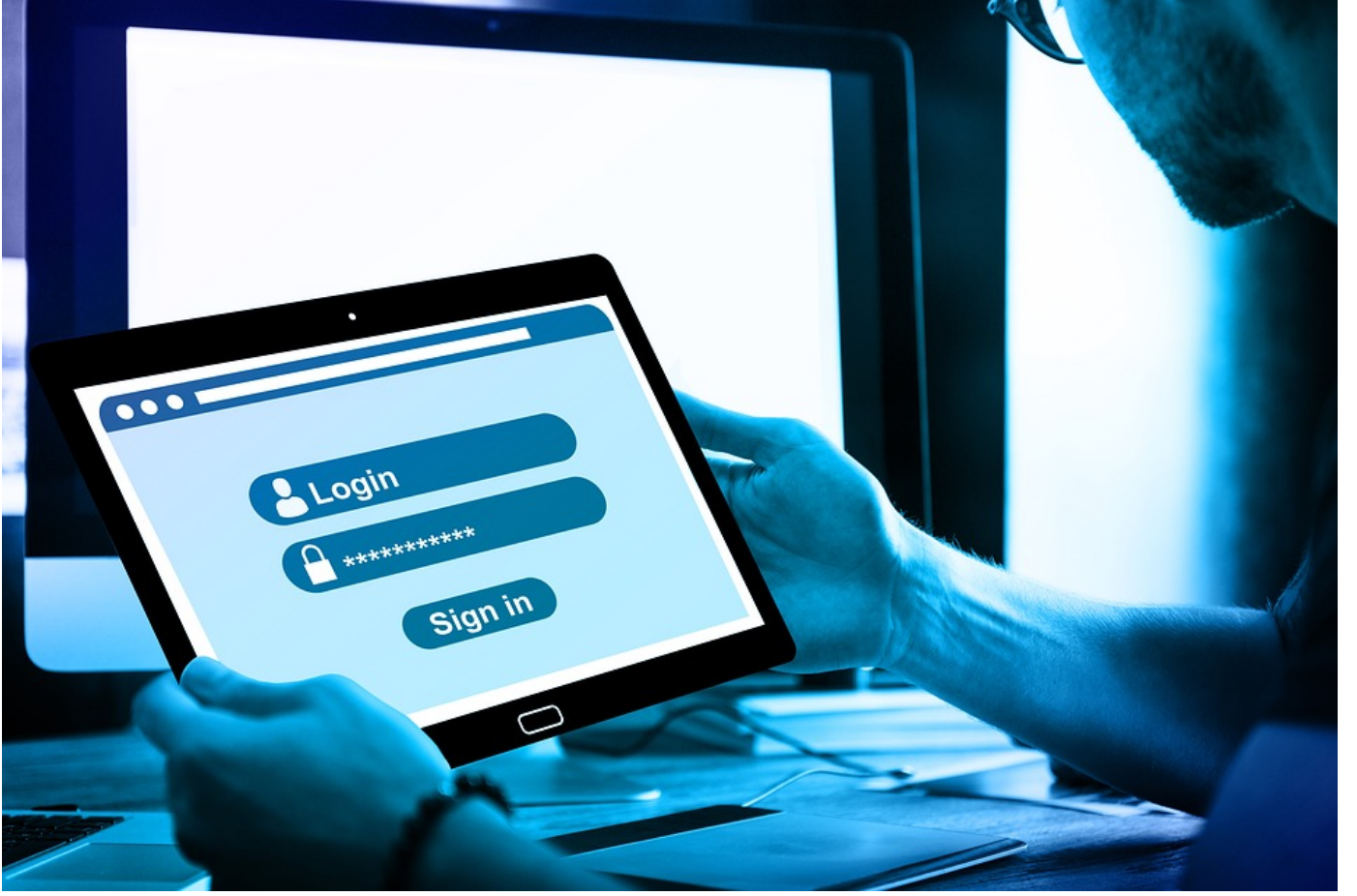
Eğer bir sosyal ağ, e-posta veya benzeri bir internet hesabınız tehlike altındaysa veya hacklendiyse, bu durumla başa çıkabilmeniz için bazı yolları bulunmaktadır.



Günümüzde sıkça karşılaşılan bir sorun olan e-posta hesaplarının ve sosyal medya hesaplarının güvenliğini sağlamak, kullanıcıların ve güvenlik şirketlerinin daima üzerinde durması gereken bir konu olarak karşımıza çıkmaktadır. E-posta hesabının ele geçirilmesi aynı zamanda e-posta hesabına bağlı sosyal medya hesaplarının da ele geçirilmesi anlamına gelebileceğinden olay domino etkisi yararmaktadır. Bu konuda şirketlerin üstüne büyük bir yük düşmekte ancak son kullanıcıların da yapabileceği şeyler bulunmaktadır.

- Giriş şifresinin ne kadar güvenli olduğunun kontrol edilmesi gerekmektedir. Birçok internet sitesi şifre oluşturma adımında oluşturulan şifrenin ne kadar güvenli olduğunu belirtir. Hatta bazıları belirli karakterleri içermeyen ve belirli bir düzen içine olmayan şifreleri kabul etmez ve kullanıcıyı bu şifreleri değiştirmeye zorlar. Bu konuda belirli bir şifrenin ne kadar sürede kırılabilirliğini söyleyen howsecureismypassword.net internet sitesinden fikir edinilebilir. Örneği; "Trncyd!" olarak belirlenen bir kullanıcı şifresi karışık ve zor kırılacak bir şifre gibi gelebilir, ancak ilgili sitede bu şifrenin 3 dakikada kırılabilirliği belirtilmektedir. Burada önemli olan hem uzun hem de değişik karakterler içeren şifre kullanmaktır.
- Şifrenin en popüler şifreler arasında olmamasına dikkat edilmelidir. Yapılan bir araştırmaya göre en çok kullanılan 5 şifre şöyledir:
 - "password"
 - "123456789"
 - "12345678"
 - "12345"
 - "111111"
- E-posta adresine iki adımlı doğrulamayı eklemek önemlidir. Bir şifre zayıf olduğu için ele geçirilebilse de saldırganın iki adımlı doğrulama şifresini ele geçirebilmesi için cep telefonuna, bilgisayara ya da tablete doğrudan ihtiyacı vardır. E-posta hesabınıza erişmek için iki adımlı

doğrulama eklemek, oturum açma işlemine sadece birkaç saniye geciktirir.



- Kullanıcının, sosyal medya hesaplarının erişim kayıtlarını incelemesinde fayda vardır. Diğer bir deyişle erişim kayıtlarının, sosyal medya hesabı giriş kayıtlarıyla tutarlı olup olmadığı kontrol edilmelidir. Öyle ki; çoğu banka uygulaması sisteme en son ne zaman giriş yapıldığını kullanıcılara girişte söylemektedir. Eğer yabancı bir IP adresi ile karşılaşırsa, kullanılan şifre hemen değiştirilmelidir.
- Sadece bilgisayara değil cep telefonu veya tablete de güçlü şifreler eklenmelidir. Giriş deseni uygulamasını destekleyen cihazlarda, desenin karışık olmasına dikkat edilmelidir. Çoğu kullanıcı, cihazını hemen açmak için karışık olmayan şifreler koyar. Eğer telefon veya tablet destekliyorsa, parmak izi okuyucuyu kullanmak iyi bir güvenlik önlemi sayılabilir.
- Okul ya da kütüphane gibi herkese açık yerlerde yer alan bilgisayarlardan kişisel hesaba erişmekten kaçınılması gerekmektedir. Bu bilgisayarlarda şifre saklayan keylogger programı yüklü olabilir. Eğer kişisel hesaba girilmesi zorunluysa mümkün olan en kısa süre içinde şifrenin değiştirilmesi gerekmektedir.
- İşyerinde ya da alışveriş yapılan internet sitesinde kullanılan şifre ile sosyal medya hesabında kullanılan şifre aynı hatta benzer olmamalıdır. Her teknoloji firması üyelerinin şifrelerini aynı güvenlik seviyesinde korumaz ve eğer saldırgan bir şifreyi ele geçirirse, bu şifreyi diğer tüm hesaplarınızda dener. Birçok şifreyi akılda tutmanın zor olduğunu düşünülürse, bir şifre yöneticisi programı kullanılabilir.
- E-postalardaki bağlantılar, sosyal medya hesaplarındaki tweetler, kısa mesajların içindeki linkler ve çevrimiçi reklamlar siber suçluların bilgisayarları ve sosyal medya hesaplarını ele geçirmek için sıkça kullandığı araçlardır. Kaynağı bilinse dahi, şüpheli bir şey görüldüğünde, yapabilecek en iyi şey o içeriği açmadan silmektir.
- Sosyal medya hesabının tehlike altında olduğunu düşünen kişi ilgili firmayla aşağıda verilen örnekler doğrultusunda iletişime geçebilir:

Facebook hesabı tehlike altındaysa;

<https://www.facebook.com/help/131719720300233>

G-mail hesabını tehlike altındaysa;

https://support.google.com/mail/troubleshooter/2402620?cbid=1uslv13hx7tyw&src=cb&lev=answer&hl=tr&visit_id=1-636337388742739292-1430258302&rd=2

Twitter hesabı tehlike altındaysa;

<https://help.twitter.com/tr>

Microsoft hesabı tehlike altındaysa;

<https://support.microsoft.com/tr-tr/help/10494/microsoft-account-get-back-compromised-account>
<https://support.microsoft.com/tr-tr/help/13956/microsoft-account-temporarily-suspended>

Ayrıca Instagram, Periscope, Youtube, Whatapp, Snappchat, Google Plus, Tumblr ile ilgili bilgilere aşağıdaki linkten ulaşılabilir.

<https://www.guvenliweb.org.tr/sosyal-medya-rehberi>

ETİKETLER

[#SaldırıyaUğramışHesaplar](#) [#Hacked](#) [#Güvenlik](#) [#Önerileri](#)

KAYNAKÇA

- [1] <https://gizmodo.com/the-25-most-popular-passwords-of-2018-will-make-you-fee-1831052705>
- [2] <https://www.complex.com/life/2018/11/how-to-avoid-getting-hacked/encryption-software>