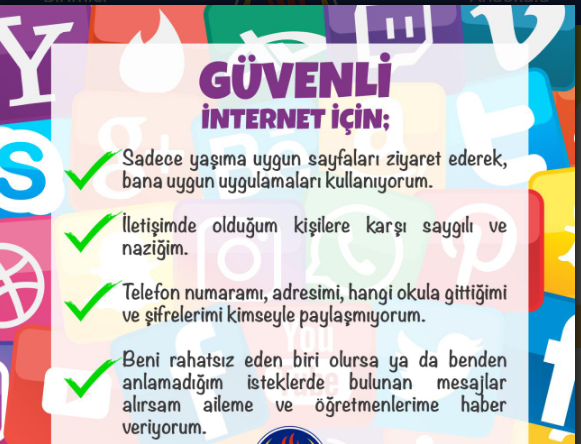
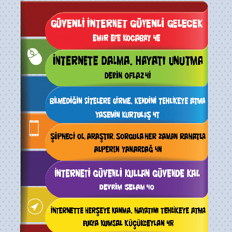
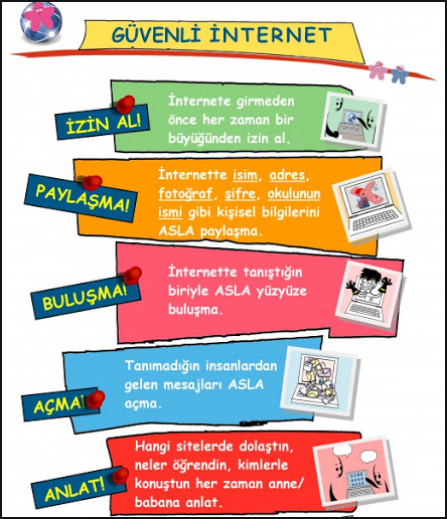
**e-Güvenlik Dokümanları**













.

[**BİLGİSAYAR GÜVENLİĞİ.**](http://sehitturkmentekinaihl.meb.k12.tr/meb_iys_dosyalar/48/02/762342/dosyalar/2020_01/28191007_Bilgisayar_GuvenliYi-1_v2.pdf)

**[](https://www.bilimnettasarim.com/wp-content/uploads/2014/03/computer-security.jpg)**

**Bilgisayar güvenliği, elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür. Bunun sağlanması için duruma uygun güvenlik politikasının belirlenmesi ve uygulanması gereklidir.**

**Bu politikalar;**

* **Etkinliklerin sorgulanması**
* **Erişimlerin izlenmesi**
* **Değişikliklerin kayıtlarının tutulup değerlendirilmesi**
* **Silme işlemlerinin sınırlandırılması**

**gibi bazı kullanım şekillerine indirgenebilmektedir.**

**Bilgisayar teknolojilerinde yer alan bilgisayar güvenliğinin amacı ise: “Kişi ve kurumların bu teknolojilerini kullanırken karşılaşabilecekleri tehdit ve tehlikelerin incelemelerinin yapılarak gerekli önlemlerin önceden alınmasıdır”. Bilgi ve bilgisayar güvenliği daha genel anlamda, güvenlik konularını detaylı olarak ele alan “güvenlik mühendisliği”nin bir alt alanı olarak görülmektedir.**

[**İNTERNETTE NELER YAPABİLİRİZ? GÜVENDE MİYİZ? İÇİN**](http://sehitturkmentekinaihl.meb.k12.tr/icerikler/%20http:/sehitturkmentekinaihl.meb.k12.tr/meb_iys_dosyalar/48/02/762342/dosyalar/2020_01/28191118_Ynternette_neler_yapabiliriz-guvende_miyiz_v2.pdf)

**İnternette güvenli olmanın yolları**



**İnternet güvenliği neden önemli?**

Bilgisayarımızda tuttuğumuz bilgilerin yüzde 100 güvende olduğunu varsaymak ne kadar yanlışsa, email hesaplarımızı ya da bulut teknolojisi kullanarak sakladığımız fotoğrafları daha güvenli kılamayacağımızı düşünmek de o kadar yanlıştır.

**Bulutta bir şey saklamadığımdan eminim**

Son günlerde özel fotoğrafları çalınıp da haber konusu olan ünlülerin çoğu da böyle düşünüyor olmalıydı. Fakat bulut hizmetleri yaygınlık kazandıkça akıllı telefon türü cihazların fabrika ayarları, kullanıcı bilgilerinin uzak depolarda saklanmasına göre düzenlenmiştir. Fotoğraflarınızın başkalarının eline geçmesini istemiyorsanız, telefon ayarlarınızı ve ne tür bilgilerin otomatik olarak buluta aktarıldığını kontrol ederek otomatik yüklemeyi devre dışı bırakabilirsiniz.



Bulutun yine de ne kadar yararlı olduğunu telefonu kaybolan ya da bozulanlar teyit edecektir. Neyse ki bulutta da güvenliği sağlamanın yolları var. Her şeyden önce güvenli bir şifre belirlemeniz gerekir.

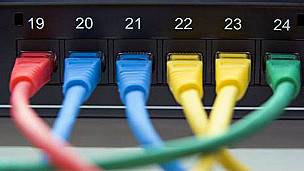
**En güvenli şifre nasıl oluşturulur?**

Bazı bilgisayar uzmanları en önemli etkenin şifre uzunluğu olduğunu söylüyor. Örneğin, 16 karakterden oluşan “arabamiseviyorum” gibi hatırlanabilir bir şifreyi tahmin etmek, 8 karakterli “T9$ey!!q” anlamsız bir şifreden daha zordur. Çünkü 16 karakterde kombinasyon sayısı çok daha fazladır; yani casus programların bu şifreleri çözmek için çok daha uzun süre uğraşması gerekecektir. Bir araştırmada, “etkili” olarak düşünülen sekiz karakterli şifrelerin yüzde 22’sinin 10 milyar denemenin ardından bulunduğu, 16 karakterli şifrelerde ise bu oranın yüzde 12’de kaldığı tespit edildi.

**Tahmin Edilemezi Tahmin Etmek** adlı kitabında William Poundstone başka önerilerde de bulunuyor. Örneğin, “l” ya da “i” harflerinin yerine “1” koymak tahmin yürüterek çok kolay bulunacağından ve sahte bir güvenlik hissi yarattığından bundan kaçınılması gerektiğini belirtiyor. Onun yerine, sizin için anlamlı olan bir cümlenin baş harflerini birleştirerek bir şifre yaratmanın daha güvenli olacağını ifade ediyor.

**Email şifremi değiştirdim, şimdi güvende miyim?**

Tam olarak değilsiniz. Bilmediğiniz bir yerde güvenli olmayan bir wi-fi kullanıyorsanız aynı noktadaki bir dinleyici aygıt sizin internetteki gezintinizi takip edip şifrenizi okuyabilir. Herhangi bir wi-fi’ye girmek için size şifre sorulmuyorsa büyük olasılıkla güvenli olmayan bir ortam söz konusudur. Bu noktalarda internet aktivitenizin email kontrolü ya da buluta veri yükleme gibi işlemleri içermemesine dikkat edin. Bu işlemleri evinizde kendi wi-fi sisteminize bağlanarak, telefonunuzda 3G ya da 4G sembolünü görerek yapmanız tavsiye olunur.



Daha güvende olmak için, telefonunuza bir sanal özel ağ (VPN) uygulama programı yükleyip dışardayken herhangi bir wi-fi noktasında bunu aktif hale getirebilirsiniz. Bu program internet aktivitenizdeki email şifreleriniz de dahil bütün verileri karıştırarak casus programlar açısından çözülemez hale getirir. Bu VPN’ler paralıdır.

**Bu beni veri hırsızlarından korur mu?**

Bunlar sadece başlangıç. Güvende olmak için atılacak başka adımlar da var. Ünlülerle ilgili son sızma olayının nasıl gerçekleştiğine dair fazla bilgi yok. Apple’ın iCloud bulut servisindeki bir zayıflıktan yararlanarak kullanıcının şifresini buluncaya kadar denemeler yaptıklarını biliyoruz. Fakat şifre ne kadar etkili olsa da bir hesaba girmenin başka bir yolu daha var. Eğer birisinin kullanıcı adını biliyorsanız “şifremi unuttum” fonksiyonunu kullanarak şifreyi yeniden oluşturmanız mümkündür. Bunu yapmak için elinizde doğum tarihi, annenin kızlık soyadı, gidilen okul, vb. bazı bilgilerin olması yeterli. Böylece güvenlik sorularına doğru yanıtlar verilerek şifreyi yeniden oluşturmak ve bu yolla hesaba girmek mümkün olur.

Özellikle ünlülerin bu tür bilgileri saklı tutması zor. Ama birçoğumuz da sosyal haberleşme ağlarında örneğin tam doğum tarihimizi ve diğer bazı kişisel bilgilerimizi hiç düşünmeden ifşa ediyoruz. Bu sitelerdeki hesap ayarlarımızı, biraz zaman ayırarak bu tür bilgilerimizi başkalarının görmeyeceği şekilde düzenlemek güvenliğimiz açısından önemlidir.

Bazıları ise bu tür hesaplarda sahte doğum tarihi kullanarak bu sorunu çözmüş oluyor.

**Bütün bunları yaptım, şimdi güvende miyim?**



Maalesef hayır. Ama bu adımları atarak bilgisayar korsanlarının kişisel bilgilerinize ulaşmasını çok daha zorlaştırdığınız kesin. Yapabileceğiniz bir başka şey de şu: Birçok email ve bulut hizmeti artık iki aşamalı kimlik testi uyguluyor. Bu hizmeti aktif kıldığınızda sadece şifrenizi yazarak hesabınıza ulaşamıyorsunuz. İkinci aşamada da cep telefonunuza gelen özel şifreyi girmeniz gerekiyor.

**Kişisel bilgilerim internette hiç güvende olacak mı?**

*Economist* dergisinde yayımlanan bir makalede belirtildiği gibi, “Siber ortamı güvenli kılmak zordur; çünkü internet güvenlikten ziyade bağlantıyı teşvik etmek üzere tasarlanmıştır.” Aklınıza gelebilecek her türlü cihazdan internete girmek artık mümkün olduğu için bu durum önümüzdeki yıllarda daha da karmaşık hale gelecek.

Aynı makalede şöyle deniyor: “Yeni yazılım programları hızla piyasaya sürülüyor ve ondan sonra da bunların ortaya çıkan zayıflıkları yeni eklentilerle giderilmeye çalışılıyor. Bu durumda tek kaybedilen şey veri olsa belki tolerans gösterilir, ama insanların kişisel güvenliği söz konusu olduğunda tüketiciler daha az tolerans gösterecektir.”

[**İNTERNETTEKİ TEHLİKELER**](http://sehitturkmentekinaihl.meb.k12.tr/meb_iys_dosyalar/48/02/762342/dosyalar/2020_01/28191145_Ynternetteki_Tehlikeler_v2.pdf)

**İnternette Kendinizi Korumanın 10 Yolu**



İnternetin hayatımızın temel parçalarından biri haline geldiğine hiç şüphe yok. Ancak birçoğumuz internetin aslında ürkütücü ve tehlikeli bir ortam olduğunun da farkında. Siber casusluk ve kimlik hırsızlığı, hacker’ların bilgisayarlarımıza siber saldırılar düzenleyerek şahsi bilgilerimizi çalması olasılığı, hepimizin korkulu rüyası.

Avrupa bankalarından bir milyar dolara yakın miktarda para çalan hackerlar ve Rusya, Hindistan, Çin, İran başta olmak üzere birçok ülkede milyonlarca harddisk’e kalıcı olarak gizlice yerleştirilen casus yazılım programlarıyla ilgili haberler gündemi işgal ediyor, internet kullanıcıları arasında korkuya neden oluyor. Başkan Barack Obama da kısa süre önce California’da katıldığı bir zirve toplantısında yaptığı açıklamada, son derece hayati önem taşıyan siber güvenliğin hükümetlerden şirketlere ve bireylere herkesin sorumluluğu olduğunu belirtmişti.



Peki bizler son derece sofistike becerilere sahip hacker’lara ya da siber savaşa giren ülkelere karşı nasıl mücadele edebiliriz? Bu sorunun yanıtı, ne yazık ki ‘hayır, mücadele edemeyiz’dir. Eğer bir hükümet ya da hacker bilgisayarınıza girmek isterse, girer, bunun kaçarı yoktur. Ancak bazı önlemler alarak hackerların işini zorlaştırmak, bizim elimizde. ‘Siber temizlik’ yapmak, internette kendimizi bir nebze de olsa güvence altına almak için çok önemli. İşte bu temizliği yapmanın yolları:

**Zor bir şifre oluşturun:**Bilin bakalım geçen yıl internet kullanıcıları arasında en popüler şifre ne? En popüler şifre, ‘şifre,’ derseniz pek de yanılmış olmazsınız. Şifre uygulamaları üreten SplashData şirketi, her yıl ‘yılın en kötü şifreleri’ni açıklayan bşr rapor yayınlıyor. Bu listeye göre geçen yıl en çok kullanılan, hack edilmeye en yatkın, en kötü şifre, ‘şifre’ kelimesinin İngilizce karşılığı olan ‘password’dü. SplashData’ya göre listenin ikinci sırasında ‘123456’ var. İnternet güvenliğinizi sağlamak için hiçbir şey yapmasanız bile şifrenizi zorlaştırın, kimsenin tahmin edemeyeceği hale getirin. En az sekiz karakter kullanın, büyük ve küçük harfleri, sembolleri ve rakamları karıştırın. Ve kesinlikle kedi ya da köpeğinizin, gittiğiniz okulların ya da sevgilinizin adını şifre olarak kullanmayın.

**Şifrenizi sık sık değiştirin:**  Birçoğumuzun en çok düştüğü hatalardan biri tek bir şifteyi birkaç hesapta birden kullanmak ya da şifremizi aylarca, hatta yıllarca hiç değiştirmemek. Zor bir şifre yaratmak başlıbaşına bir iş! Bunu hepimiz biliyoruz. Ve böyle bir şifreyi sık sık değiştirmek daha da zor bir iş. Ancak internet güvenliği için bunu yapmaya kesinlikle değer. Unutmayın, ne kadar zor olursa olsun, kırılamayacak şifre yoktur. Bu nedenle sık değişiklik yapmak şart.

**Ön belleğinizi sık sık temizleyin**: Bu öneri, evde ve işte kullandığınız bilgisayarlar, ara sıra kullandığınız arkadaşınızın tablet bilgisayarı gibi tüm cihazlar için geçerli. Firefox ya da Chrome gibi bir tarayıcıları kullandığınız zaman bu tarayıcılar hangi sitelere girdiğinizin, bu sitelerde neler yaptığınızın hesabını tutuyor. Girdiğiniz her site, internetten indirdiğiniz ya da internete yüklediğiniz her şey bu ön bellekte günlerce, hatta haftalarca listeleniyor. Başkalarının bu ön belleğe erişim sağlaması ve internetteki faaliyetlerinizin ayrıntılı dökümünü çalması son derece kolay. Bu nedenle arama motorlarında iz bırakmamak için gereken ayarları yapmak ya da işiniz bitince izlerinizi yok etmek son derece önemli.

**Ücretsiz Wi-Fi hizmetlerini kullanmayın**: Kafelerin, restoranların, barların, mağazaların ve kamuya açık başka yerlerin sunduğu ‘ücretsiz wi-fi’ hizmetinin hepimize cazip geldiği, yadsınmaz bir gerçek. Ancak unutmayalım ki ücretsiz wi-fi aynı zamanda güvenliksiz wi-fi anlamına geliyor.  Çok ihtiyacınız olmadığı sürece ücretsiz wi-fi hizmetlerinden olabildiğince uzak durun.

**HTTPS’yi kullanın**: HTTPS, HTTP’nin farklı bir türü. ‘S,’ ‘secure’ yani güvenli anlamına geliyor. Bu da internetteyken ek güvenlik katmanı ya da kriptolama sağlıyor. İnternet kullanıcıları ve HTTPS destekli internet siteleri arasındaki iletişim, kriptolu olarak gerçekleşiyor. HTTPS ayrıca sahte ve şüpheli siteleri de orijinallerinden ayırt edebiliyor.

**Flash sürücüleri kullanırken dikkatli olun**: Flash sürücüler, çok fazla veriyi taşıyacak kapasiteye sahip. Bu sürücüleri farklı plarformlarda kullanmak da büyük kolaylık sağlıyor. Ancak flash sürücüler, virüslerin yayılmasına ya da kötü amaçlı yazılımların sizin haberiniz olmadan bilgisayarınıza yerleşmesine de yol açabiliyor. Bu nedenle herhangibir flash sürücüyü bilgisayarınıza takmadan önce sürücünün kimlerin elinden geçtiğini iyi düşünün.

**Tıkladığınız yere dikkat edin:** Bazen hiçbir şüphe uyandırmayan internet sitelerinden gelen elektronik postalar, bilgisayarınızın hacklenmesi için gereken herşeyi içerebiliyor. Bu nedenle beklenmedik bir zamanda elektronik postayla bir dosya aldığınızda, konu başlığı ‘bak bunu çok seveceksin’ gibi gayet cazip sözcükler içerse de kesinlikle bu dosyaları açmayın.

**Kamuya açık bilgisayarları kullanmayın**: Evinde bilgisayarı ya da internet erişimi olmayanlar için bu, zor bir seçenek çünkü bu kişiler için internet kafeler, hala en popüler yerler. Ancak bir bilgisayar ne kadar çok kişi tarafından kullanılırsa bu bilgisayara virüs ya da elektronik posta hesapları gibi şahsi hesaplarınıza giren kötü amaçlı yazılım bulaşma olasılığı o kadar artar. Kimi kullanıcılar, internet kafelere giderken Tor ya da Psiphon gibi kişinin gizlililk ve güvenliğini sağlayarak internette hesaplarına girmesini ve gezinti yapmasını mümkün kılan yazılımları da flash sürücülerinde yanlarında götürüyor. Ancak bunlar bile kamuya açık bilgisayarlarda tam güvenlik sağlamıyor.

**Anti virüs programı kullanın**: Piyasada Kaspersky’den Norton’a, TrendMicro’ya, bazıları ücretsiz bazılarıysa ücretli olan çok sayıda anti virüs yazılımı bulunuyor. Bu yazılımlar, geniş kapsamlı koruma sağlıyor. Bu şekilde hacker’lara karşı profesyonel yardım almış oluyor ve her zaman hacker’ların bir adım önünde ilerliyorsunuz.

**İzinizi belli etmemeye çalışın**: Web siteleri, çerezler sayesinde hepimizin internette nerelere girip çıktığını çok iyi takip ediyor. Örneğin favori mağazanızın internet sitesinin istediğiniz ürünü çıkarıp karşınıza koyarak sizi hayretler içinde bırakması, işte bu çerezlerin marifeti. Her tarayıcı, ayarlar bölümünde, çerezleri silme tercihini yapmanızı sağlıyor. Ancak şunu unutmayın ki birçok internet sitesi, çerez kullanmayı kabul etmeyenlere hizmeti sınırlı tutuyor. Eğer Google gibi attığınız her adımı, aldığınız her soluğu takip eden bir arama motoruna bir alternatif arıyorsanız DuckDuckGo.com’a bir şans verebilirsiniz. DuckDuckGo.com, kullanıcıların kişisel gizliliğini koruma üzerine kurulu bir arama motoru.

Bu 10 öneri, internette daha güvenli bir biçimde işlem yapmanıza ve gezinmenize yardımcı olacaktır. Ancak her ne kadar önlem alırsak alalım, bilgisayarımızı hackleme hedefini aklına takmış becerikli hackerlardan kaçmanın hiç de kolay olmayacağını da akıldan çıkarmamakta fayda var.

[**KİŞİSEL GÜVENLİK**](http://sehitturkmentekinaihl.meb.k12.tr/icerikler/%20http:/sehitturkmentekinaihl.meb.k12.tr/meb_iys_dosyalar/48/02/762342/dosyalar/2020_01/28191229_KiYisel_Guvenlik_v2.pdf)



[**SOSYAL MEDYA**](http://sehitturkmentekinaihl.meb.k12.tr/meb_iys_dosyalar/48/02/762342/dosyalar/2020_01/28191315_sosyal_medya_v2.pdf)

**Kullanılmayan Hesaplar**

Günün birinde kullanabilirim diye açtığınız bir hesabınızın olduğunu düşünün. Çok güvenli olmayan bir parola belirlemiş veya bu parolayı bir yere not etmiş olabilirsiniz. Ancak kullanmıyor olsanız dahi kötü niyetli kişiler bu hesaplarınıza göz dikebilirler. Sizin adınıza söz konusu bu sosyal ağda paylaşımlar yapabilir, arkadaşlarınızdan sizin adınıza taleplerde bulunabilirler.

Kullanmadığınız hesaplar için de güvenli bir parola belirlemek, çift adımlı doğrulamayı açmak yapacağınız ilk işlem olmalı. Ya da hiçbir zaman kullanmayacağınızı düşünüyorsanız hesabı kapatmak da iyi bir seçenek.

**İnsan hatası**

Herkes hata yapar. Günümüzde hayatlarımızın ne kadar yoğun olduğunu göz önünde bulundurduğumuzda bir kişinin yanlışlıkla çevrimiçi tehditlere maruz kalması çok kolay. Küresel Bilgi Güvenliği Araştırmasına katılanların %77’si, dikkatsiz bir kullanıcının siber güvenlik tehdidinin en olası kaynağı olduğunu ortaya koyuyor.

Yanlış bağlantıya tıklamak veya yanlış bir dosyayı indirmek kadar basit bir şey hasara yol açabilir.

**Üçüncü parti uygulamalar**

Otel, kafe gibi halka açık noktalarda internete bağlanmak istediğinizde sizden sosyal medya hesaplarınızla giriş yapmanızı isteyebilir. Bu özellik başlangıçta büyük bir kolaylık gibi görünse de bir kullanıcı adı ve parola sormadığı, cep telefonu doğrulaması yapmadığı için güvenli değil. Bu nedenle üçüncü parti uygulamaları dediğimiz bu tarz uygulamaların sosyal medya hesaplarınızda nelere ulaşabildiğine mutlaka dikkatli bir şekilde bakmalısınız.

Söz gelimi bu yazıyı yazmak için oturduğum kafede internet bağlantısı için sistem benden Twitter ya da Facebook hesabımla giriş yapmamı istedi. Facebook’u seçerek devam ettiğimde bu halka açık kablosuz ağ Facebook’ta belirttiğim ad soyad, doğum tarihi ve Facebook arkadaşlarımın bilgilerini alacağını söyledi. İzin vermediğimde bu ağdan yararlanamayacak olsam da kişisel bilgilerimi paylaşmamayı tercih ettim. Tercih sizin.

**Olta saldırıları ve dolandırıcılığı**

Kimlik avı dolandırıcılığı ya da oltalama olarak geçen saldırılar son dönemde sıkça karşılaştığımız saldırı yöntemlerinden biri. Twitter ya da Facebook hesabınıza gönderilen bir özel mesajda “sosyal medya hesap şifrenizi yeniden girmeniz” gerektiği söyleniyor ve bir bağlantıya yönlendiriliyorsunuz. Bağlantıya tıkladığınızda açtığınız sayfanın ara yüzü resmi bir sayfa gibi görünse de aslında öyle değil. Bu sayfadaki form kişisel bilgilerinizi (kişisel verileriniz, banka bilgileriniz, parolalarınız gibi) teslim etmeye yönlendirmek için kullanılıyor olabilir.

**Kötü amaçlı yazılımlar (Malware’ler)**

Bilgisayar saldırganları sosyal medyada gün geçtikçe daha sofistike hâle geliyor. Saldırganlar, Kylie Jenner ve Mark Zuckerberg’e kadar çok sayıda ünlü kişinin Twitter hesaplarına eriştiler. Bilgisayarlarınıza bulaşabilecek virüs ya da malware ile klavyenizde yazdığınız tüm yazıların (buna parolalarınız da dahil) bir kopyasının saldırganların e-posta adreslerine gönderilmesini sağlayabilirsiniz. Bu durumda kurtulmanın en iyi yolu bilgisayarınızda güncel bir anti-virüs programı kullanmaktır.

**Güvenli olmayan cep telefonları**

Mobil cihazlar, sosyal ağlara erişmek için en popüler yolların başında geliyor. Hem her an yanımızda hem kullanımı çok kolay. Telefonunuz sizin elinizde kaldığı sürece bir sorun yok. Ancak, telefonunuzun kaybolması veya çalınması durumunda, tek dokunuşla sosyal medya hesaplarınıza erişim hakkının kötü niyetli kişilere geçmesi an meselesi. Telefonunuzu fiziken ele geçiren bu kişiler sosyal medya hesaplarınızdaki tüm bağlantılarınızı olta saldırılarıyla dolandırabilir.

Cihazlarınızı güçlü bir parola ile korumak bu gibi durumlarda oldukça önem taşır. Bunun yanı sıra böyle bir durum başınıza geldiğinde ilk yapmanız gereken şeylerden biri kullandığınız sosyal ağlardaki parolalarınızı değiştirmek ve diğer cihazlarınızdan uzaktan çıkış yapmak olacaktır.

Güvenli hesaplar için 3 önemli yol

**Şüpheli durumlar için bildirimlerinizi açın**

Sosyal medya hesaplarınızı korumanın bir yolu, mobil cihazınızda şüpheli durumlar için bildirimlerinizi açmaktır. Twitter, Facebook, Instagram, Google/Youtube gibi bilinen tüm popüler sosyal ağlar bu özelliği desteklemekte. Bu özellik sayesinde hesabınıza giriş yapmaya çalışan yeni bir cihaz olduğunda size e-posta ile bildirim gelecektir, erken teşhis ile hesabınızı kurtarabilmeniz mümkün.

**Parola Yönetici kullanın**

123456 gibi parolalar kullanmayın! Bilinçli kullanıcılar “böyle parola kullanan kaldı mı bu devirde” diye kızacak olsa da sıfırdan başlamakta fayda var.

Parolarınız mümkünse ezberleyemediğiniz, gerçekten karmakarışık bir şeyden oluşmalı. Bunun için [Duckduckgo.com](https://duckduckgo.com/) arama motorundan yararlanabilirsiniz. Duckduckgo’nun arama çubuğuna “[password 12](https://duckduckgo.com/?q=password+12&t=h_&ia=answer)” yazdığınızda 12 karakterli (Örnek: t8MjKNishb2Z) rastgele bir parola oluşturuyor. Daha sonra bu parolayı parola yöneticisi [Encryptr](https://play.google.com/store/apps/details?id=org.devgeeks.encryptr&hl=tr" \t "_blank)’e kaydedebilirsiniz. Ezberlemeniz gerekmiyor. Bu parolaya ihtiyaç duyduğunuzda ana şifrenizle Encryptr’e giriş yapmanız yeterli.

Sizin ve kurumunuzun sosyal medya hesap parolaları, siz ve bilgisayar saldırganları arasında duran şeydir. Sosyal hesaplarınız saldırıya uğrarsa, siz ve/veya kurumuzun itibarı zarar görebilir, bu nedenle güçlü parolalar oluşturduğunuzdan ve bunları sık sık değiştirdiğinizden emin olun.

[LastPass](https://www.lastpass.com/), [1Password](https://1password.com/) veya Encryptr gibi bir araç parolalarınızı korumayı kolaylaştırır ve şifreli bir kasada saklar. Parola yöneticisi uygulamalar, hesaplarınızın çevrimiçi güvenliğini aynı anda sağlarken, sürekli olarak giriş yapmanın zorluklarını ortadan kaldırır. Ayrıca, yeni sitelere erişim için kayıt olurken güçlü ve güvenli şifreler oluşturmanıza yardımcı olan rastgele bir şifre üreticisi de sağlar.

**Sosyal Hesaplarınıza Erişim Kontrolü**

Özellikle kurumsal sosyal medya hesaplarına erişimi olan çok sayıda kişi varsa bu çok sayıda tehlike olasılığı da var demektir. Bir hesabı birden fazla kişinin kullanması gerekiyor ve güvenlik riskini en aza indirgemek istiyorsanız bunun için üretilmiş çeşitli araçlar mevcut.

Twitter’ın kendi uygulaması olan [TweetDeck](https://tweetdeck.twitter.com/" \t "_blank) bu uygulamaların başında geliyor. TweetDeck gibi [Hootsuite](https://hootsuite.com/" \t "_blank) veya [SproutSocial](https://sproutsocial.com/" \t "_blank) gibi bir sosyal medya yönetim sistemleri ile hesap bilgilerinizi paylaşmadan istediğiniz kişilere erişim ve kullanım hakkı verebilirsiniz.

Sosyal medya hesaplarına kaydolurken iş ve/veya halka açık olarak kullandığınız e-posta adresi kullanmaktan kaçınmanız gerektiğini de unutmayın. Halka açık e-posta adresinizi kullanmak yerine sadece bu tip amaçlar için bir e-posta açmanız saldırganların hesabınıza saldırmasına bir engel oluşturacaktır.

[**E GÜVENLİK**](http://sehitturkmentekinaihl.meb.k12.tr/meb_iys_dosyalar/48/02/762342/dosyalar/2020_01/28191509_E_GUVENLYK.pdf)

