

Məlumatlarınızı və cihazlarınızı təhlükəsiz saxlamaq

Necə hədəf ola bilərsiniz?

Bir çox kiberhücumlar giriş məlumatlarınızı aşkar etmək məqsədilə **“fişinq”** (kiberdələduzluğun xüsusi növü) e-poçtu göndərirlər. Bunlara misal olaraq, sizin ünvanınıza hesabın sıfırlanması sorğuları kimi görünən e-poçt, saxta giriş səhifəsinə keçid və ya sənədin yönləndirilməsi kimi başqa bir prosedur tələb edən e-poçt daxil ola bilər.

Yüksək profilli şəxslərin e-poçt hesabları “fişinq” kampaniyalarında hədəflənə bilər və siz “fişinq” e-poçtlarını necə aşkar etmək barədə ətraflı məlumatları veb-saytımızda tapa bilərsiniz.

Hesablarınızın qorunması

Bunlar özünü və işçilərinizi kiberhücumlardan qorumaq üçün atacağınız addımlardır. Təvsiyə etdiyimiz ehtiyat tədbirləri sırasına, proqram təminatınızın və cihazlarınızın daim yenilənməsini təmin etmək və onlayn hesablarınızı güclü şifrələrlə qorumaq daxildir.

Sosial media hesabları

Sosial mediadan istifadə edərkən şəxsi məlumatlarınızı hansı dərəcədə təfərrüatlı paylaşdığınızdan xəbərdar olmalısınız. Bu tip məlumatlar tez-tez toplanır və kiberhücumları daha inandırıcı etmək üçün istifadə olunur.

Məsələn, “fişinq” e-poçtuna şəxsi məlumatlarınızın təfərrüatlarını əlavə etməklə daha inandırıcı görünməsinə təmin edə bilərsiniz.

Bütün sosial media hesablarınızın məxfilik parametrlərini nəzərdən keçirməli və təhlükəsizlik parametrlərinin sizi qane etdiyindən əmin olmalısınız.

Məsajlaşma proqramları

Məsajlaşma proqramlarından istifadə edərkən alıcıların kim olduğunu bilməlisiniz. İştirakçı sayı çox olan qrup söhbətində şəxsi məlumatlara nəzarət etmək çətin ola bilər.

Sosial mediada olduğu kimi, yazılarınızı kimin görə biləcəyini bilməlisiniz. Bura deputat olmazdan əvvəl etdiyiniz paylaşımlar da daxildir.

Şifrələrin başqa şəxslərlə paylaşılması

Siyasətçilərin sosial media hesabları çox vaxt hesabın şifrəsinin bir neçə nəfərlə paylaşılmasına görə oğurlanır.

Şifrə paylaşıldıqda hesaba kimin daxil olduğuna nəzarət etmək imkanınız olmayacaq. Bunun qarşısını almaq üçün çoxistifadəçi sosial media hesabı yaratmalısınız.

Şifrələr və ikimərhələli doğrulama (2SV)

Şifrələr

Zəif şifrələr asanlıqla sındırıla bilər. Şifrə nə qədər uzun olarsa, bir o qədər güclüdür və onu qırmaq çətin olacaq. Şifrənizi güclü etmək üçün üç təsadüfi sözdən istifadə edin.

Gizli məlumatları özündə saxlayan hesablarda güclü şifrədən istifadə etməli və təyin olunmuş şifrə yalnız həmin hesab üçün istifadə edilməlidir, eyni şifrə digər hesablarınızda təkrarlanmamalıdır. Bir çox şifrəni eyni anda yadda saxlamaq çətin ola bilər, bunun üçün şifrə menecerindən istifadə edə və ya şifrə brauzerinizin yaddaşında saxlaya bilərsiniz.

İkimərhələli doğrulama (2SV)

Hər bir “vacib” hesab ikimərhələli doğrulama (2SV) ilə qorunmalıdır. Bu, hər hansı bir yeni cihazdan ilk dəfə daxil olduqda mobil telefonunuza PIN kodun göndərilməsidir. Bu, hesabınızın iqiqat qorunmasını təmin edir və hakerlərin giriş əldə etməsini çətinləşdirir.

Sizin əsas e-poçt ünvanınız “vacib” hesabın qüsursuz nümunəsidir. Hər hansı hesaba girişi itirsəniz, şifrənin sıfırlama təfərrüatları əsas e-poçt ünvanınıza göndəriləcək. Buna görə də bu e-poçt hesabı “onlayn şəxsiyyətinizi” təmin edən açar rolunu oynayır. Bu səbəblərə görə əsas e-poçt ünvanınız 2SV ilə qorunmalıdır.

Kompüterlərinizi, telefonlarınızı və planşetlərinizi qorumaq

Girişin qorunması

Fiziki giriş əldə edən hakerlərin fəaliyyətini çətinləşdirmək üçün siz cihazlarınızı, cihaz yandırıldıqda və ya yenidən başladıqda daxil edilməli olan şifrəylə qorumalısınız.

Gözləmə rejimindən kilidi açmaq üçün siz şifrə, PIN kod, ekranda kiliddən açma işarəsi, barmaq izi və ya üz tanıma kimi sizə uyğun olan biometrik girişdən istifadə edə bilərsiniz. Əksər cihazlar, cihazın yerini müəyyən etməyə, itirildikdə və ya oğurlandıqda onu izləməyə imkan verir. Cihaz itirildikə şəxsi məlumatların uzaqdan silməyə imkan verən bir xüsusiyyət də vardır.

Bu funksiyanın (iPhone-da “Məni tap”, Android-də isə “Cihazımı tap”) aktiv olduğundan əmin olun.

Cihazlarınızın proqram təminatının yenilənməsi

Kibercinayətkarlar cihazlarınıza və ya hesablarınıza daxil olmaq üçün əməliyyat sistemi və proqramlardakı səhvlərdən və ya boşluqlardan istifadə edə bilərlər. Buna görə də istehsalçılar müntəzəm yeniləmələr təqdim edərək sizin təhlükəsizliyinizi təmin etmək üçün daima çalışırlar.

Cihazlarınızda ən son proqram təminatı, proqramlar və əməliyyat sistemindən istifadə etməklə nasazlıqları düzəldə və təhlükəsizliyinizi daha da artırma bilərsiniz.

Şəxsi cihazlarınızı müntəzəm olaraq yeniləyin və ya telefonunuzun, planşetinizin, noutbukunuzun, kompüterinizin avtomatik yenilənmə funksiyasını aktiv edin. Bu yeniləmələrin quraşdırılması haqqında məlumatları Apple, Microsoft və Google-dan asanlıqla tapa bilərsiniz.

Vacib məqamlar

- Güclü şifrələrdən istifadə edin;
- Şifrələri təkrarlamayın və ya digər hesablar arasında paylaşmayın;
- İkimərhəlləli doğrulamayı aktiv edin (2SV). Bu, vacib hesablarınızda, xüsusən də əsas e-poçt hesabınızda ikiqat qorunmanı təmin etmək üçün istifadə olunur;
- Yenilənmələrə laqeyd yanaşmayın;
- Telefon, planşet, noutbuk və kompüterinizin avtomatik yenilənməsini aktiv edin;
- Cihazınızı kilidləyin;
- Şifrə, PIN kod, kiliddən açma işarəsi, barmaq izi və ya üz tanıma kimi biometrik girişdən istifadə edin;
- Sosial media hesablarınızda məxfilik parametrlərinizi nəzərdən keçirin. Bütün sosial media hesablarınızda məxfilik parametrlərinin sizi qane etdiyindən əmin olun. Şifrəni heç kimlə paylaşmayın, başqa şəxslərin girişi üçün çoxistifadəçi hesabı qurun.