İB Təhlükəsizlik Əlavələr

Rabitəbank

Sosial mühəndislik
(Social engineering, Human hacking)

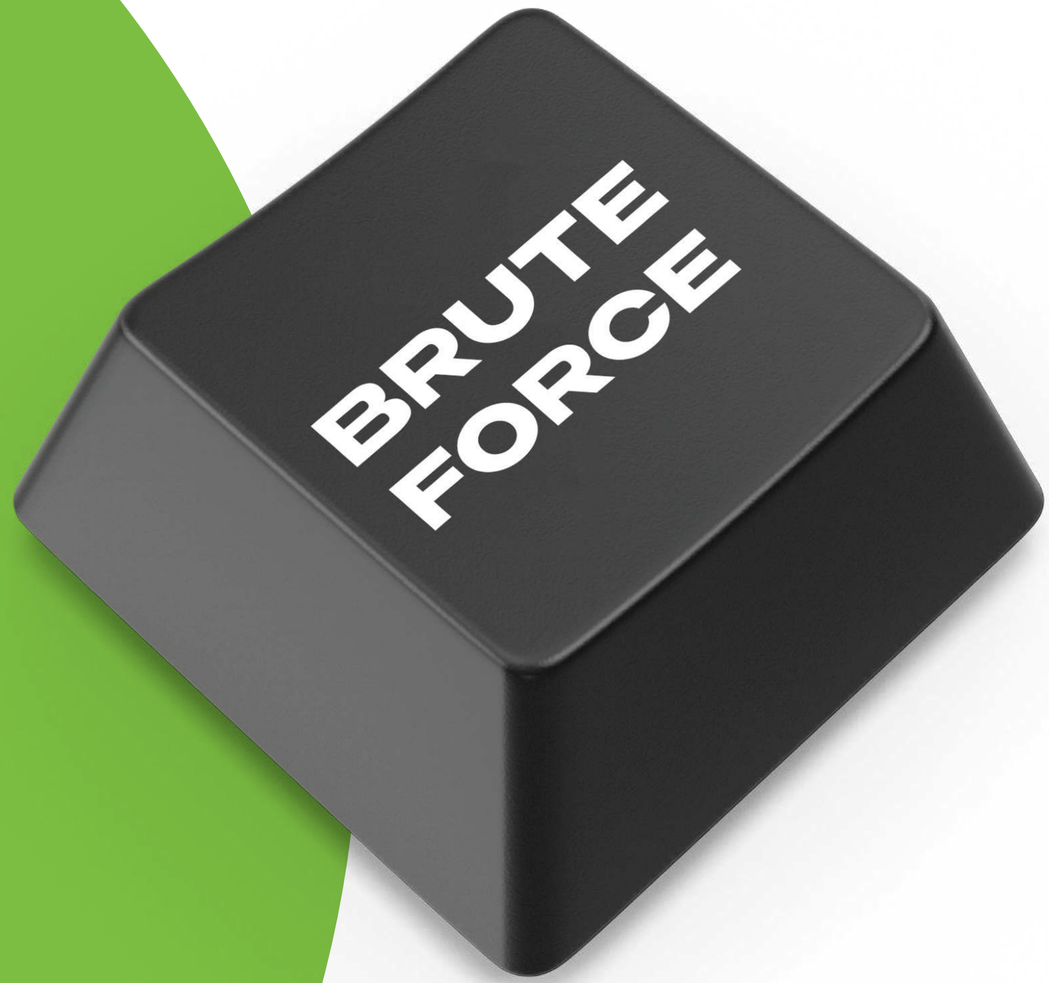
Sosial mühəndislik - insanlarla qarşılıqlı əlaqədə olaraq onlardan məlumat toplamaqdır. Bu növün əsas amillərindən biri saxta profillərdən (başqa adla açılmış və ya hər hansı bir saxta şirkət, kampaniya və s.), virtual dostluq və tanışlıqdan istifadə edib sizi aldatmaqdır. Əsas məqsədi tanışlıq, virtual dostluq və ya hər hansı digər etibar qazanmış mənbədən sui-istifadə etməklə məlumat yığmaqdır.
Bu təhlükədən qorunmaq üçün öz şəxsi məlumatlarınızı kənar şəxsə ötürməyin. Kimə ötürdüyünüzdən əmin olun. Toplanan məlumatlar sizin şifrələrinizin, məxfi suallarınızın tapılmasını asanlaşdırır.
Bədniyyət şəxs (haker və s.) və ya sizin etibarınızı qazanmış virtual dostunuz sizi müxtəlif saytlara yönləndirə və orada qeydiyyatdan keçmənizi istəyə bilər. Bu halda yönləndirilən saytın adına xüsusi diqqət yetirin, çünki hətta bir hərf dəyişməklə saxta sayt yaradıla bilər. (məs: www.facebook.com saytı əvəzinə sizi özünün idarə etdiyi www.-facabook.com saytına yönləndirə, daha sonra şifrə yazıb daxil olduğunuz halda şifrəni oğurlaya bilər). Bədniyyət şəxs sizə maraq dairənizdə olan şəkil, musiqi, video göndərə bilər və bu vasitə ilə zərər verən proqramları yoluxdura bilər.

“Brute-forcing”

“Brute-force” nədir?

Bu hücum sizin hər hansı e-mail hesabınıza (gmail, mail, rambler və s.) və ya digər hesabınızdakı şifrələr toplusuna edilən hücumdur. “Brute-force” hücumunu həyata keçirtmək üçün xüsusi proqramlar vasitəsi ilə sizin istifadəçi (login-parol) olduğunuz hesaba müdaxilə edilir.

Ən çox sizə aid məlumatlardan (məs: ad, soyad, doğum tarixi, maşın nömrəsi, telefon nömrəsi, yaşadığınız yer, valideyn və ya övladınızın adı və doğum tarixləri və s.) istifadə edərək “manual” (əl ilə bir-bir) və ya avtomatik şəkildə müxtəlif vasitələrlə hesabınızdakı şifrələr yoxlanılır. Bu texnika vasitəsi ilə şifrə (parol) tapılır. Bu texnikada əvvəl qeyd etdiyimiz kimi hədəf istifadəçiyə “Social engineering” olunur və yetərincə məlumat toplanılır. Bu hücumdan qorunmaq üçün şifrələrin təhlükəsizliyi bərpa edilməlidir.



Şifrələrin təhlükəsizliyi üçün bu qaydalara diqqət yetirilməsi vacibdir:
Şifrələrinizin eyni olmamasına diqqət yetirin. Müxtəlif sosial şəbəkələrdə, "mail"lərdə və ya digər hesablarınızda eyni şifrə istifadə etməyin. Bu hal sizin bir hesabınızın sındırıldığı halda digər hesablar da həmin şifrə ilə silsilə kimi sındırılacaq. Məs: "Facebook" şifrəsi ilə "Instagram" hesabının şifrəsi eynidirsə, biri bilindiyi halda digəri də ələ keçiriləcək. Bura müxtəlif alqoritm vasitəsi ilə yadda saxlanılan şifrələr də daxildir (məs: Əli_mail, Əli_facebook, Əli_instagram, Əli_123 - bunlardan istifadə etməyin)

- Yuxarıda göstərilən ən çox rast gəlinən sizə aid məlumatları (ad, soyad, doğum tarixi, maşın nömrəsi, telefon nömrəsi) şifrə qoyarkən istifadə etməyin.

- "Default" şifrələrdən istifadə etməyin (sistem tərəfindən verilən, məs: admin, 123456 və s.)

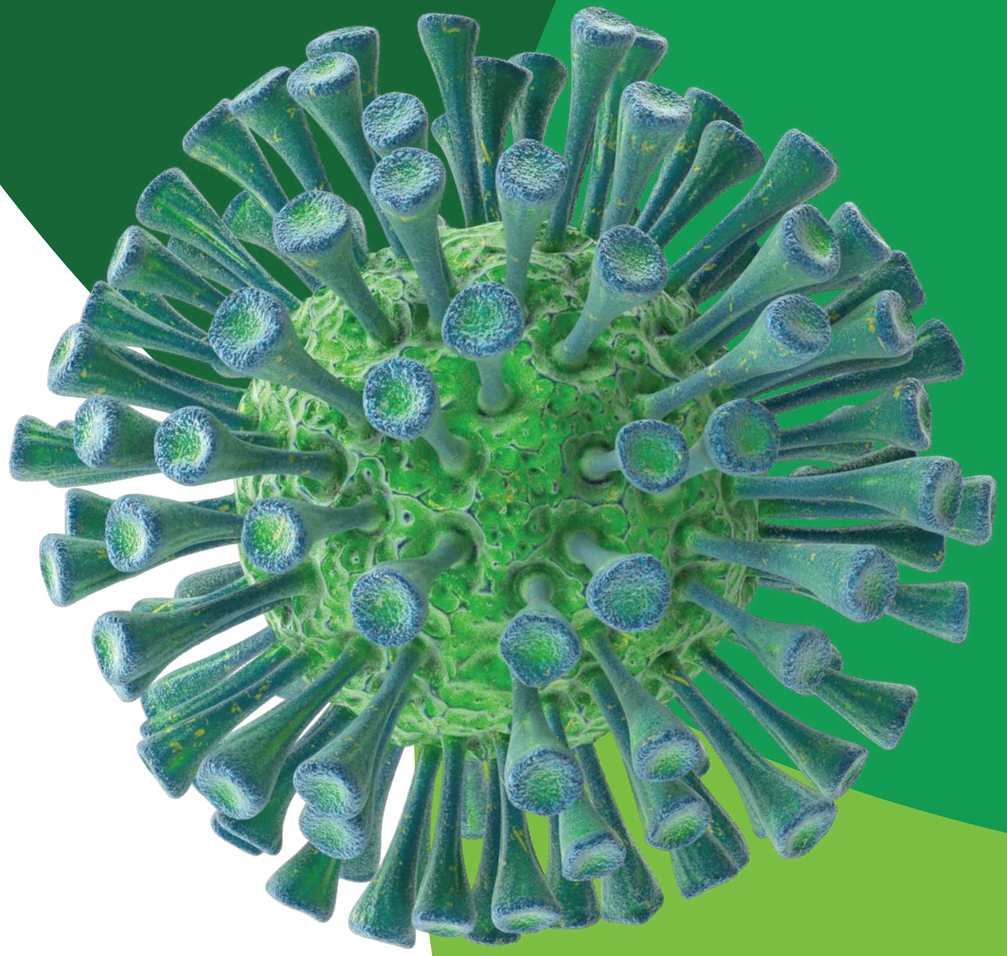
- Klaviaturada ardıcıl rəqəm, hərf, simvollardan istifadə etməyin (məs: qwerty, 123456, asdfgh)

- Şifrələri 2-3 aydan bir yeniləyin.

- Şifrələri hansısa vasitəyə və ya kağıza yazıb, iş masanıza qoymayın.
  Həmçinin onları ".word .txt" kimi fayllara yazıb kompüterdə saxlamayın.

- İkiqat şifrədən (two-factor authentication) (məs: Şifrə + SMS xidmətindən yararlanın) istifadə edin. Hesaba daxil olarkən SMS vasitəsi ilə ikinci şifrə gələcək.

Zərərverici proqramlar vasitəsilə yoluxdurma
(Malware, virus, trojans)



Zərərverici yoluxdurma texnikası istifadəçiyə video, şəkil, musiqi, kino, hər hansı fayl .doc, .txt), link vasitəsi ilə kompüterə “malware” (ziyanverici proqram) yüklənməsinə nail olmaqdır. Bu proqramların əsas məqsədi hədəfdən informasiya oğurlamaqdır. Məs: troyanların ən təhlükəli cəhəti yükləndikdən sonra özünü gizlətmək üçün özünü silərək, başqa adla kompüterinizin yaddaşında gizlənir və əməliyyatları arxa fonda yerinə yetirir. Bu halda kompüteriniz üçüncü şəxs tərəfindən idarə olunur və sizin materiallar, məlumatlar, şəxsi şəkil, video və s. hətta kompüterinizin kamerası xəbəriniz olmadan istifadə edilə bilər.

Malware simptomları:

- İnternet “browser”inizin əsas səhifəsi dəyişir;
- İnternetdə axtarış zamanı əlaqəsiz saytlar açılır;
- Əməliyyat sisteminizin qoruyucu divarı (firewall) avtomatik sönür;
- Heç bir iş görülmədiyi halda şəbəkədə aktivlik müşahidə edilir;
- Çoxlu sayda əlavə pəncərələrin açılması;
- Yeni proqram işarələrinin öz-özünə əmələ gəlməsi;
- Sistemin performansının zəifləməsi.

“Malware” təhlükədən qorunmaq üçün:

•Antivirus proqramından istifadə edilməli və bu proqram daim yenilənməlidir.

•Elektron ünvanınıza gələn tanımadığınız məktubları açarkən, müxtəlif linklər, sənədlər (.doc .pdf .txt) və digər faylları yükləyərkən ehtiyatlı olun.

•Kompüterinizdə hər hansı anomaliya baş verərsə, məs: kompüterin sönməsi, əlavə yazıların meydana gəlməsi – bunlar kompüter və ya mobil telefonda böyük ehtimal “malware” olmasından xəbər verir.

“Malicious software”lərdən qorunma üsulları:

•Gələn “mail”lərin əlavələrində olan faylları göndərən ünvandan əmin olmadıqca açmayın;

• Gələn “mail”lərin daxilində olan linklərə onların həqiqiliyinə əmin olmadıqca klik etməyin.

• Sadəcə əmin olduğunuz veb-səhifələrdən proqram, musiqi və digər bu kimi faylları yükləyin.

Fişinq (Phishing)

Kibercinayətin xüsusi növü olan fişinq (Phishing) - balıq ovu deməkdir. Bu metod vasitəsi ilə istifadəçiləri aldadıb, onların fərdi məlumatları oğurlanır. Haker sizi müxtəlif yollarla eyni olan, amma saxta olan hansısa sayta və ya digər resursa yönəltməklə apardığınız bütün əməliyyatları izləyir. Burada sizin bank kredit kartınızın parametrləri, ID nömrəniz, e-mail ünvanınız və s. məlumatlar ola bilər.

Bu təhlükədən qorunmaq üçün sizə yönləndirilən hər hansı saytın və həmin saytda sizdən tələb olunan bank kredit kartı, bank hesabı və bu kimi məxfi məlumatları yazmağınız tələb olunan sorğulardan şübhələnmək və etibarli mənbələrdən istifadə etmək tövsiyə olunur.

Elektron məktublarda xaker izləri:

Tanımadığınız mail ünvanlarından gələn mailləri mütləq silin;

- Bu “mail”lər yüksək professionallıqla hazırlanır və sizi tələyə düşməyə sövq edir;
- Daxil olan “mail”lərdəki əlavələri istifadə etməmiş əmin olun ki, bu həqiqətən sizə gəlib;
- Sizin iş yoldaşınız sizə mail yazıb? Bundan əminsinizmi?
- Digər təşkilatdan sizə mail gəlib, açmazdan əvvəl dəqiqləşdirin;
- “Mail”də sizə hansısa səhifəyə link göndərilib, açarkən diqqət edin.

Əlavələr:

- Bütün əməkdaşlar informasiya təhlükəsizliyi üzrə məlumatlar ilə tanış olmalıdırlar;
- Əmək müqaviləsində xidməti məlumatların kənar şəxslərə ötürülməməsi ilə əlaqədar bəndin tələblərinə riayət olunmalıdır;
- İşdən çıxarkən kompüterlər söndürülməlidir;
- Parollar kənar şəxslərə ötürülməməlidir.