Elektron Təhlükəsizlik Mərkəzi

Qaynar xətt: 1654
Email: reports@cert.az
Ünvan: Azərbaycan, Bakı, Droqal döngəsi, 702-ci məhəllə

İnternet vasitəsilə saxtakarlıqların qurbanı olmamaq üçün istifadəçilərin diqqət etməli olduğu amillər

Kiberfəzada şəxsi məlumatların oğurlanması təhlükənin yeni növü deyil. Lakin, son zamanlarda kibercinayətkarların sayının artması ilə bərabər, bu təhlükənin istifadəçilərə vurduğu ziyan da artmışdır.

Sizin internet üzərində yerləşən hesablarınızı hədəf seçən cinayətkarlar, ad, istifadəçi adları və ya şifrələr kimi şəxsi məlumatları ələ keçirə bilmək üçün ən çox phishing üsulundan istifadə olunur. Phishing müxtəlif qanuna zidd üsullarla login və şifrə kimi konfidensial (məxfi) məlumatların oğurlanmasıdır.

Praktikada phishing-in müxtəlif üsullarına rast gəlmək mümkündür. Bunlardan biri – elektron poçt vasitəsilə göndərilən saxta məktublardır. Bu məktublar sizin bildiyiniz və güvəndiyiniz şəxsdən və ya qurumdan (məsələn, bankdan hesabınızın bağlanması ilə əlaqədar gələn və ya digər vacib hallarla bağlı məzmuna malik məktublar) gəlmiş kimi görünür. Məktubların məzmununda sizdən hər hansı linklərə klikləmək və şəxsi məlulatlarınızı daxil etmək tələb olunur. Əslində həmin linklər saxta saytlara yönəlmişdir və sizin daxil etdiyiniz məlumatlar cinayətkarların əlinə keçir.

Lotareya oyunları və digər pul qazandıran üsullarla bağlı gələn elektron məktublar əslində təhlükə ola bilər. Məsələn, böyük miqdarda pulu sizin hesabınıza köçürmək və s. bu kimi maliyyə əməliyyatları üçün icazənizi tələb edən elektron məktublar əslində informasiyalarınız üçün riskdir.

Daha çox rast gəlinən hallardan biri tanımadığınız şəxslər tərəfindən göndərilmiş, məzmununda kiminsə varisi olmanızı və hesabınıza çoxlu pul köçürülməsini təklif edən məktublardır.

Digər təhlükə - saxta təhlükəsizlik proqram təminatlarıdır. İnternetdə saytları ziyarət etdiyiniz zaman kompüterinizin risk altında olduğunu göstərən veb səhifələr və ya pop-up pəncərələrlə qarşılaşa bilərsiniz. Bu xəbərdarlıqlarda hansısa proqramı endirməniz və kompüterinizə quraşdırmanız tələb olunur.

Əslində bu saxta və casus proqramları quraşdırmaqla kompüterinizin sisteminə ziyan vermiş olursunuz, həmçinin, lazımsız proqram üçün pul ödəmiş olursunuz.

Phishing qarşımıza harada çıxa bilər?

- *Elektron məktublar dostunuz və ya tanışlarınızın birindən gəlsə də, təhlükəli ola bilər;*
- *Sosial şəbəkələr ən riskli mənbələrdir;*
- *Yardım toplamaq məqsədilə qurulmuş kimi görünən veb səhifələr təhlükəli ola bilər;*
- *Sizin axtardığınız veb saytın ünvanına çox bənzəyən domenlərdən istifadə edən və həmin sayta çox bənzəyən veb səhifələr;*
- *Çatlaşma proqramları;*
- *Yalnız kompüter mühitində deyil, mobil telefonlarınızda və qurğularınızda da bu cür təhlükələrlə qarşılaşa bilərsiniz.*

İnternet vasitəsilə həyata keçirilən saxtakarlıqlar maliyyə itkilərinə, eyni zamanda kompüterinizin ciddi risk altına düşməsinə səbəb ola bilər. Bu tövsiyədə bu cür riskləri azaltmaq üçün bu cür saxtakarlığın necə müəyyən olunması və onlardan mümkün qədər uzaq qalmaq üsulları haqqında bəhs olunur.

✓ Phishing təhlükəsini müəyyən etmə üsulları

- "Dəyərli müştərilərimiz" şəklində ifadələr məktub göndərənin sizi tanımadığını göstərir. Diqqətli olmalısınız;
- Sizə xəbərdarlıq edən və ya sizdən təcili şəkildə "hərəkətə keçmənizi" istəyən məktublar phishing üsulu ola bilər;
- Adınız, istifadəçi adlarınız, şifrələriniz, kredit kartı nömrələriniz və ya bank hesab nömrəniz, doğum tarixiniz yaxud sizinlə bağlı digər şəxsi və maliyyə məlumatları soruşan məktublar – həmin məlumatları oğurlamaq üçün istifadə oluna bilər;

- Xüsusilə veb ünvanları yazarkən kiçik bir hərf səhvi sizi "tələ"yə sala bilər. Açılan səhifə sizin daxil olmaq istədiyiniz veb sayta çox bənzəyə bilər. Diqqət etməsəniz, müəyyən mərhələyə qədər məlumatlarınızı çoxdan oğurlamış ola bilər. Məsələn, www.microsoft.com əvəzinə, www.micrsoft.com daxil etdiyiniz zaman qarşınıza axtardığınız sayta çox bənzəyən səhifə çıxa bilər;

- Sizə gələn hər hansı məktubda və ya qarşılaşdığınız xəbərdarlıqda verilən linkə kliklədiyiniz zaman qarşınıza çıxan link, sizin kliklədiyinizlə eyni deyilsə, bu hal sizin məlumatlarınız üçün təhlükə yarada bilər;

- Hər hansı məktuba cavab verdiyiniz zaman cavab yazdığınız ünvan sizə məktub göndərən ünvandan fərqli olarsa, diqqətli olmalısınız.

✓ **Phishing təhlükəsinə qarşı müdafiə üsulları:**

- Spam məktubları silin, qəti şəkildə açmayın və ya cavablamayın;

- Elektron poçt məktublarındakı, mesajlardakı, pop-up pəncərələrdəki və ya çatlaşma proqramları vasitəsilə gələn mesajlardakı linklərə kliklədiyiniz zaman açılan səhifəyə diqqət edin. Məktubdan birbaşa linkə klikləmək əvəzinə linki kopyalamaqla yeni pəncərədə əlavə edib açın;

- Şəxsi və maliyyə məlumatlarınızı İnternet mühitində paylaşdığınız zaman diqqətli olun. Bu cür məlumatları tələb edən məktublar əslində təhlükədir. Buna görə də əmin olmadığınız anketlərə məlumat əlavə etməyin;

- Güclü şifrələrdən istifadə edin, bank və digər vacib hesablarınız üçün eyni şifrədən istifadə etməyin. Şifrənizin etibarlılığını test etmək üçün bu məqsədlə yaradılmış xüsusi proqram təminatlarından istifadə edə bilərsiniz. Məsələn, Microsoft şirkətinə məxsus olan Pasword Checker proqramı;

- Kompüterinizin firewall-nun aktiv olduğuna əmin olun. Avtomatik yeniləmə edə bilən antiviruslardan istifadə edin.

- Bank hesabı və ya kredit kartı ödəmələri barədə məlumatları tez-tez yoxlayın. Sizin məlumatınız olmadan edilmiş ödəmə ilə bağlı tədbirlər görün;

- Hər kəsin istifadə etdiyi şəbəkə və kompüterdən istifadə etməklə heç bir bank və ödəmə əməliyyatları həyata keçirməyin.

✓ **Saxta məzmunlu və casusluq xarakterli hallarla qarşılaşdıqda həyata keçirməli olduğunuz tədbirlər**

Hər hansı bir məktubun casusluq məqsədli məzmuna malik olduğunu düşünürsünüzsə, aşağıdakı tədbirləri reallaşdırmanız tövsiyə olunur:

- Məktubu silin, cavablamayın, məktubdakı linkə klikləməyin;

- Şübhəli hallarla qarşılaşdıqda lazımi orqanları bu barədə məlumatlandırın. Məsələn, hər hansı bir bankın adından sizə saxta məktub göndərilibsə, banka bu barədə məlumat verin.

- Şəxsi hesablarınızın başqaları tərəfindən istifadə olunduğunu düşünürsünüzsə, şifrələrinizi dəyişin. Bundan başqa, vacib hesablarınızın şifrələrini müəyyən periodlarla dəyişməniz faydalı olar.

- Phishing məqsədli məktubların məzmununda arzuolunmaz və ya pis niyyətli proqramlar mövcud ola bilər.Əgər kompüterinizdə belə bir proqramın quraşdırılmış olduğunu düşünürsünüzsə, online müdafiəni təmin edən təhlükəsizlik proqram təminatlarından birini istifadə edə bilərsiniz.