

Kā pasargāt sevi no pikšķerētājiem

TVNET

2011. g. 7. jūnijs

http://www.tvnet.lv/tehnologijas/internets/380456-ka_pasargat_sevi_no_pikskeretajiem/print

Lielāks mazāks Mainīt teksta izmēru

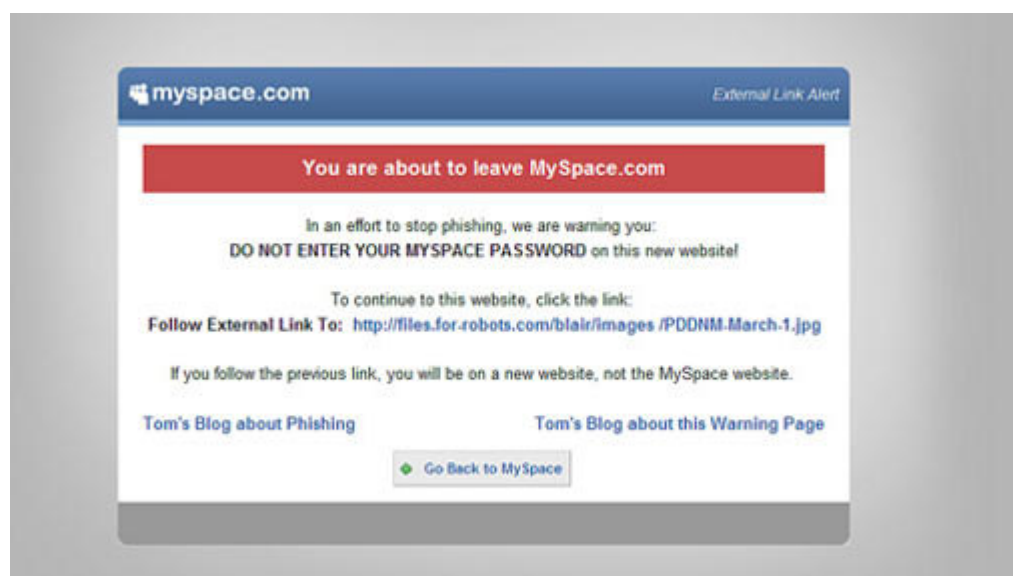


Foto: Flickr/paul_irish

Pikšķerēšanas jeb tā dēvētie "phishing" uzbrukumi pasaulē vairs nav nekāds jaunums. Interneta lietotāji ik dienas saņem miljoniem surogātpasta vēstuļu ar aicinājumiem veikt dažādas darbības, kas it kā "nodrošinās turpmāku kredītkartes darbību" vai "palīdzēs bankai precizēt lietotāja informāciju".

Resursi

Pikšķerētāji ielaužas ASV kodollaboratorijas datortīklos

Sniegtā informācija, protams, nokļūst krāpnieku rokās un tūlīt pat vai vēlāk tiek likta lietā, norāda "Cert.lv" vadītāja Baiba Kaškina.

Pavisam nesen šādu krāpšanas mēģinājumu Latvijā piedzīvoja "Swedbank", kuras klientiem maija pēdējās dienās tika izsūtīta viltota vēstule ar aicinājumu precizēt savu e-pasta adresi. Kādam nolūkam elektroniskajiem krāpniekiem bija vajadzīgas šīs klientu adreses, nav ilgi jādomā. Arī "Swedbank" šoreiz reaģēja zibenīgi un brīdināja savus lietotājus par viltvāržu darbībām, ko bija pamanījuši bankas modrie klienti.

Tomēr, neskatoties uz plaši izplatīto informāciju par "phishing" uzbrukumiem, vēl joprojām netrūkst cilvēku, kas uzķeras uz pikšķerētāju ēsmas, tādā veidā labprātīgi nododot savus datus krāpnieku rokās. Lai mazinātu kaitējuma risku, ko nezinātājiem var nodarīt pikšķerētāji, Informācijas tehnoloģiju drošības incidentu novēršanas institūcija (CERT.LV) ir sagatavojusi dažus padomus par to, kā pasargāt sevi no šādiem uzbrukumiem. Par tiem sīkāk stāsta CERT.LV vadītāja Baiba Kaškina.

Īpaši jāuzmanās no ziņām, kas sūtimas it kā bankas vārdā

Pirmkārt, nekad un nekur internetā vai ārpus tā nevajag sniegt informāciju par saviem finanšu instrumentiem. Bankas nekad šādu informāciju no saviem klientiem nevāc nedz ar e-pasta vēstuļu palīdzību, nedz telefoniski. (Starp citu, tieši to "Swedbank" arī uzsvēra savā oficiālajā paziņojumā, kad brīdināja klientus par uzbrukumu.) Tāpēc, "ja nu tiešām rodas šaubas, ka kādi dati būtu jāsniedz, vienmēr ir iespēja piezvanīt vai labākajā gadījumā pat aiziet uz savu banku, lai par to pārliecinātos," saka B.Kaškina, uzsverot, ka "protams, jāzvana uz bankas

oficiālajā mājaslapā, nevis šaubīgajā vēstulē norādīto tālruņa numuru". Banka visdrīzāk apstiprināšot to pašu, proti, šāda informācija vajadzības gadījumā tiek ievākta tikai un vienīgi klātienē, piemēram, kādā no bankas filiālēm.

Otrkārt, nav ieteicams vērt vai jā nekādus pievienotos failus, kas saņemti no nepazīstama sūtītāja. "Bieži vien zem tādiem šķietami nevainīgiem failiem kā attēli, prezentācijas, mūzika u.c. ir paslēptas programmas vai vīrusi, kas no lietotāja datora vai klaviatūras nolasa bankas paroles un citu konfidenciālu informāciju," skaidro CERT.LV vadītāja. Atverot tādu pielikuma failu, zagļu programma tiek automātiski lejupielādēta lietotāja datorā. Parasti tas nerada nekādus traucējumus pārējās programmatūras darbā un tādēļ ir sevišķi bīstami. Lietotājs var par to nezināt pat gadiem. Tāpēc, ja nu gadījumā ir sanācis atvērt kādu šaubīgu pielikumu no nezināma sūtītāja, būtu ļoti ieteicams datoru pārbaudīt pret vīrusiem (labāk to darīt nevis pašam, bet gan pie kompetenta datorspeciālista).

Treškārt, iepirkties var tikai labi zināmās un pārbaudītās interneta vietnēs. Ir pieredzēti gadījumi, kad krāpnieki izveido tādus interneta veikalus, kuru mērķis ir izmānīt kredītkaršu numurus un paroles. Ja viņiem tas izdodas, tad kārotā pirkuma vietā lētticīgie pircēji parasti saņem tukšu kontu. "Tāpēc visdrošāk par pirkumiem ir maksāt nevis nezināma interneta veikala sistēmā, ievadot kredītkartes numurus un kodus, bet gan no sava bankas konta, apmaksājot iepriekš izrakstītus rēķinus. Tādā veidā vismaz netiek norādīti dati, ko var izmantot, lai bez jūsu piekrišanas no konta novilktu **naudu**," norāda Baiba Kaškina. Tiesa, viņa atzīst, ka ne visas interneta veikalu sistēmas piedāvā rēķinu izrakstīšanu. Tāpēc, pirms iepērkaties nezināmā interneta veikalā, būtu ieteicams vismaz iepriekš palasīt kādas citu lietotāju atsauksmes par šo vietni.

© TVNET. Visas tiesības paturētas.