OUCH! 2023 - 06

OUCH!

SANS SECURITY AWARENESS

Ikmēneša informācijas drošības izdevums tev

Finanšu kontu drošība

Pārskats

Jūsu finanšu konti ir nozīmīgs kibernoziedznieku mērķis. Ja jums ir nauda, viņi darīs visu, lai to nozagtu. Ar finanšu kontiem mēs saprotam ne tikai jūsu norēķinu vai krājkontus, bet arī ieguldījumu, pensiju un tiešsaistes maksājumu kontus, piemēram, PayPal. Par laimi, veicot dažus vienkāršus un būtiskus pasākumus, varat sevi aizsargāt.

Kā kibernoziedznieki uzbrūk?

Bankas iegulda milzīgus līdzekļus savu sistēmu aizsardzībā, tāpēc kibernoziedzniekiem ir ārkārtīgi grūti uzlauzt to sistēmas. Tāpēc kibernoziedznieki uzbrūk jums un jūsu kontiem. Viņi zina, ka jums nav savas drošības komandas, kas jūs aizsargātu, tāpēc apkrāpt jūs ir daudz vieglāk nekā banku. Šeit ir aprakstīti divi visbiežāk sastopamie veidi, kā viņi var jums uzbrukt un mēģināt nozagt jūsu naudu:

Paroles: Katru jūsu finanšu kontu aizsargā parole. Ja kibernoziedzniekam izdodas uzminēt vai uzzināt kādu no jūsu parolēm, viņš var pieteikties jūsu vārdā un pēc tam pārskaitīt jūsu naudu uz viņa kontrolētiem bankas kontiem. Pastāv vairāki veidi, kā kibernoziedznieki mēģina iegūt jūsu paroli. Viena no izplatītākajām metodēm ir datora inficēšana ar ļaunprātīgu programmatūru. Ja jūsu dators ir inficēts, viņi var iegūt jūsu lietotājvārdu un paroli, kamēr piekļūstat bankas vietnei. Vēl viena izplatīta metode ir pikšķerēšanas e-pasta vēstuļu sūtīšana, uzdodoties par jūsu bankas pārstāvjiem. Noklikšķinot uz e-pastā norādītās saites, jūs domājat, ka pieslēdzaties bankas vietnei, taču patiesībā pieslēdzaties viltotai vietnei, kuru kontrolē noziedznieki. Tādējādi viņi var iegūt jūsu lietotājvārdu un paroli, ko pēc tam var izmantot, lai pieteiktos jūsu vārdā.

Informācijas lūgšana: Kibernoziedznieki var vienkārši lūgt jums paroli vai pārskaitīt viņiem naudu. Šādi sociālās inženierijas uzbrukumi bieži sākas ar to, ka kibernoziedznieki jūs sazvana pa tālruni. Kibernoziedznieki zina, ka, tiklīdz viņi jūs uzrunā, viņiem ir daudz vieglāk izmantot emocijas, lai piespiestu jūs kļūdīties. Tāpēc arvien biežāk sāk parādīties pikšķerēšanas e-pasta vēstules, balss pasts un pārlūkprogrammas uznirstošie logi, kas rada steidzamības sajūtu, norādot, ka jums jāzvana uz tālruņa numuru, lai atrisinātu kādu problēmu vai izmantotu kādu lielisku iespēju, pirms tā ir beigusies. Tiklīdz jūs piezvanāt uz norādīto tālruņa numuru, noziedznieki rada milzīgu spiedienu, lai jūs viņiem piešķirtu piekļuvi saviem kontiem vai pārskaitītu savu naudu uz citiem kontiem viņu labā. Piemēram, viņi var paziņot, ka pārstāv tehniskā atbalsta dienestu vai valdību, apgalvojot, ka jūsu dators ir inficēts un, ja nerīkosieties nekavējoties, jūs zaudēsiet visu savu naudu.

Sargāt sevi

Par laimi, bankas kontu aizsardzība ir vienkāršāka, nekā domājat. Lūk, trīs vienkārši soļi, kā sevi pasargāt.

1. **Esiet piesardzīgi**: Pirmkārt un galvenokārt, jūs pats varat sevi vislabāk aizsargāt. Ja saņemat e-pasta vēstuli, īsziņu, balss pastu vai pārlūka uznirstošo logu, kas šķiet dīvains vai aizdomīgs, iespējams, tas ir uzbrukums. Jo lielāka steidzamības izjūta un jo vairāk uz jums tiek izdarīts spiediens rīkoties TAGAD, jo lielāka iespēja, ka notiek uzbrukums.

2. **Izmantojiet drošas paroles / vairāku faktoru autentifikāciju (MFA)**: Aizsargājiet katru savu finanšu un personīgo e-pasta kontu ar garu, unikālu paroli. Nevarat atcerēties visas šīs unikālās paroles? Apsveriet iespēju izmantot paroļu pārvaldnieku, lai tās visas droši atcerētos un uzglabātu. Vislabākais veids, kā aizsargāt katru savu finanšu kontu, ir katrā kontā iespējot funkciju, ko sauc par vairāku faktoru autentifikāciju (MFA).

3. **Uzraugiet savus profilus**: Uzraugiet visus savus finanšu kontus. Varat iestatīt automātiskus brīdinājumus, kas nosūtīs jums e-pastu vai īsziņu, kad nauda tiks ieskaitīta kontos vai izņemta no tiem. Šādā veidā varat ātri pamanīt jebkuru neautorizētu vai aizdomīgu darījumu. Jo ātrāk atklāsiet, ka kaut kas nav kārtībā, un ziņosiet par to savai bankai, jo lielāka ir iespēja atgūt naudu.

Viesredaktors

Lina Doma (Lynn Dohm) ir organizācijas Women in CyberSecurity (WiCyS) izpilddirektore. Sākot no pieredzes kiberdrošības izglītības nozarē līdz aktīvai iesaistei grantu finansētās programmās un bezpeļņas organizācijās, Lina aizstāv un izplata izpratni par kiberdrošības darbaspēka dažādošanas nozīmi.
Twitter: @lynn_dohm. Linkedin: https://www.linkedin.com/in/lynndohm/.

Resursi

Emocionālie ierosinātāji: Kā kiberuzbrucēji piemāna cilvēkus: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
Pikšķerēšanas uzbrukumi kļūst piņķerīgāki: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/
Paroļu pārvaldnieki: https://www.sans.org/newsletters/ouch/password-managers/
Vairāku faktoru autentifikācija: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/

Tulkojums: CERT.LV