OUCH! 2024. gada

Ikmēneša informatīvais biļetens drošības izpratnes veicināšanai

Neļaujiet kibernoziedzniekiem izkrāpt jūsu uzkrājumus: pasargājiet savus finanšu kontus!

Viltīga krāpšana un tukšs bankas konts

Emīlijai bija ierasta rosīga otrdiena. Viņa paķēra savu rīta kafiju, paskatījās tālrunī un pamanīja īsziņu no savas bankas: "Vai veici šo darījumu?" Atbildi ar "JĀ" vai "NĒ." Viņa neizpratnē sarauca pieri. Tajā dienā viņa vēl nebija veikusi nevienu pirkumu. Varbūt tā bija tikai kļūda.

Viņa atbildēja "NĒ", un pēc dažām minūtēm viņai piezvanīja. Tā bija sieviete, kas apgalvoja, ka ir no viņas bankas krāpšanas nodaļas, un runāja mierīgā, profesionālā tonī. "Mēs esam konstatējuši neparastas darbības jūsu kontā. Lai to pasargātu, mums ir jāpārbauda daži dati." Emīlija, vēl aizvien miegaina, piekrita. Zvanītāja iepazīstināja Emīliju ar vairākiem soļiem, lūdzot viņas internetbankas paroli un pat norādot, lai viņa apstiprina paziņojumu savā tālrunī. "Tas bloķēs hakera piekļuvi," sieviete viņai apliecināja. Emīlija rīkojās atbilstoši norādījumiem, nenojaušot, ka iekrīt lamatās.

Dažas stundas vēlāk Emīlija saņēma vēl vienu paziņojumu. Šoreiz tas bija paziņojums: no viņas krājkonta bija izņemti 5000 dolāru. Panikā viņa pieteicās bankas lietotnē, taču bija jau par vēlu. Lietotne neatpazina viņas paroli. Viņai bija bloķēta piekļuve kontam. Pēc tam viņa redzēja, ka notiek vēl viena naudas izņemšana un vēl viena.

Emīlija acumirklī saprata. "Krāpšanas nodaļas" zvans bija izdomāts, labi organizēts kibernoziedznieku uzbrukums, kuri tagad pilnībā kontrolēja viņas kontu. Emīlija ātri piezvanīja savai bankai, cerot, ka varēs laikus glābt savu bankas kontu.

Kāpēc nepieciešams aizsargāt savus finanšu kontus

Mūsu tiešsaistes finanšu kontos – norēķinu, krājkontos un ieguldījumu vai investīciju kontos – glabājas vairāk nekā tikai nauda; tie atspoguļo smaga darba gadus, nākotnes plānus un finansiālo stabilitāti. Kibernoziedznieki nemitīgi meklē iespējas piekļūt jūsu naudai, un viena kļūda var novest pie ievērojamiem finansiāliem zaudējumiem. Ja domājat, ka vienkārša parole neļaus šiem noziedzniekiem iekļūt kontā, padomājiet vēlreiz.

Mūsdienu kibernoziedznieki ir gudri, viltīgi un neatlaidīgi. Ir ļoti svarīgi aktīvi aizsargāt savus finanšu kontus. Tas ne tikai palīdzēs novērst nesankcionētu piekļuvi, bet arī nodrošinās jums sirdsmieru, zinot, ka jūsu smagā darbā nopelnītā nauda ir drošībā.

Pieci soļi, lai aizcirstu durvis kibernoziedzniekiem

1. **Ieslēdziet vairāku faktoru autentifikāciju (MFA) jau tagad:** Vairāku faktoru autentifikācija jūsu tiešsaistes kontiem nodrošina papildu drošības līmeni, pieprasot, lai jūs apliecinātu savu identitāti, izmantojot divas vai vairākas metodes – kaut ko, ko jūs zināt (parole), kaut ko, kas jums ir (viedtālrunis), vai kaut ko, kas jūs esat (pirkstu nospiedums vai sejas atpazīšana). Pat ja kibernoziedznieks iegūst piekļuvi jūsu parolei, lai piekļūtu jūsu kontam, viņam joprojām būs nepieciešams otrais faktors. Vienmēr izvēlieties MFA, ja vien tas ir pieejams, jo īpaši attiecībā uz finanšu kontiem.

2. **Izmantojiet spēcīgas un unikālas paroles:** Katram kontam izveidojiet spēcīgas, unikālas paroles. Jo garāka parole un jo vairāk rakstzīmju tajā ir, jo labāk. Viena no idejām ir izmantot frāzveida paroli, kas sastāv no vairākiem vārdiem. Grūtības atcerēties? Bez problēmām. Izmantojiet paroļu pārvaldnieku, kas palīdz ģenerēt un saglabāt visas šīs garās un unikālās paroles.

3. **Krāpšana notiek nepārtraukti – neuzķerieties:** Viens no vieglākajiem veidiem, kā kiberuzbrucēji var iegūt piekļuvi jūsu kontiem, ir to jums palūgt. Viņi izveido e-pasta vēstules, īsziņas vai pat veic tālruņa zvanus, kas izskatās vai izklausās kā no jūsu bankas vai finanšu iestādes. Pirms noklikšķināt uz saitēm, lejupielādēt pielikumus vai atbildēt uz ziņojumiem vai tālruņa zvaniem, vienmēr pārbaudiet avotu. Jo lielāka steidzamības sajūta, jo lielāka varbūtība, ka e-pasts, ziņa vai tālruņa zvans ir uzbrukums. Labākais veids, kā sevi pasargāt, ir doties tieši uz savas bankas oficiālo tīmekļa vietni, ievadot adresi pārlūkprogrammā, vai arī piezvanīt bankai vai finanšu iestādei, izmantojot uzticamu tālruņa numuru.

4. **Kļūstiet apsēsts ar savu kontu uzraudzību:** Izveidojiet ieradumu bieži pārbaudīt savus finanšu kontus, lai konstatētu jebkādus neparastus darījumus. Pat vēl labāk, vairums finanšu iestāžu piedāvā automātiskus brīdinājumus par lieliem naudas izņemšanas apjomiem vai aizdomīgām darbībām. Automātisko brīdinājumu iestatīšana var palīdzēt savlaicīgi pamanīt krāpnieciskus darījumus un ātri rīkoties, lai samazinātu zaudējumus. Ja kaut kas neizskatās pareizi, negaidiet – rīkojieties nekavējoties.

5. **Turiet ierīces stingri pasargātas:** Jūsu tālrunis, klēpjdators un planšetdators ir kā seifs, kas nodrošina jūsu finanšu pasauli. Nodrošiniet to drošību, izmantojot spēcīgu ekrāna bloķēšanu un jaunākos programmatūras atjauninājumus; iesakām ieslēgt automātisko atjaunināšanu.

Viesredaktore

Elizabete Rasnika (Elizabeth Rasnick) ir Rietumfloridas Universitātes Kiberdrošības centra docente, kurai ir pieredze programmēšanā un darbā incidentu reaģēšanas komandā. Viņa ir WiCyS Floridas filiāles vecākā viceprezidente un ir ieguvusi doktora grādu informācijas tehnoloģiju jomā.

Resursi

Trīs populārākie veidi, kā kiberuzbrucēji vēršas pret jums: https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/
Kā kibernoziedznieki jūs apmuļķo: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/

Tulkojums: CERT.LV