



Aizmirsto kontu slēptie draudi: kāpēc ir svarīgi sakārtot digitālo telpu

Emmas aizmirstais spēļu foruma konts

Emma, 33 gadus veca programmatūras izstrādātāja, jau sen bija aizmirsusi par savu veco spēļu foruma kontu. Viņa bija reģistrējusies tajā pirms vairāk nekā desmit gadiem, kad studēja koledžā un bija apsēsta ar tiešsaistes stratēģijas spēli. Laika gaitā forums apsīka, spēle zaudēja popularitāti, un Emma turpināja savu dzīvi.

Kādu rītu Emma bija pārsteigta, atklājot savā personīgajā iesūtņē daudz e-pastu ar paroles atjaunošanas pieprasījumiem, tostarp no bankas, mākoņpakalpojuma konta un pat Netflix. Viņu pārņēma panika, kad viņa saprata, ka kāds ir pārņēmis kontroli pār viņas personīgo e-pasta kontu. Ļaundaris izmantoja piekļuvi viņas e-pastam, lai atiestatītu paroles vairākos citos pakalpojumos.

Pēc nelielas izpētes Emma atklāja iemeslu. Nesenā datu noplūdes gadījumā bija uzlauzts viņas aizmirstais tiešsaistes spēļu forums. Visu šī foruma lietotāju paroles bija apdraudētas, tostarp arī Emmas. Un parole, ko viņa toreiz izmantoja vecajam spēļu foruma kontam? Tā bija tā pati parole, ko viņa izmantoja savam personīgajam e-pasta kontam. Tikai dažu stundu laikā vecais konts bija kļuvis par milzīgu personīgās drošības risku. Tagad viņai bija jāveic saspringts uzdevums – atgūt savus kontus, sākot ar e-pastu.

Kāpēc vecie konti ir pakļauti riskam un kāpēc jums tas ir jāņem vērā

Katrs konts, ko jūs izveidojat, neatkarīgi no tā, cik necīgs tas šķiet tajā brīdī, glabā kādu personisko informāciju. Šī informācija var ietvert jūsu vārdu, e-pasta adresi, dzimšanas datumu, tālruna numuru, fizisko adresi un pat maksājumu informāciju.

Vecie konti var atrasties vecākās platformās, kas vairs netiek uzturētas, un novecojusi drošība padara jūsu datus neaizsargātus. Kad šīs vietnes tiek uzlauztas, jūsu paroles un personīgā informācija ir pakļauta riskam. Ja jūs esat kā Emma un izmantojat vienu un to pašu paroli vairākos kontos, jūs esat pakļauts daudz lielākam riskam. Kiberuzbrucēji bieži atkārtoti izmanto no viena konta iegūtās paroles, lai mēģinātu pierakstītos citos jūsu kontos.

Kā atrast vecos kontus

Jūs varbūt neatceraties visas vietnes, kurās reģistrējāties, bet ir veidi, kā atklāt savu digitālo pēdu nospiedumus:

- **Meklējiet sava e-pasta iesūtņē:** meklējiet e-pastus, kuros ir frāzes, *“piemēram,” “laipni lūdzam,” “apstipriniet savu e-pastu”* vai *“atjaunojiet savu paroli”*. Tās var palīdzēt atrast aizmirstos kontus.

- **Pārbaudiet savu paroli pārvaldnieku:** ja izmantojat paroli pārvaldnieku, pārskatiet saglabātos ierakstus. Tajā, visticamāk, ir ieraksti par jūsu izveidotajiem kontiem. Bieži vien varat filtrēt pēc vecākajiem kontiem vai tiem, kuriem nav piekļūts vairāk nekā gadu.
- **Pārskatiet savu mobilo ierīci:** pārskatiet visas savas mobilās lietotnes, lai identificētu kontus, kurus vairs neizmantojat.

Ko darīt ar vecajiem kontiem

Kad atrodat vecos vai neizmantotos kontus, ir laiks rīkoties.

1. **Dzēsiet to, ko neizmantojat:** ja vairs neizmantojat kontu, piesakieties un dzēsiet vai deaktivizējiet to. Ja platforma neļauj to dzēst, mainiet paroli uz unikālu un nejaušu, pēc tam no profila izdzēsiet visu personisko informāciju, piemēram, savu vārdu, adresi un maksājumu informāciju.
2. **Atjauniniet paroles kontiem, kurus saglabājat:** kontiem, kurus joprojām lietojat, nodrošiniet, ka katram ir droša, unikāla parole. Lietojiet paroli pārvaldnieku, lai palīdzētu izsekot un pārvaldīt savas paroles. Patiesībā vairums paroli pārvaldnieku jūs brīdinās, ja divi vai vairāki konti izmanto vienu un to pašu paroli.
3. **Pieslēdziet daudzfaktoru autentifikāciju (MFA):** svarīgiem kontiem, piemēram, e-pastam, bankai vai sociālajiem medijiem, iespējotiet MFA. Tas pievieno papildu aizsardzības slāni, pat ja jūsu parole kādreiz tiek apdraudēta. Ja iespējams, izmantojiet MFA visos kontos, kas to atbalsta.
4. **Padomājiet, pirms reģistrējaties:** turpmāk izveidojiet jaunus kontus tikai tad, ja tas ir nepieciešams. Ja izmantojat vietni tikai vienu reizi, izmantojiet viesu izrakstīšanās opcijas, nevis veidojiet jaunu kontu.

Padariet savu kontu pārskatīšanu par daļu no ikgadējās pavasara tīrīšanas. Neatkarīgi no tā, vai runa ir par vājām parolēm, novecojusi drošības sistēma vai aizmirsta personīgā informācija, jūsu "nākotnes Es" pateiksies jums par to.

.Viesredaktore

Džodija Frānsisa (Jodie Francis) ir WiCyS Ontario Canada biedru komitejas priekšsēdētāja un kibernetikas arhitekta ar vairāk nekā desmit gadu pieredzi IT un drošības jomā. Viņa aktīvi aizstāv sievietes un meitenes, veicinot viņu iesaistīšanos STEM karjeras jomā, un izglīto cilvēkus par labākajām personīgās kibernetikas praksēm.



Resursi

Kā kibernetikas nozogs jūsu paroles: <https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords/>
 Kā kibernetikas nozogs jūsu emocijas: <https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions/>
 Paroli pārvaldnieku spēks: <https://www.sans.org/newsletters/ouch/power-password-managers/>
 Frāzveida paroli spēks: <https://www.sans.org/newsletters/ouch/power-passphrase/>

Tulkojums: CERT.LV

OUCH! Izdevējs: SANS Security Awareness, izplatīts saskaņā ar [Creative Commons BY-NC-ND 4.0 licenci](https://creativecommons.org/licenses/by-nc-nd/4.0/). Jūs varat brīvi dalīties ar šo biļetenu vai izplatīt to, ja vien jūs to nepārdodat vai nepārveidojat. Redakcijas kolēģija: Fils Hofmans, Leslijs Ridouts, Princese Janga.

Vairāk informācijas par Ouch! Varat atrast šajā saitē: <https://www.sans.org/newsletters/ouch>