OUCH! 2026. gada

Workforce Security and Risk Training

Ikmēneša informatīvais biletens drošības izpratnes veicināšanai

Vairs nevarat piekļūt savam kontam? Kā atgūt piekļuvi

Neveiksmīga paroles atiestatīšana

Nadija steidzās uz vilcienu, kad viņas tālrunis pēkšņi pārtrauca sinhronizēt e-pastu. Viņa mēģināja pieteikties vēlreiz, taču parole tika noraidīta. Viņa izmantoja iespēju "Aizmirsāt paroli?", cerot ātri atiestatīt paroli. Taču atkopšanas kods tika nosūtīts uz vecu e-pasta adresi, ko viņa nebija izmantojusi gadiem. Viņa izmēģināja citu iespēju. Pakalpojums piedāvāja nosūtīt kodu īsziņā uz tālruņa numuru, kuru viņa vairs neizmantoja.

Nu jau satraukusies, Nadija mēģināja vēl vairākas reizes. Nekas nedarbojās – viņa vairs nevarēja piekļūt savam e-pasta kontam. Vēl sliktāk – viņas e-pasta konts bija saistīts ar bankas paziņojumiem, iepirkšanās kontiem, mākoņkrātuvi, sociālajiem plašsaziņas līdzekļiem un citu kontu paroļu atiestatīšanu. Bez piekļuves šim vienam kontam viņas digitālā dzīve sāka brukt kā domino kauliņi.

Tad viņa saņēma ziņu it kā no "konta atbalsta dienesta", kurā tika piedāvāts atjaunot piekļuvi, ja viņa samaksās noteiktu summu un sniegs personisko informāciju. Izmisīgi cenšoties atgūt savu kontu, viņa gandrīz izpildīja ziņā norādīto, taču tad saprata, ka viņas konts ir uzlauzts un šī ziņa ir krāpniecība. Nadija bija aizsargājusi savu kontu ar, viņasprāt, spēcīgu paroli. Taču viņa nebija padomājusi par vienu būtisku jautājumu: **ja viņa kādreiz zaudētu piekļuvi, vai viņa tiešām spētu to atgūt?** Konta atkopšana: jūsu digitālā rezerves atslēga

Konta atkopšana: jūsu digitālā rezerves atslēga

Daudziem tiešsaistes kontiem ir pieejams kāds konta atkopšanas process. Tas ir rezerves risinājums gadījumiem, kad aizmirstat paroli, pazaudējat tālruni, nomainät ierīci vai jums tiek liegta piekļuve kontam, piemēram, aizdomīgu darbību dēļ. Konta atkopšanai var tikt izmantota rezerves e-pasta adrese, mobilā tālruņa numurs, atkopšanas kods, uzticama ierīce, drošības atslēga vai cita iepriekš konfigurēta metode.

Problēma ir tā, ka šīs rezerves iespējas ir viegli vienreiz iestatīt un pēc tam par tām aizmirst. Pēc vairākiem gadiem rezerves e-pasta adrese var vairs netikt izmantota, tālruņa numurs var piederēt citai personai, bet atkopšanas kodi var būt pazuduši. Spēcīga parole aizsargā jūsu digitālās durvis. Pārdomāts atkopšanas plāns nodrošina, ka jums joprojām ir drošs veids, kā atgriezties atpakaļ.

Izveidojiet atkopšanas plānu, pirms tas ir nepieciešams

1. Pārbaudiet atkopšanas informāciju

Sāciet ar svarīgākajiem kontiem, piemēram, e-pastu, finanšu pakalpojumiem, mākoņkrātuvi un paroļu pārvaldnieku. Atveriet drošības iestatījumus un pārskatiet norādītās atkopšanas e-pasta adreses un tālruņu numurus. Vai tie ir aktuāli? Vai joprojām kontrolējat tos? Ja ne, atjauniniet tos tagad.

© SANS Institute 2026

2. Saglabājiet atkopšanas kodus

Daudzi pakalpojumi, kuros tiek izmantota daudzfaktoru autentifikācija, nodrošina vienreizlietojamus rezerves vai atkopšanas kodus. Šie kodi var palīdzēt atgūt piekļuvi, ja pazaudējat tālruni vai nevarat izmantot ierasto autentifikācijas metodi.

Glabājiet tos drošā vietā, piemēram, paroļu pārvaldniekā vai droši glabātā paroļu piezīmju grāmatiņā.

3. Nodrošiniet vairāk nekā vienu piekļuves atgūšanas veidu

Kad vien iespējams, konfigurējiet vairāk nekā vienu atkopšanas metodi. Piemēram, varat izmantot rezerves e-pasta adresi kopā ar atkopšanas kodiem vai drošības atslēgu. Paļaušanās tikai uz vienu ierīci vai tālruņa numuru rada vienu kritisku ievainojamības punktu. Ja šī atkopšanas metode vairs nav pieejama, varat zaudēt arī piekļuvi kontam.

4. Īpaši aizsargājiet atkopšanai izmantoto e-pasta kontu

Daudzi tiešsaistes konti ļauj atiestatīt paroli vai atkopt kontu, nosūtot atkopšanas e-pasta ziņojumu uz jūsu personīgo e-pasta kontu. Pārliecinieties, ka jūsu galvenais e-pasta konts ir drošs. Tāpat kā visiem tiešsaistes kontiem, ņemiet vērā kiberhigiēnas pamatprincipus: aizsargājiet savu personīgo e-pastu ar garu, unikālu paroli un daudzfaktoru autentifikāciju. Ja kibernoziedznieks apdraud jūsu personīgo e-pasta kontu, ko izmantojat citu kontu atkopšanai, viņš var atiestatīt paroles un pārņemt arī šos kontus.

5. Neizpaudiet atkopšanas informāciju

Izturieties pret rezerves kodiem un atkopšanas informāciju tāpat kā pret parolēm. Nekad neizpaudiet tos personai, kura negaidīti ar jums sazinās. Oficiālā atbalsta dienesta darbinieki nekad neprasīs jūsu paroli, daudzfaktoru autentifikācijas vai rezerves atkopšanas kodu.

6. Reizi gadā pārskatiet savu atkopšanas plānu

Tālruņu numuri mainās. E-pasta konti vairs netiek izmantoti. Ierīces tiek nomainītas. Reizi gadā veltiet dažas minūtes, lai pārskatītu savu svarīgāko kontu atkopšanas iestatījumus. Var būt noderīgi drošā vietā glabāt arī savu svarīgāko kontu sarakstu, lai katru gadu varētu ātri pārskatīt to atkopšanas iestatījumus. Visbeidzot, apsveriet iespēju ārkārtas gadījumam uzticamam ģimenes loceklim nodrošināt piekļuvi būtiskai atkopšanas informācijai.

Konta atkopšanu ir viegli ignorēt, kamēr viss darbojas, līdz pēkšņi vairs nedarbojas. Pazaudēts tālrunis, aizmirsta parole, nozagta ierīce vai uzlauzts konts var kļūt par daudz lielāku problēmu, ja jūsu atkopšanas iespējas ir novecojušas.

Viesredaktore



Prija Saravanana (Priya Saravanan) ir uzņēmuma UltraViolet Cyber vecākā drošības konsultante ar vairāk nekā septiņu gadu pieredzi ofensīvās drošības jomā. Viņa specializējas tīmekļa lietotņu ielaušanās testēšanā attiecībā un API, mobilajām lietotnēm un mākoņvidi. Viņa ir WiCyS Indianapolis nodaļas viceprezidente.

Resursi

Nepieļaujiet paroļu radītas galvassāpes: izmantojiet uzticamu paroļu pārvaldnieku https://www.sans.org/newsletters/ouch/stop-password-pain-reliable-password-manager
Frāžveida paroļu spēks: https://www.sans.org/newsletters/ouch/power-passphrase-why-longer-beats-smarter
Kā kibernoziedznieki nozog jūsu paroles: https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords

Tulkoja: CERT.LV

OUCH! Izdod SANS Security Awareness un izplata ar Creative Commons BY-NC-ND 4.0 licenci . Jūs varat brīvi dalīties ar šo biļetenu vai izplatīt to, ja vien jūs to nepārdodat vai nepārveidojat. Redkolēģija: Fils Hofmans (Phil Hoffman), Leslija Ridauta (Leslie Ridout), Prinsesa Janga (Princess Young).

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

© SANS Institute 2026