OUCH! 2025. gada

Workforce Security and Risk Training

OUCH!

Ikmēneša informatīvais biļetens drošības izpratnes veicināšanai

Piekļuves (passkeys) atslēgas – vienkāršāks un drošāks veids, kā autorizēties

Ar Sāras "spēcīgo" paroli nepietika

Sāra uzskatīja sevi par diezgan tehniski zinošu Viņa strādāja mārketinga jomā, izmantoja daudzus tiešsaistes dizaina rīkus un aizsargāja visus savus kontus ar garām, spēcīgām parolēm. Kādu rītu, dzerot kafiju un pārskatot īsziņas, Sāra pamanīja steidzamu ziņu no savas bankas: "*Mēs esam pamanījuši aizdomīgu darbību jūsu kontā." Noklikšķiniet šeit, lai nekavējoties pieteiktos un pārskatītu savu kontu*." Satraukta viņa noklikšķināja uz saites. Tīmekļa vietne izskatījās tieši tāpat kā viņas banka – ar to pašu logotipu un identisku izkārtojumu. Viss izskatījās leģitīms. Uztraucoties par sava konta drošību, viņa ievadīja savu lietotājvārdu un paroli, bet tīmekļa vietne paziņoja par kļūdu. Viņa vairākkārt mēģināja autorizēties, taču nesekmīgi. Tieši tad parādījās uznirstošais brīdinājums, kas atgādināja, ka viņa kavē sanāksmi. Es tikšu ar to skaidrībā vēlāk, viņa nodomāja, gatavojoties doties uz sarunu.

Stundu vēlāk viņa saņēma paziņojumu - no jūsu bankas konta tika izņemti **2000 ASV dolāru.** Viņai sažņaudzās sirds.

Viņa nekavējoties piezvanīja bankai. Izrādījās, ka ziņa bija viltota, tā bija smikšķerēšanas krāpšana. Tā ir līdzīgs pikšķerēšanas e-pasta uzbrukumam, taču tā vietā, lai izmantotu e-pastu, uzbrucējs nosūtīja īsziņu. Tīmekļa vietne, kuru viņa apmeklēja, bija viltota, taču bija veidota tā, lai izskatītos īsta un tādējādi izkrāptu viņas lietotājvārdu un paroli. Lai gan viņas parole bija gara un spēcīga, tam nebija nozīmes, **jo viņa to neapzinoties nodeva kibernoziedzniekam.**

Sliktākais? Tā kā Sāra uzskatīja, ka viņas parole ir pietiekami droša, viņa to izmantoja arī citos savos tiešsaistes kontos, lai gan zināja, ka tas nav ieteicams. Kad kiberuzbrucējs ieguva viņas bankas lietotājvārdu un paroli, viņš mēģināja izmantot tos pašus piekļuves datus, lai pieslēgtos arī citiem viņas kontiem. Viņas tiešsaistes iepirkšanās, multivides straumēšana un pat e-pasta lietošana pēkšņi kļuva apdraudēta. Tā bija ļoti gara diena.

Laiks atvadīties no parolēm – sveicinātas piekļuves atslēgas!

Vai esat noguris pastāvīgi ievadīt paroles un izmantot dažādas lietotnes un unikālus kodus, lai apliecinātu savu identitāti? Vai jūs uztrauc tas, ka neatkarīgi no tā, ko darāt, kiberuzbrucēji atradīs veidu, kā uzlauzt jūsu kontus? Iepazīstieties ar **piekļuves atslēgām**: vienkāršāku, ātrāku un daudz drošāku veidu, kā pieteikties jūsu kontiem.

Kas padara piekļuves atslēgas (passkeys) tik aizraujošas – tās ir drošas un vienlaikus vienkāršāk lietojamas nekā paroles; viss, kas jums nepieciešams, lai pieteiktos – esat jūs pats!

Kas īsti ir piekļuves (passkeys) atslēga?

Piekļuves atslēga ir slepens kods (tehniski – kriptogrāfisko atslēgu pāris), ko izveido jūsu dators, un daļa koda tiek saglabāta gan jūsu datorā, gan konkrētā tīmekļa vietnē. Jūsu kods ir unikāls tikai šai vietnei; katru reizi, kad iestatāt jaunu piekļuves atslēgu citai jaunai vietnei, tiek izveidots jauns, unikāls kods, kas tiek saglabāts jūsu datorā. Kad saglabājat kodu, bieži vien jums ir iespēja to saglabāt operētājsistēmā, paroļu pārvaldniekā vai pārlūkprogrammā. Pēc saglabāšanas nākamreiz, kad apmeklēsiet šo vietni, tā vietā, lai pieteiktos, izmantojot lietotājvārdu un paroli, jums, visticamāk, tiks lūgts atbloķēt slepeno kodu, izmantojot tā saukto biometriju. Biometrija ir autentifikācijas veids, kurā tiek izmantoti paša lietotāja bioloģiskie dati, piemēram, pirkstu nospiedums vai sejas atpazīšana. Vairs nav jāatceras vai jāievada paroles, jāraksta unikāli kodi, kas tiek nosūtīti ar īsziņu vai ģenerēti tālrunī, izmantojiet pirkstu nospiedumu vai sejas atpazīšanu. Turklāt jūsu biometriskā informācija nekad netiek kopīgota ar citiem tiešsaistē vai tīmekļa vietnēm, visa jūsu personiskā informācija paliek lokāli jūsu ierīcē.

Piekļuves atslēgas ir salīdzinoši jauna tehnoloģija, un katra tīmekļa vietne to var izmantot nedaudz atšķirīgi. Dažos gadījumos jums var tikt lūgts ieiet sistēmā ar savu paroli, pēc tam apstiprināt savu identitāti, izmantojot savu piekļuves atslēgu. Ja tiek prasīts izmantot paroles, pārliecinieties, ka parole ir unikāla un spēcīga. Izmantojot piekļuves atslēgu, lai aizsargātu savu kontu, jūs atvieglojat savu ikdienu, kā arī palīdzat bloķēt dažus no vismodernākajiem kiberuzbrucējiem no visas pasaules.

Viesredaktors

Dr. Johanness Ulrihs (Johannes Ullrich) ir SANS Tehnoloģiju institūta koledžas pētniecības dekāns. Viņš ir izveidojis un pašlaik vada SANS Internet Storm Center. SANS biedrs Dr. Ulrihs pasniedz tīmekļa lietotņu drošības (SEC522) un ielaušanās atklāšanas (SEC503) kursus. Viņa ikdienas īsformāta raidieraksts informē drošības profesionāļus par jaunākajām kiberdrošības aktualitātēm.

Resursi

Kā kibernoziedznieki nozog jūsu paroles: https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords/
Kā kibernoziedznieki izmanto jūsu emocijas: https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions/
Paroļu pārvaldnieku spēks: https://www.sans.org/newsletters/ouch/power-password-managers/
Frāzveida paroļu spēks: https://www.sans.org/newsletters/ouch/power-passphrase/

Tulkojums: CERT.LV