OUCH! 2025. gada

Workforce Security and Risk Training

Ikmēneša informatīvais biļetens drošības izpratnes veicināšanai

Kiberdrošības jautājumi jums šķiet pārāk sarežģīti? Koncentrējieties uz četriem pamatprincipiem

Stāsts

Marija vienmēr centās būt piesardzīga internetā, taču neskaitāmie padomi lika viņai justies apjukušai. Viņa bija dzirdējusi, ka nepieciešamas spēcīgas paroles, pretvīrusu programmatūra, VPN, ugunsmūri, privātuma iestatījumi, rezerves kopijas un vēl daudz kas cits. Nezinādama, ar ko sākt, viņa mēģināja pielāgot dažus sava Wi-Fi maršrutētāja tehniskos iestatījumus, taču drīz vien apjuka un padevās.

Vēlāk tajā pašā dienā Marija saņēma svarīgu īsziņu, kas izskatījās, it kā būtu no viņas bankas. Tajā bija brīdinājums, ka viņas konts tiks bloķēts, ja viņa nekavējoties neapstiprinās savu pieteikšanās informāciju. Uztraukta un neuzmanīga, viņa noklikšķināja uz saites un ievadīja savu lietotājvārdu un paroli. Dažu stundu laikā kibernoziedznieki bija iekļuvuši viņas bankas kontā. Tā kā viņa izmantoja vienu un to pašu paroli gan e-pastā, gan iepirkšanās vietnēs un pat sociālajos tīklos, viņi ātri ieguva pieeju gandrīz visai viņas digitālajai dzīvei.

Marija nekļuva par upuri tāpēc, ka bija nevērīga, viņa kļuva par upuri, jo nezināja, ar ko sākt.

Četri pamatprincipi: drošības vienkāršošana

Daudziem lielākais izaicinājums ir pārvarēt šo apjukuma sajūtu. Tāpēc Nacionālā kiberdrošības alianse (NCA) ir izveidojusi "četrus pamatprincipus" – vienkāršus, bet efektīvus soļus, kurus ikviens var ievērot. Koncentrējoties uz šīm četrām darbībām, jūs varat ieguldīt savu enerģiju tur, kur tā sniedz vislielāko drošību.

1. Spēcīgas, unikālas paroles (un paroļu pārvaldnieks)

Jūsu paroles ir atslēgas uz jūsu digitālo dzīvi. Diemžēl kibernoziedznieki nepārtraukti cenšas tās nozagt vai uzminēt. Ja izmantojat vienu un to pašu paroli vairākos kontos, ar vienu nozagtu paroli var atvērt visus kontus.

Lūk, kā "četru pamatprincipu" pieeja to vienkāršo:

- Katram kontam izmantojiet**garu un unikālu paroli**. Viena vienkārša metode ir izmantot frāzveida paroli – vairāku vārdu virkni, ko viegli atcerēties, bet grūti uzminēt. Dažos gadījumos var būt nepieciešams iekļaut arī burtus, ciparus un īpašās rakstzīmes.
- Nemēģiniet atcerēties visas savas paroles – ļaujiet **paroļu pārvaldniekam** paveikt to jūsu vietā. Šie rīki ģenerē spēcīgas paroles, droši tās glabā un automātiski ievada, kad piesakāties kontā. Uztveriet paroļu pārvaldnieku kā savu personīgo drošības seifu. Kad izveidojat spēcīgu galveno paroli, pārvaldnieks parūpējas par visu pārējo – tas samazina stresu un ietaupa jūsu laiku.

2. Daudzfaktoru autentifikācija (MFA)

Pat visdrošākā parole nav pilnīga. Šeit talkā nāk daudzfaktoru autentifikācija (MFA). To pazīst arī kā divfaktoru autentifikāciju vai divpakāpju verifikāciju – MFA pievieno papildu drošības slāni, pieprasot kaut ko papildus jūsu parolei, piemēram, uz tālruni nosūtītu kodu, pirksta nospiedumu vai drošības atslēgu.

Kāpēc tas ir svarīgi? Ja kibernoziedznieks nozog jūsu paroli, viņš joprojām nevar piekļūt jūsu kontam bez otrā faktora. Ieslēdziet MFA visur, kur tas ir iespējams, īpaši svarīgākajos kontos.

3. Automātiskie atjauninājumi

Kibernoziedznieki vienmēr meklē ievainojamības programmās un lietotnēs. Kad uzņēmumi atklāj šīs kļūdas, tie izlaiž atjauninājumus, lai tās novērstu. Ja atliekat atjauninājumu instalēšanu, jūs atstājat durvis vaļā uzbrucējiem, kas var izmantot zināmās ievainojamības. Vienkāršākais risinājums ir ieslēgt automātisko atjaunināšanu savās ierīcēs, lietotnēs un kontos. Tas nodrošina, ka labojumi tiek piemēroti fonā, bieži vien jums neko neliekot darīt.

4. Atpazīstiet un apturiet sociālās inženierijas (krāpniecības) uzbrukumus

Kibernoziedzniekiem ne vienmēr ir vajadzīgi tehniski triki – viņi bieži izmanto manipulēšanu ar cilvēkiem. Šo paņēmienu sauc par sociālo inženieriju, un tas ietver pikšķerēšanas e-pastus, viltus īsziņas un tālruņa zvanus, kas paredzēti, lai jūs apmānītu – noklikšķinātu uz saites, lejupielādētu ļaunatūru vai atklātu savas kredītkartes datus vai paroli.

Lūk, daži brīdinājuma signāli, kam jāpievērš uzmanība:

- **Steidzamība:** "Rīkojieties tūlīt, citādi zaudēsiet piekļuvi!"
- **Pārāk labi, lai būtu patiesība:** "Jūs esat laimējis balvu!"
- **Pieprasījumi pēc konfidenciālas informācijas:** paroles, PIN kodi vai bankas dati

Ja rodas šaubas – apstājieties, nesteidzieties un pārbaudiet.

Drošība var būt vienkārša

Drošībai nav jābūt sarežģītai. Koncentrējoties uz "četriem pamatprincipiem", jūs varat izveidot noturīgus tiešsaistes ieradumus. Neatkarīgi no tā, vai runa ir par jūsu kolēģiem, bērniem, vecākiem vai kopienu, "Četri pamatprincipi" piedāvā vienkāršu, bet efektīvu veidu, kā palīdzēt visiem būt drošākiem internetā.

Viesredaktore

Dženifera Kuka (Jennifer Cook) ir Nacionālās kiberdrošības alianses mārketinga vecākā direktore. Viņa vada organizācijas mārketinga stratēģiju un uzrauga kampaņas, kas iesaista miljoniem cilvēku. Kopš pievienošanās 2017. gadā Dženifera ir vadījusi iniciatīvas, tostarp Kiberdrošības informētības mēnesi un Datu privātuma nedēļu, sadarbojoties ar partneriem visā pasaulē. https://www.linkedin.com/in/jennifer-h-cook/

Resursi

Nacionālā kiberdrošības alianse: https://staysafeonline.org
Atjauninājumu spēks: https://www.sans.org/newsletters/ouch/power-updating/
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/
Paroļu frāžu spēks: https://www.sans.org/newsletters/ouch/power-passphrase/

Kopienai tulkoja: CERT.LV

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