Ikmēneša informācijas drošības izdevums tev

Mana iekārta ir uzlauzta. Ko darīt?

Vai mana iekārta ir uzlauzta?

Internets var būt mulsinošs, jo tajā jaunas tehnoloģijas nepārtraukti mainās. Lai arī cik drošs jūs censtos būt, agrāk vai vēlāk var gadīties, ka tiek uzlauzts jūsu konts vai kāda ierīce. Jo drīzāk konstatēsiet, ka ir noticis kaut kas slikts, un ātrāk reaģēsiet, jo vairāk varēsiet samazināt negatīvo ietekmi. Turpinājumā ir minētas pazīmes, kas liecina par to, ka jūsu konts vai ierīce varētu būt uzlauzta, un, ja tas tā ir, ieteikumi, kā to risināt.

Pazīmes, ka, iespējams, ir uzlauzts kāds no jūsu tiešsaistes kontiem

- Jūsu draugi vai ģimenes locekļi saņem no jums dīvainus ziņojumus vai uzaicinājumus, kurus jūs neesat sūtījuši.
- Ievadot paroli, jums paziņo, ka parole nav derīga, kaut arī jūs ļoti labi zināt, ka paroli esat ievadījuši pareizi.
- Jūs saņemat paziņojumus no vietnēm par pierakstīšanos tajās (log-in), kaut arī paši to neesat veikuši.
- Jūs saņemat e-pastus, kas apstiprina izmaiņas jūsu tiešsaistes profilā, kuras neesat veicis.

Pazīmes, ka ir uzlauzts jūsu dators vai mobilā ierīce

- Jūsu antivīruss ģenerē paziņojumus, ka jūsu iekārta ir inficēta. Pārliecinieties, ka tie tiešām ir jūsu antivīrusa paziņojumi, nevis uznirstoši logi kādā tīmekļa vietnē, kas cenšas jūs iebiedēt un panākt, ka piezvanāt uz paziņojumā norādīto telefona numuru vai lejupielādējat kaut ko. Neesat droši? Atveriet savu antivīrusa programmatūru un pārbaudiet, vai jūsu dators tiešām ir inficēts.
- Pārlūkojot internetu, jūs bieži tiekat pārmesti uz vietnēm, kuras nemaz nevēlējāties apmeklēt, vai bez jūsu ziņas tiek atvērtas jaunas tīmekļa vietnes.
- Jums parādās uznirstošais logs, kurā tiek paziņots, ka jūsu dators ir sašifrēts un jums jāmaksā izpirkuma maksa, lai atgūtu savus failus.

Pazīmes, ka ir uzlauzta jūsu kredītkarte vai finanses

- No jūsu maksājumu kartes vai bankas konta ir veikti savādi maksājumi, par kuriem droši zināt, ka tos neesat veikuši.

Ko tagad darīt? - Kā atgūt kontroli

Ja jums ir aizdomas, ka ir notikusi uzlaušana, saglabājiet mieru. Jūs tiksiet ar to galā. Ja uzbrukums ir saistīts ar jūsu darbu, necentieties situāciju atrisināt pašrocīgi. Nekavējoties ziņojiet par to. Ja uzlauzts jūsu personīgais konts vai iekārta, ir sekojošas lietas, ko varat darīt:

- **Tiešsaistes kontu atgūšana:** Ja jums joprojām ir piekļuve jūsu kontam, piesakieties no uzticama datora un atjaunojiet paroli ar jaunu, unikālu un drošu paroli – jo garāku, jo labāk. Ja neesat aktivizējis daudzfaktoru autentifikāciju (MFA), tagad ir īstais laiks to aktivizēt. Ja vairs nevarat piekļūt savam kontam, sazinieties ar tīmekļa vietnes uzturētāju un informējiet viņu par to, ka jūsu konts ir pārtverts. Ja jums ir citi konti, kuriem ir tāda pati parole kā jūsu uzlauztajam kontam, nekavējoties nomainiet arī šīs paroles.
- **Personīgā datora vai iekārtas atgūšana:** Ja jūsu antivīruss netiek galā ar infekciju, vai arī jūs vēlaties būt pilnīgi pārliecināti, ka jūsu sistēma ir drošībā, apsveriet iespēju pārinstalēt operētājsistēmu, tādā veidā nodrošinot, ka sistēma tiks veidota pilnīgi no jauna. Vai arī, ja jūsu dators vai iekārta ir novecojusi, varbūt pienācis laiks iegādāties jaunu.
- **Finanses:** Par problēmām ar savām maksājumu kartēm vai bankas kontiem nekavējoties sazinieties ar savu banku vai maksājumu karšu izsniedzēju. Jo drīzāk sazināsieties, jo lielāka ir iespēja, ka varēsiet atgūt savu naudu. Piezvaniet viņiem, izmantojot uzticamu telefona numuru, piemēram, to, kas norādīts uz jūsu maksājumu kartes, kas redzams uz jūsu konta pārskata izrakstiem, vai norādīts viņu mājas lapā. Regulāri pārbaudiet savu kontu izrakstus un maksājumu vēsturi. Ja iespējams, ieslēdziet automātiskos paziņojumus, kad tiek iekasēta maksa vai veikts naudas pārskaitījums.

Ko darīt, lai aizsteigtos priekšā kiberuzbrucējiem?

OUCH informācijas drošības biļetens tiek publicēts ik mēnesi, un tajā ir vesela rakstu sērija par to, kā pasargāt sevi. Turpmāk sadaļā "Resursi" norādām svarīgākos OUCH biļetenus, kas ir jāizlasa, lai aizsargātu sevi. Šajos resursos galvenā uzmanība tiek pievērsta trim galvenajām darbībām:

1. Uzturiet visas savas sistēmas un ierīces atjauninātas ar jaunākajām versijām.
2. Izmantojiet drošas, unikālas paroles katram savam kontam, pārvaldiet šos kontus, izmantojot paroļu pārvaldnieku, un iespējojiet MFA.
3. Esiet skeptiski: uzmanieties no sociālās inženierijas taktikām, piemēram, pikšķerēšanas e-pastu ziņojumiem.

Viesredaktors

Sāra Moralesa (Sarah Morales) (@SarahManley) ir vecākā programmu vadītāja Google Privātuma, drošības un aizsardzības komandā. Viņa vada ārējo sadarbību, galveno uzmanību pievēršot kopienas veidošanai, sadarbībai un partnerībām. Viņa ir Wicys valdes locekle un aktīvi iesaistās DEI centienos kiberdrošības kopienā.

Resursi

Paroļu pārvaldnieki: https://www.sans.org/newsletters/ouch/password-managers/
MFA: vienkārša darbība kontu drošībai: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/
Emocionālie ierosinātāji – kā kiberuzbrucēji piemāna cilvēkus: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
Pikšķerēšanas uzbrukumi kļūst piņķerīgāki: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/

Tulkojums: CERT.LV