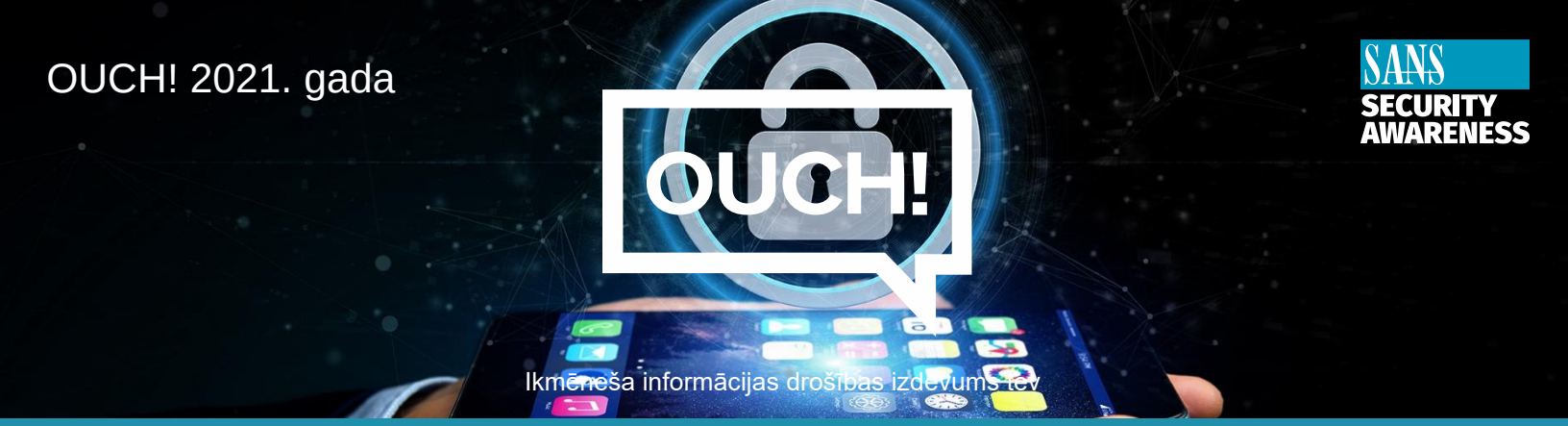

Ikmēneša informācijas drošības izdevums lietotājiem

Mobilo ierīču aizsardzība

Pārskats

Mobilās ierīces nodrošina lielisko iespēju sazināties ar draugiem, iepirkties, izmantot bankas pakalpojumus tiešsaistē, skatīties filmas, spēlēt spēles un veikt neskaitāmas citas darbības. Tā kā šīm ierīcēm ir būtiska loma jūsu dzīvē, ir svarīgi, lai jūs un jūsu ierīces būtu drošas un aizsargātas.

Jūsu ierīču aizsardzība

Iespējams, jūs pārsteigs atklājums, ka savu mobilo ierīci, visticamāk, jūs pats apdraudat vairāk nekā kibernoziedznieki. Pazaudēt vai kaut kur atstāt savu mobilo ierīci ir lielāka iespēja, nekā kādam to uzlauzt. Pirmais, kas jums būtu jāizdara, lai aizsargātu savu ierīci, ir jāiestata automātiskā ekrāna bloķēšana, kad ierīci nelietojat. Tas nozīmē, ka, lai lietotu ierīci, tā jāatbloķē, izmantojot drošu paroli, pirkstu nospiedumu vai sejas atpazīšanu. Šī funkcija nodrošina sarežģītāku piekļuvi jūsu datiem gadījumā, ja ierīci esat pazaudējis vai tā nozagta. Turklāt lielākajā daļā mobilo ierīču ekrāna bloķēšana ieslēdz arī datu šifrēšanu, tādējādi tie ir labāk pasargāti.

Lūk, vēl daži padomi, kā aizsargāt savu ierīci:

1. **Atjaunināšana**: Savā ierīcē ieslēdziet automātisko atjaunināšanu, lai vienmēr tajā pieejama jaunākā operētājsistēmas un lietotņu versija. Uzbrucēji pastāvīgi meklē nepilnības programmatūrā, un ražotāji regulāri laiž klajā atjauninājumus un ielāpus, lai tās novērstu. Ierīces atjaunināšana padara to daudz grūtāk uzlaužamu. Izvēloties jaunu Android ierīci, pārliecinieties, ka ražotājs ir apņēmies ierīci regulāri atjaunināt. Apple iOS ierīces atjaunina pats uzņēmums, taču Android mobilās ierīces atjaunina konkrētās ierīces ražotājs, un ne visi ražotāji to dara regulāri. Ja lietojat vecāku ierīci, ko vairs nav iespējams atjaunināt, apsveriet iespēju iegādāties jaunu, kura atbalsta atjauninājumu instalēšanu.

2. **Ierīces izsekošana**: Instalējiet vai ieslēdziet uzticamu programmu, kas attālināti izsekos jūsu ierīci ar interneta palīdzību. Šādā veidā varat izveidot savienojumu ar to, izmantojot internetu, un atrast tās atrašanās vietu, ja ierīce ir nozaudēta vai nozagta, vai, sliktākajā gadījumā, attāli izdzēst visu tajā esošo informāciju.

3. **Uzticamas mobilās lietotnes**: Instalējiet tikai nepieciešamās lietotnes un izmantojiet uzticamus avotus. Apple iOS ierīcēm iPad vai iPhone tas ir Apple App Store. Ja jums ir Android ierīce, izmantojiet Google Play; ja jums ir Amazon planšete, izmantojiet Amazon App Store. Lai gan varat instalēt lietotnes arī no citām vietnēm, tur tās nav pārbaudītas, un pastāv daudz lielāka iespēja, ka tās ir inficētas vai ļaundabīgas, radot risku jūsu privātumam. Pārliecinieties arī par to, ka lietotnei ir daudz pozitīvu atsauksmju un ka tā tiek regulāri atjaunināta. Izvairieties no pilnīgi jaunām lietotnēm, lietotnēm, par kurām ir maz atsauksmju vai kuras tiek reti atjauninātas.

4. **Privātuma iespējas**: Mobilās ierīces par lietotājiem ievāc lielu apjomu informācijas, it īpaši tāpēc, ka tās tiek visur ņemtas līdzi. Rūpīgi pārskatiet savas ierīces privātuma iestatījumus, tai skaitā atrašanās vietas izsekošanu, un pārliecinieties, ka sensitīvi paziņojumi (piemēram, verifikācijas kodi) netiek parādīti ekrānā, kad ierīce ir bloķēta.

5. **Darbs**: Pārliecinieties, ka jebkuru mobilo ierīci, ko izmantojat darba vajadzībām, ir atļauts tam izmantot. Esiet uzmanīgi darba vietā un neuzņemiet foto vai video, kuros nejauši varētu būt iekļauta sensitīva informācija kā tāfeles vai datoru ekrāni.

Jūsu mobilā ierīce ir spēcīgs rīks, un mēs vēlamies, lai jūs izbaudītu tā lietošanu. Ievērojot šos pāris vienkāršos padomus, varat nodrošināt savu un savu iekārtu drošību.

Viesredaktors

Džerons Bekerss (Jeroen Beckers) ir uzņēmuma NVISO mobilās drošības eksperts, drošības standartu OWASP MASVS un MSTG līdzautors, instruktors institūtā SANS un autors SEC575: Mobile Device Security and Ethical hacking course (Mobilo ierīču drošības un ētiskas uzlaušanas kurss). Džeronu iespējams atrast LinkedIn: https://www.linkedin.com/in/beckersjeroen/.

Resursi

Atjaunināšana: https://www.sans.org/newsletters/ouch/the-power-of-updating
Droša mobilo lietotņu izmantošana: https://www.sans.org/newsletters/ouch/securely-using-mobile-apps/
Teksta paziņojumu/ smikšķerēšanas uzbrukumi: https://www.sans.org/newsletters/ouch/messaging-smishing-attacks
Kā padarīt paroles vieglāk iegaumējamas: https://www.sans.org/newsletters/ouch/making-passwords-simple
Vikšķerēšana — tālruņa zvanu uzbrukumi un krāpniecība: https://www.sans.org/newsletters/ouch/vishing

Tulkojums: CERT.LV