

OUCH!

Ikmēneša informācijas drošības izdevums tev

Atbrīvošanās no mobilās ierīces

Pārskats

Mobilās ierīces, piemēram, viedtālruni, viedpulksteņi un planšetdatori, turpina pārsteidzoši strauji attīstīties un pieredzēt inovācijas. Tāpēc jaunu ierīci var nākties nomainīt pat katru gadu. Diemžēl, iespējams, pat nenojaušat, cik daudz personas datu ir jūsu ierīcēs — daudz vairāk nekā datorā. Turpmāk aprakstīti dažādi datu veidi mobilajās ierīcēs un tas, kā varat droši formatēt ierīci pirms atbrīvošanās no tās vai nomaiņas. Ja mobilo ierīci jums ir izsniedzis darba devējs, vispirms sazinieties ar savu vadītāju par to, kā atbrīvoties no ierīces.

Jūsu informācija

Jūsu mobilajās ierīcēs tiek glabāts vairāk sensitīvu datu, nekā jūs domājat, tostarp . . .

Jūsu dzīves un darba vieta, kā arī ikdienas pārvietošanās paradumi.

Kontaktinformācija par visiem jūsu adresu grāmatā esošajiem cilvēkiem, tostarp ģimeni, draugiem un kolēģiem.

Telefona zvānu vēsture, tostarp ienākošie, izejošie zvani, balss pasts un neatbildētie zvani.

Īsziņas vai tērzēšanas sesijas lietotnēs, piemēram, drošas tērzēšanas lietotnēs, spēlēs un sociālajos tīklos. Personiskie fotoattēli, videoklipi un audioieraksti.

Saglabātās paroles un piekļuve jūsu kontiem, piemēram, bankai, sociālajiem tīkliem vai e-pastam.

Ar veselību saistīta informācija, tostarp par jūsu vecumu, sirdsdarbības frekvenci vai fizisko aktivitāšu vēsturi.

Finanšu informācija, tostarp kredītkartes, maksājumu metodes un darījumi.

Ierīces formatēšana

Neatkarīgi no tā, kā atbrīvojaties no savas mobilās ierīces, piemēram, ziedojot to, apmainot pret jaunu, atdodot kādam citam, pārdodot tālāk vai pat pārstrādājot, vispirms izdzēsiet visu sensitīvu informāciju. Neuzskatiet, ka nākamais īpašnieks „rīkosies pareizi”. Pirmais solis ir izveidot ierīces dublējumu, lai varētu atjaunot un pārsūtīt visus datus un iestatījumus uz jauno ierīci. Kad ir veikta dublēšana, vajadzētu atiestatīt ierīci, jo tādējādi tiek izdzēsti dati un atjaunoti rūpnīcas noklusējuma iestatījumi. Atiestatīšanas procesa laikā jums var tikt piedāvāts ievadīt mākoņa paroli, lai pārtrauktu visas saites starp šo ierīci un mākonī — noteikti to izdriest. Turpmāk norādītās atiestatīšanas darbības ir paredzētas divām visizplatītākajām ierīcēm — Apple un Android.

Apple iOS ierīces: Iestatījumi | Vispārīgi | Pārsūtīšana vai atiestatīšana | Dzēst visu saturu un iestatījumus.

Android ierīces: Iestatījumi | Sistēma | Atiestatīšanas opcijas | Dzēst visus datus (šīs opcijas atšķiras atkarībā no ierīces ražotāja).

SIM un ārējās kartes

Papildus ierīces atiestatīšanai apsveriet arī to, ko darīt ar SIM (abonenta identifikācijas moduļa) karti. Tā ir mazā karte tālrunī, ko jums ir izsniedzis mobilo sakaru operators; tā identificē ierīci un ļauj tai izveidot mobilo vai datu savienojumu. Formatējot ierīci, SIM kartē tiek saglabāta informācija par jūsu kontu, un tā ir saistīta ar jums. Ja saglabājat savu tālruņa numuru un pārejat uz jaunu ierīci, sazinieties ar tālruņa pakalpojumu sniedzēju par SIM kartes pārvešanu. Ja tas nav iespējams, saglabājiet veco SIM karti un fiziski to iznīciniet. Daudzos mūsdienu viedtālruņos ir tā dēvētā eSIM, kas ir virtuāla SIM karte, nevis fiziska SIM karte. Atiestatīšanas procesa laikā eSIM tiek dzēsta.

Visbeidzot, dažās Android mobilajās ierīcēs papildu atmiņai tiek izmantota izņemama SD (Secure Digital) karte. Pirms iznīcināšanas izņemiet šīs ārējās atmiņas kartes no mobilās ierīces. Šīs kartes bieži vien var atkārtoti izmantot jaunās mobilajās ierīcēs vai arī tās var izmantot kā vispārīgu atmiņu datorā, izmantojot USB pāreju. Ja nav iespējams atkārtoti izmantot SD karti, tāpat kā veco SIM karti, iesakām to fiziski iznīcināt.

Ja neesat pārliecināts par kādu no iepriekš aprakstītajiem soļiem vai ja ierīces atiestatīšanas opcijas atšķiras, nogādājiet mobilo ierīci veikalā, kurā to iegādājāties, un lūdziet palīdzību. Visbeidzot, ja vēlaties ierīci izmest, apsveriet iespēju to ziedot. Ir daudzas lieliskas labdarības organizācijas, kas pieņem lietotas mobilās ierīces, un daudzi mobilo sakaru pakalpojumu sniedzēji savos veikalos ir izvietojusi atkritumu urnas, lai tās pārstrādātu.

Viesredaktors

Hetera Mahalika (@HeatherMahalik) ir Cēlebrīte digitālās izlūkošanas vecākā direktore (Sr. Dir) un SANS DFIR mācību programmas vadītāja, [FOR585](#) autore un SANS fakultātes pasniedzēja. Heteras karjeras pamatā ir tiesu ekspertīžu pētījumi un 20 gadus ilgs darbs ar izmeklēšanas lietām. Emuārus viņa raksta vietnē www.smarterforensics.com/blog.



Resursi

Droša mobilo lietotņu izmantošana: <https://www.sans.org/newsletters/ouch/securely-using-mobile-apps/>

Mobilo ierīču pasargāšana: <https://www.sans.org/newsletters/ouch/securing-mobile-devices/>

Mobilā tālruņa ziedošana: <https://www.makeuseof.com/best-places-to-donate-your-old-phone/>

SANS kurss: Padziļināts viedtālruņu kriminālistikas kurss: <https://sans.org/for585>

Tulkojums: CERT.LV

OUCH! To publicējais "SANS Security Awareness", un tas tiek izplatīts saskaņā ar "Creative Commons BY-NC-ND" 4.0 licenci. Jūs varat brīvi koplietot vai izplatīt šo rakstu, kamēr vien jūs to nepārdodat un nepārveidojat. Redakcijas kolēģija: Valters Skrivenss (Walter Scrivens), Fils Hofmans (Phil Hoffman), Alans Vagoners (Alan Waggoner), Leslija Rīdauts (Leslie Ridout), Princesa Janga (Princess Young).