

OUCH!

Ikmēneša informatīvais biļetens drošības izpratnes veicināšanai

Jūsu viedtālrunis ir zelta raktuve kibernoziem

Kabatas izmēra katastrofa

Emma baudīja nedēļu ilgu atvaļinājumu skaistā, saulainā salā. Kādu pēcpusdienu pēc vairākām pludmalē pavadītām stundām viņa pirms atgriešanās viesnīcā iegriezās nelielā kafejnīcā, lai paēstu pusdienas. Sajūsmināta par skatu uz okeānu un vēloties pēc iespējas ātrāk atgriezties ārā, viņa, aizietot, nejauši atstāja savu viedtālruni uz galda. Tikai pēc vairākām stundām viņa saprata, ka tālrunis ir pazudis.

Sākumā Emma pārāk neuztraucās. Viņa devās atpakaļ uz kafejnīcu meklēt savu viedtālruni, taču tā tur vairs nebija. Tam, kurš bija atradis viņas tālruni, tagad bija potenciāla piekļuve Emmas personīgajam e-pastam, sociālo mediju kontiem, banku lietotnēm un pat autentifikācijas lietotnei, ko viņa izmantoja savas identitātes apliecināšanai, piesakoties svarīgās vietnēs.

Turklāt ceļojuma laikā Emma palāvās uz tālruni, lai izmantotu kartes, viesnīcu rezervācijas un aviosabiedrību informāciju, kā arī lai sazinātos ar ģimeni. Viņa vairs nevarēja piekļūt iekāpšanas kartei, apstiprināt ceļojuma plānus vai saņemt uz ierīci nosūtītos drošības kodus.

Par laimi, Emma pirms ceļojuma bija ielēgusi ekrāna bloķēšanu un attālo izsekošanu. Atgriezusies viesnīcas numurā, viņa savā klēpjdatorā pieteicās kontā un konstatēja, ka ierīce vairs neatrodas kafejnīcā. Kad kļuva skaidrs, ka tālruni atgūt neizdosies, viņa attālināti bloķēja tālruni un izdzēsa tā saturu, lai aizsargātu savu informāciju. Laimīgā kārtā viņa varēja arī ātri atgūt savus datus, jo bija izveidojusi informācijas dublējumkopiju.

Pieci soļi kā aizsargāt savu mobilo ierīci

1. Ieslēdziet drošu ekrāna bloķēšanu

Pirmā aizsardzības līnija ir neatļautas piekļuves novēršana jūsu ierīcei. Lai bloķētu tālruni vai planšetdatoru, izmantojiet PIN kodu, piekļuves kodu, pirksta nospiedumu vai sejas atpazīšanu. Ja ierīce tiek pazaudēta vai nozagta, droša ekrāna bloķēšana var neļaut citai personai uzreiz piekļūt jūsu lietotnēm, kontiem un personiskajai informācijai. Uztveriet ekrāna bloķēšanu kā savas digitālās mājas ārdurvis. Iestatiet savu ierīci tā, lai tā automātiski bloķētos, kad tā ir neaktīva jums ērtā, pēc iespējas īsākā laika posmā. Izveidojiet ieradumu apzināti bloķēt tālruni ikreiz, kad to noliekat malā.

2. Ieslēdziet ierīces izsekošanu un attālinātu datu dzēšanu

Kas notiek, ja jūsu ierīce tiek pazaudēta vai nozagta? Lielākajā daļā mūsdienu mobilo ierīču ir iebūvēti pakalpojumi, kas ļauj tās atrast kartē, likt tām zvanīt, attālināti bloķēt vai izdzēst visus datus, ja ierīci nav iespējams atgūt.

“Apple” lietotāji var ieslēgt funkciju “Find My” jeb “Atrodi mani”. “Android” lietotāji var ieslēgt funkciju “Find My Device” jeb “Atrodi manu ierīci”. Šie pakalpojumi ir bez maksas un bieži vien jau ir pieejami jūsu ierīcē. Veltot dažas minūtes, lai pārbaudītu, vai šīs funkcijas ir ieslēgtas, vēlāk varat izvairīties no milzīga stresa. Ja ierīce pazūd, varat to ātri atrast vai attālināti izdzēst savu informāciju, pirms tai piekļūst kāds cits.

3. Ieslēdziet automātiskos atjauninājumus.

Kibernoziedznieki pastāvīgi meklē ievainojamības mobilajās operētājsistēmās un lietotnēs. Ja šādas ievainojamības tiek atklātas, programmatūras uzņēmumi izlaiž atjauninājumus to novēršanai. Problēma ir tā, ka daudzi cilvēki atliek atjauninājumus uz vairākām dienām, nedēļām vai pat mēnešiem. Vienkāršākais risinājums ir ieslēgt automātisko atjaunināšanu, tostarp mobilajām lietotnēm. Tas nodrošina, ka jūsu ierīce saņem "drošības ielāpus", tiklīdz tie kļūst pieejami, pārsvarā bez jebkādas rīcības no jūsu puses.

4. Instalējiet lietotnes tikai no uzticamiem avotiem

Viens no izplatītākajiem veidiem, kā mobilās ierīces tiek apdraudētas, ir ļaunprātīgas lietotnes. Lejupielādējiet mobilās lietotnes tikai no oficiālajiem lietotņu veikaliem, piemēram, “Apple App Store” vai “Google Play”. Arī tad pirms instalēšanas pārskatiet vērtējumus, atsauksmes un pieprasītās atļaujas. Īpaši piesardzīgi izturieties pret lietotnēm, kas pieprasa piekļuvi informācijai vai funkcijām, kuras tām nav nepieciešamas. Piemēram, lukturīša lietotnei nevajadzētu pieprasīt piekļuvi jūsu kontaktpersonām, mikrofonam vai atrašanās vietai. Ja lietotne šķiet aizdomīga vai pieprasa pārmērīgi plašas atļaujas, izvēlieties citu lietotni.

5. Ieslēdziet automātisko dublēšanu

Ierīces pazaudēšana rada stresu. Ja tālrunis pazūd, tiek bojāts vai salūst, nesen izveidota dublējumkopija ļauj dažās minūtēs atjaunot visu jaunā ierīcē, tostarp ne tikai visas instalētās lietotnes, bet arī to iestatījumus. Pārlicinieties, ka automātiskā dublēšana ir ieslēgta.

Viesredaktore

Dr. Kuši Gupta (Khushi Gupta) ir Ziemeļdžordžijas Universitātes kibernetikas docente. Viņai ir doktora grāds kibernetikas izmeklēšanā, viņa ir vairāk nekā 30 publikāciju autore un savā darbā izmanto pieredzi tiesībsargāšanas iestāžu kriminālistikā. Viņa darbojas kā padomdevēja “WiCyS”, “Women4Cyber” un BBWIC programmās.



Resursi

Lejupielādes briesmas: kā pārspēt ļaunprātīgas mobilās lietotnes: <https://www.sans.org/newsletters/ouch/download-danger-how-to-outwit-malicious-mobile-apps>

Teksta ziņojumapmaiņas uzbrukumi: smiķerēšanas sāga: <https://www.sans.org/newsletters/ouch/text-messaging-attacks-smishing-saga>

Kā kibernetikas nozogs jūsu paroles: <https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords>

Tulkoja: CERT.LV

OUCH! Izdod SANS Security Awareness un izplata ar [Creative Commons BY-NC-ND 4.0 licenci](https://creativecommons.org/licenses/by-nc-nd/4.0/). Jūs varat brīvi dalīties ar šo biļetenu vai izplatīt to, ja vien jūs to nepārdodat vai nepārveidojat. Redkolēģija: Fils Hofmans (Phil Hoffman), Leslija Ridauts (Leslie Ridout), Prinsesa Janga (Princess Young).

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