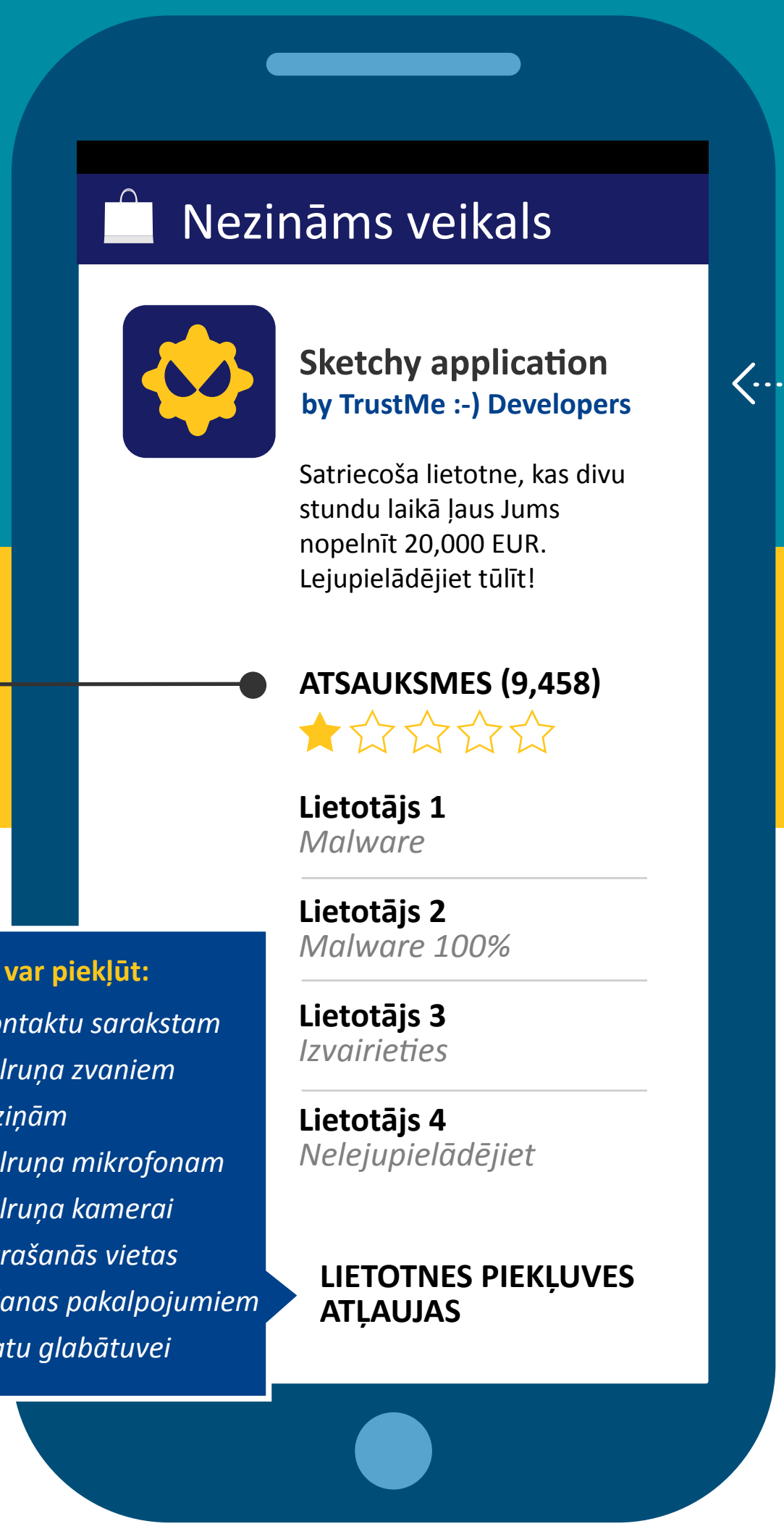
APPS

TIKAI SPĒLE?

Instalējiet lietotnes tikai no oficiāliem lietotņu veikaliem.

Pirms lietotnes lejupielādes izpētiet gan lietotni, gan tās publicētājus. Uzmanieties no saitēm, ko Jūs saņemat e-pastā, un no īsziņām, kas var ar viltu likt Jums instalēt trešo pušu lietotnes vai nezināmas izcelsmes lietotnes.



IEPAZĪSTIETIES AR CITU LIETOTĀJU ATSAUKSMĒM UN NOVĒRTĒJUMIEM

IZLASIET INFORMĀCIJU PAR LIETOTNES PIEKĻUVES ATĻAUJĀM

noskaidrojiet, kāda veida datiem lietotne var piekļūt un vai tā var kopīgot Jūsu informāciju ar trešajām pusēm. Vai ir nepieciešams tai sniegt visas šīs piekļuves atļaujas? Ja nav, neveiciet lietotnes lejupielādi.

INSTALĒJIET MOBILO IERĪČU DROŠĪBAS LIETOTNI

Tā pārbaudīs visas Jūsu ierīces lietotnes un katru jaunu lietotni, ko Jūs instalēsiet vēlāk, un brīdinās Jūs, ja tiks atklāta ļaunprogrammatūra.

EUROPOL EC3 European Cybercrime Centre

LATVIJAS VALSTS POLICIJA

#MobileMalware

MOBILĀS BANKAS ĻAUNPROGRAMMATŪRA

ĻAUNPROGRAMMATŪRA VAR RADĪT JUMS IZMAKSAS

Mobilās bankas ļaunprogrammatūra ir izstrādāta, lai nozagtu finanšu informāciju, kas glabājas Jūsu ierīcē.

KĀ TĀ TIEK IZPLATĪTA?

Ļaunprātīgas tīmekļa vietnes apmeklējuma laikā

Veicot ļaunprātīgu lietotņu lejupielādi

Pikšķerējot

KĀDI IR RISKI?

Jūsu personiskās autentifikācijas informācijas iegūšana

Prettiesiska naudas pārskaitīšana no konta

KO ES VARU DARĪT?

https://

Lejupielādējiet Jūsu bankas oficiālo mobilo lietotni un katru reizi pārliecinieties, ka Jūs apmeklējat īsto bankas tīmekļa vietni.

Ja Jūs pazaudējat savu telefonu vai nomainât numuru, sazinieties ar savu banku, lai tās darbinieki varētu atjaunināt Jūsu informāciju.

Neļaujiet savai internetbankas vietnei vai lietotnei pieteikt Jūs sistēmā automātiski.

Neizpaudiet nekāda veida informāciju par savu kontu īsziņās vai e-pastos.

Nekopīgojiet vai neatklājiet nevienam savas bankas kartes numuru vai konta paroli.

Vienmēr izmantojiet drošu Wi-Fi tīklu, lai atvērtu savas bankas mobilo vietni vai lietotni. Nekad nedariet to, izmantojot atklātu Wi-Fi tīklu.

Ja iespējams, instalējiet mobilo ierīču drošības lietotni, kas brīdinās Jūs par jebkāda veida aizdomīgu darbību.

Ik pa laikam pārbaudiet savu finanšu pārskatu.

EUROPOL EC3 European Cybercrime Centre

LATVIJAS VALSTS POLICIJA

#MobileMalware

MOBILĀ
IZSPIEDĒJPROGRAMMATŪRA

PAMĀJIET ARDIEVAS SAVIEM PERSONISKAJIEM FAILIEM

Izspiedējprogrammatūra tur Jūsu mobilo ierīci un datus gūstā, līdz iegūst atlīdzību. Šī tipa ļaunprogrammatūra nobloķē Jūsu ierīces ekrānu vai neļauj Jums piekļūt kādiem konkrētiem failiem un funkcijām.

KĀ TĀ TIEK IZPLATĪTA?

Kompromitētas tīmekļa vietnes apmeklējuma laikā.

Lejupielādējot viltotas likumīgu lietotņu versijas.

Noklikšķinot uz ļaunprātīgām saitēm un pielikumiem, kas iegulti pikšķerēšanas e-pastos.

KĀDI IR RISKI?

Var būt nepieciešams atjaunot Jūsu ierīces rūpnīcas iestatījumus, tādējādi zaudējot visus datus.

Uzbrucējs var būt ieguvis pilnīgu piekļuvi Jūsu ierīcei un var kopīgot Jūsu datus ar trešajām pusēm.

KO ES VARU DARĪT?

Ik pa laikam dublējiet savus datus un atjauniniet visas lietotnes un operētājsistēmu.

Centieties neiepirkties trešo pušu lietotņu veikalos.

Ja iespējams, instalējiet mobilo ierīču drošības lietotni, kas brīdinās, ja Jūsu ierīce būs jebkādā veidā apdraudēta.

Uzmanieties no e-pastiem un tīmekļa vietnēm, kas šķiet aizdomīgas vai ja to piedāvājumi šķiet pārāk labi, lai būtu patiesi.

Nevienam nepiešķiriet savas ierīces administratora tiesības.

Nemaksājiet izpirkšanas maksu. Tādējādi Jūs finansēsiet noziedzniekus un mudināsiet viņus turpināt veikt nelikumīgas darbības.

EUROPOL EC3 European Cybercrime Centre

LATVIJAS VALSTS POLICIJA

#MobileMalware

APDRAUDĒJUMS TĪMEKLĪ

PĀRBAUDIET DIVREIZ PIRMS KLIKŠĶINĀT

Jūsu ierīcei pārtraucot funkcionēt, Jūs varat zaudēt naudu, personisko informāciju un pat savus saglabātos datus. Neuzķerieties!

KĀ TAS VAR NOTIKT?

PIKŠĶERĒŠANAS UZBRUKUMI: Uzbrucēji izmāna no lietotājiem personisku informāciju, uzdodoties par uzticamu iestādi. Viņi izplata savus viltus paziņojumus ar e-pastu, īsziņu vai sociālo tīklu starpniecību.

TĪMEKĻA PĀRLŪKOŠANA: Jūsu mobilā ierīce var tikt inficēta, vienkārši apmeklējot nedrošas tīmekļa vietnes.

FAILU LEJUPIELĀDE: E-pastā tiešā veidā var būt iegultas ļaunprātīgas saites vai pielikumi.

KĀDĒĻ TAS IR EFEKTĪVI

Mobilās ierīces **PASTĀVĪGI IR SAVIENOTAS** ar internetu.

Galvenais ierobežojums ir **IERĪCES EKRĀNA SAMAZINĀTAIS IZMĒRS.** Mobilās pārlūkprogrammas ataino URL ierobežotā ekrāna laukā, tāpēc ir grūti saredzēt, vai domēns ir pareizs.

LIETOTĀJA NEŠAUBĪGĀ UZTICĪBA mobilās ierīces personalizētajam raksturam.

KO ES VARU DARĪT?

Uzmanieties, ja saņemat īsziņu vai tālruņa zvanu no uzņēmuma, kas lūdz atklāt personisku informāciju. Jūs varat pārbaudīt ziņas/zvana autentiskumu, tiešā veidā piezvanot uzņēmumam pa oficiālo tālruņa numuru.

Pārlūkojot tīmekli savā mobilajā ierīcē, pārliecinieties, ka Jūsu savienojuma drošību garantē HTTPS. Jūs to vienmēr varat pārbaudīt URL sākumā.

Nekādā gadījumā neatveriet saiti/pielikumu nevēlamā e-pastā vai īsziņā. Nekavējoties izdzēsiet to.

Uzmanieties, ja nokļūstat vietnē, kuras teksts sastāv no gramatikas un pareizrakstības kļūdām vai kura tiek atainota zemā izšķirtspējā.

Ja iespējams, instalējiet mobilo ierīču drošības lietotni, kas brīdinās Jūs par jebkāda veida aizdomīgu darbību.

EUROPOL EC3 European Cybercrime Centre

LATVIJAS VALSTS POLICIJA

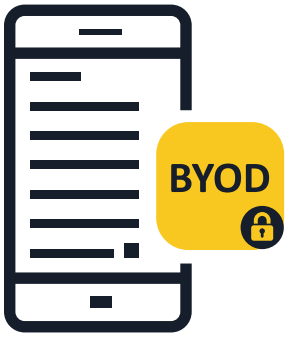
#MobileMalware

MOBILO IERĪČU ĻAUNPROGRAMMATŪRA

PADOMI UN IETEIKUMI UZŅĒMUMIEM

1 Informējiet savus darbiniekus par riskiem, kas saistīti ar mobilo ierīču drošību

- Darbā izmantojot mobilās ierīces, tiek izpludinātas robežas starp šo ierīču lietošanu darba un privātajām vajadzībām. Uzņēmumu darbību var ievērojami ietekmēt uzbrukums, kas ticis sākotnēji veikts konkrētas personas mobilajai ierīcei. Mobilā ierīce ir dators, tāpēc tai ir jānodrošina attiecīga aizsardzība.



2 Ieviesiet uzņēmuma darbinieku personisko ierīču izmantošanas (bring-your-own-device (BYOD)) politiku

- Darbiniekiem, kuri izmanto savas personiskās ierīces, lai piekļūtu uzņēmuma datiem un sistēmām (pat ja tas ir tikai e-pasts, kalendārs vai kontaktpersonu datu bāze), ir jāievēro uzņēmuma politika. Uzmanīgi izvēlieties, kuras tehnoloģijas tiks izmantotas, lai pārvaldītu un padarītu drošas mobilās ierīces, un iesakiet saviem darbiniekiem ievērot piesardzību.

3 Savā vispārīgajā drošības sistēmā iekļaujiet mobilo ierīču drošības politikas

- Ja ierīce neatbilst drošības politiku prasībām, to nedrīkst atļaut pievienot uzņēmuma tīklam un tai nedrīkst atļaut piekļūt uzņēmuma datiem. Uzņēmumiem ir jāievieš savi Mobile Device Management (mobilo ierīču pārvaldības) (MDM) vai Enterprise Mobility Management (uzņēmumu mobilitātes pārvaldības) (EMM) risinājumi.
- Papildus tam noteikti ir jāinstalē aizsardzības risinājumi pret mobilo ierīču apdraudējumu. Tādējādi tiks nodrošināta lietotņu, tīkla un operētājsistēmas apdraudējuma līmeņa redzamība un kontekstuālā izpratne.

4 Ievērojiet piesardzību, izmantojot publiski pieejamos Wi-Fi tīklus, lai piekļūtu uzņēmuma datiem

- Kopumā publiski pieejamie Wi-Fi tīkli nav droši. Darbiniekam lidostā vai kafejnīcā piekļūstot uzņēmuma datiem ar Wi-Fi tīkla savienojuma starpniecību, dati var tikt atklāti ļaunprātīgiem lietotājiem. Uzņēmumiem ir ieteicams šajā sakarā izstrādāt „efektīvas izmantošanas” politikas.

5 Vienmēr atjauniniet ierīces operētājsistēmu un lietotnes

- Iesakiet saviem darbiniekiem lejupielādēt viņu mobilo ierīču operētājsistēmas programmatūras atjauninājumus, tiklīdz viņiem tas tiek lūgts. Īpaši attiecībā uz Android — iepazīstieties ar mobilo sakaru operatoru un tālruņu ražotāju atjauninājumu politiku. Pēdējie atjauninājumi nodrošinās, ka ierīce ir ne vien daudz drošāka, bet ka ir uzlabots arī tās sniegums.

6 Instalējiet lietotnes vienīgi no uzticamiem avotiem

- Uzņēmumiem tādās mobilajās ierīcēs, kas tiek pieslēgtas uzņēmuma tīklam, būtu jāļauj instalēt lietotnes tikai no oficiāliem avotiem. Vai arī apsveriet izveidot uzņēmuma lietotņu veikalu, ar kura starpniecību galalietotāji var piekļūt lietotnēm un lejupielādēt un instalēt lietotnes, kuras ir akceptējis uzņēmums. Konsultējieties ar savu drošības risinājumu nodrošinātāju, lai saņemtu padomu par šāda veikala izveidi, vai arī izveidojiet to uzņēmuma iekšienē.

7 Nepieļaujiet ierīces drošības uzstādījumu rediģēšanu

- Drošības uzstādījumu rediģēšana ir operētājsistēmas izplatītāja uzstādīto drošības ierobežojumu atcelšanas process, kas nodrošina pilnīgu piekļuvi operētājsistēmai un tās funkcijām. Jūsu ierīces drošības uzstādījumu rediģēšana var ievērojami samazināt tās aizsardzību, atklājot drošības caurumus, kas iepriekš nebija skaidri saredzami. Uzņēmuma vidē nedrīkst izmantot ierīces, kuru lietotājiem ir piešķirtas administratora (Root) tiesības.

8 Apsveriet mākoņkrātuves izmantošanu

- Mobilo ierīču lietotāji bieži vien vēlas piekļūt svarīgiem dokumentiem ne vien ar darba datoru starpniecību, bet arī ar privāto tālruņu vai planšetdatoru starpniecību, atrodoties ārpus biroja. Uzņēmumiem ir jāapsver drošas mākoņkrātuves izveide un failu sinhronizēšanas pakalpojumu nodrošināšana, lai izpildītu šīs prasības drošā veidā.

9 Iedrošiniet savus darbiniekus instalēt mobilo ierīču drošības lietotni

- Visas operētājsistēmas ir pakļautas inficēšanās riskam. Ja iespējams, pārliecinieties, ka viņi izmanto mobilo ierīču drošības risinājumu, kas atklāj ļaunprogrammatūras, spiegprogrammatūras un ļaunprātīgas lietotnes un pasargā no tām, kā arī citas privātuma aizsardzības un zādzību novēršanas funkcijas.

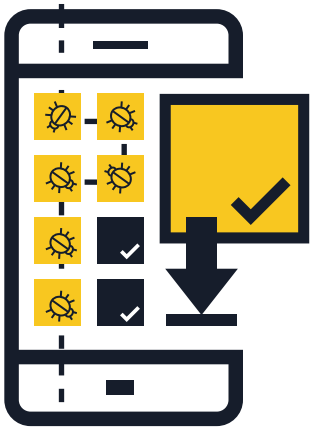
EUROPOL EC3 European Cybercrime Centre

LATVIJAS VALSTS POLICIJA

#MobileMalware

MOBILO IERĪČU ĻAUNPROGRAMMATŪRA

PADOMI UN IETEIKUMI, KĀ SEVI PASARGĀT

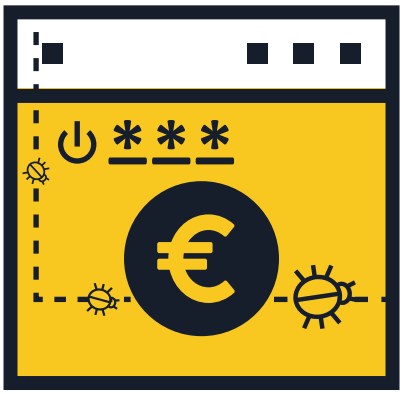


1 Instalējiet lietotnes vienīgi no uzticamiem avotiem

- **Iepērcieties respektablos lietotņu veikalos** — pirms lietotnes lejupielādes izpētiet gan lietotni, gan tās publicētājus. Uzmanieties no saitēm, ko Jūs saņemat e-pastā, un no īsziņām, kas var ar viltu likt Jums instalēt trešo pušu lietotnes vai nezināmas izcelsmes lietotnes.
- **Iepazīstieties ar citu lietotāju atsauksmēm un novērtējumiem,** ja pieejami.
- **Izlasiet informāciju par lietotnes piekļuves atļaujām** — noskaidrojiet, kāda veida datiem lietotne var piekļūt un vai tā var kopīgot Jūsu informāciju ar trešajām pusēm. Ja noteikumi Jums šķiet aizdomīgi vai tie Jūs neapmierina, neveiciet lietotnes lejupielādi.

2 Neklikšķiniet uz saitēm vai pielikumiem, kas pievienoti nevēlamiem e-pastiem vai īsziņām

- **Neuzticieties saitēm, kas iekļautas nevēlamos e-pastos vai īsziņās** (SMS un MMS) — izdzēsiet tos, tiklīdz tādus saņemat.
- **Rūpīgi pārbaudiet saīsinātus URL un QR kodus** — tie var aizvest uz kaitīgām tīmekļa vietnēm vai tiešā veidā Jūsu ierīcē lejupielādēt ļaunprogrammatūru. Pirms to atvēršanas izmantojiet URL priekšskatījuma vietnes, lai pārliecinātos, ka tīmekļa adrese ir pareiza. Pirms QR koda skenēšanas izvēlieties QR kodu lasītāju, kas priekšskata iegulto tīmekļa adresi, un izmantojiet mobilo tālruņu drošības lietojumprogrammas, kas brīdina par riskantām saitēm.



3 Izejiet no vietnēm, kad ir veikts maksājums

- **Nekādā gadījumā nesaglabājiet savus lietotājvārdus un paroles mobilās ierīces pārlūkprogrammā vai lietotnē** — ja Jūsu tālrunis vai planšetdators tiks pazaudēts vai nozagts, ikviens varēs ieiet Jūsu kontos. Kad transakcija ir pabeigta, izejiet no vietnes, nevis vienkārši aizveriet pārlūkprogrammu.
- **Nelietojiet internetbanku vai neiepērcieties tiešsaistē, izmantojot publiski pieejamu Wi-Fi tīkla savienojumu** — internetbankas lietošanai vai transakciju veikšanai izmantojiet vienīgi interneta tīklus, kurus Jūs zināt un kuriem uzticaties.
- **Rūpīgi pārbaudiet vietnes URL** — pirms pieteikšanās sistēmā vai sensitīvas informācijas nosūtīšanas pārliecinieties, ka tīmekļa adrese ir pareiza. Apsveriet Jūsu bankas oficiālās lietotnes lejupielādi, lai nodrošinātu, ka Jūs vienmēr piekļūstat īstajai vietnei.

4 Vienmēr atjauniniet savas mobilās ierīces operētājsistēmu un lietotnes

- **Lejupielādējiet Jūsu mobilās ierīces operētājsistēmas programmatūras atjauninājumus, tiklīdz Jums tas tiek lūgts** — pēdējie atjauninājumi nodrošinās, ka Jūsu ierīce ir ne vien daudz drošāka, bet ka ir uzlabots arī tās sniegums.

5 Izslēdziet Wi-Fi tīkla savienojumu, atrašanās vietas noteikšanas pakalpojumus un Bluetooth, kad tie netiek izmantoti

- **Atslēdziet Wi-Fi tīkla savienojumu, ja to neizmantojat** — ja savienojums nav drošs, Jūsu informācijai var piekļūt kibernoziedznieki. Ja iespējams, tīklāju vietā izmantojiet 3G vai 4G datu savienojumu. Jūs varat izvēlēties arī virtuālā privātā tīkla (VPN) pakalpojumu, lai Jūsu dati pārsūtīšanas laikā tiktu šifrēti.
- **Neļaujiet lietotnēm izmantot atrašanās vietas noteikšanas pakalpojumus, ja vien tas nav nepieciešams** — šī informācija var tikt kopīgota vai nopludināta un izmantota, lai uzspiestu ar Jūsu atrašanās vietu saistītas reklāmas.
- **Atslēdziet Bluetooth savienojumu, kad Jums tas nav nepieciešams** — pārliecinieties, ka tas ir pilnībā atslēgts, nevis tam ir tikai iestatīts neredzamības režīms. Noklusējuma iestatījumi bieži vien ir iepriekšiestatīti tā, lai ļautu citiem pieslēgties Jūsu ierīcei, Jums to nezinot. Ļaunprātīgi lietotāji potenciāli var nokopēt Jūsu failus, piekļūt citām pievienotajām ierīcēm vai pat iegūt pilnīgu Jūsu mobilā tālruņa vadību, lai veiktu zvanus un sūtītu īsziņas, kā rezultātā Jūs saņemat izmaksu ziņā iespaidīgus rēķinus.

6 Izvairieties atklāt personīgu informāciju

- **Nekādā gadījumā nesūtiet personisku informāciju,** atbildot uz īsziņām vai e-pastiem, kas it kā ir sūtīti no Jūsu bankas vai cita likumīga uzņēmuma. Tā vietā tiešā veidā sazinieties ar uzņēmumu, lai apstiprinātu šādas informācijas pieprasījumu.
- **Regulāri pārskatiet savu mobilo ierīču rēķinu pārskatus, lai pārliecinātos, ka tajos nav iekļautas nekāda veida aizdomīgas maksas** — ja atklājat izdevumus, kurus neesat veicis/-kusi, nekavējoties sazinieties ar savu pakalpojumu sniedzēju.

7 Nerediģējiet savas ierīces drošības uzstādījumus

- Drošības uzstādījumu rediģēšana ir operētājsistēmas izplatītāja uzstādīto drošības ierobežojumu atcelšanas process, kas nodrošina pilnīgu piekļuvi operētājsistēmai un tās funkcijām — **Jūsu ierīces drošības uzstādījumu rediģēšana var ievērojami samazināt tās aizsardzību,** atklājot drošības caurumus, kas iepriekš nebija skaidri saredzami.

8 Dublējiet savus datus

- **Daudzi viedtālruņi un planšetdatori ir aprīkoti ar iespēju dublēt datus bezvadu tīklā** — skatiet opcijas, kas ir atkarīgas no Jūsu ierīces operētājsistēmas. Dublējot sava viedtālruņa vai planšetdatora datus, Jūs varat viegli atjaunot savus personiskos datus gadījumos, kad Jūsu ierīce tiek pazaudēta, nozagta vai bojāta.

9 Instalējiet mobilo ierīču drošības lietotni

- Visas operētājsistēmas ir pakļautas inficēšanās riskam. Ja iespējams, **izmantojiet mobilo ierīču drošības risinājumu,** kas atklāj ļaunprogrammatūras, spiegprogrammatūras un ļaunprātīgas lietotnes un pasargā no tām, kā arī citas privātuma aizsardzības un zādzību novēršanas funkcijas.

EUROPOL EC3 European Cybercrime Centre

LATVIJAS VALSTS POLICIJA

#MobileMalware