

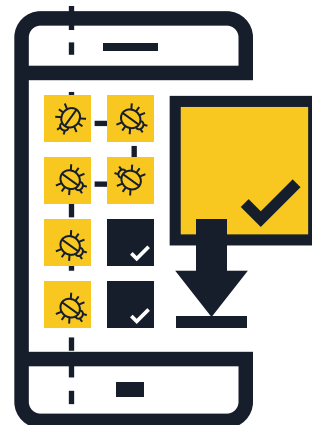
MOBILO IERĪČU ĻAUNPROGRAMMATŪRA

PADOMI UN IETEIKUMI, KĀ SEVI PASARGĀT



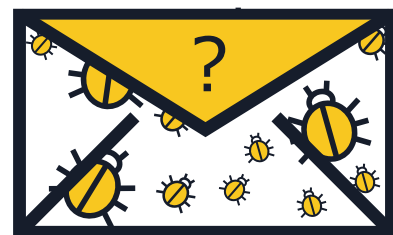
1 Instalējiet lietotnes vienīgi no uzticamiem avotiem

- **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.



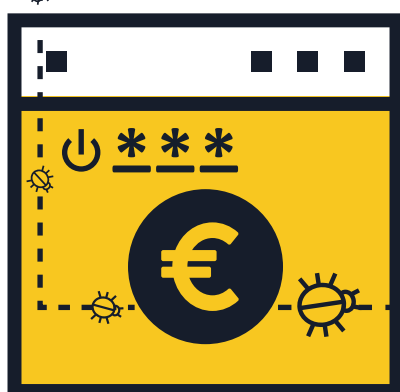
2 Neklikšķiniet uz saitēm vai pielikumiem, kas pievienoti nevēlamiem e-pastiem vai īsziņām

- **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 pārlicinātos, ka tīmekļa adrese ir pareiza. Pirms QR koda skenēšanas izvēlieties QR kodu lasītāju, kas priekšskata iegulto tīmekļa adresi, un izmantojiet mobilo tālrunu drošības lietojumprogrammas, kas brīdina par riskantām saitēm.



3 Izejiet no vietnēm, kad ir veikts maksājums

- **Nekādā gadījumā nesaglabājiēt savus lietotājevārdus 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 pārlicinieties, ka tīmekļa adrese ir pareiza. Apsveriet Jūsu bankas oficiālās lietotnes lejupielādi, lai nodrošinātu, ka Jūs vienmēr piekļūstat īstajai vietai.



4 Vienmēr atjauniniet savas mobilās ierīces operētājsistēmu un lietotnes

- **Lejupielādējiēt 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.

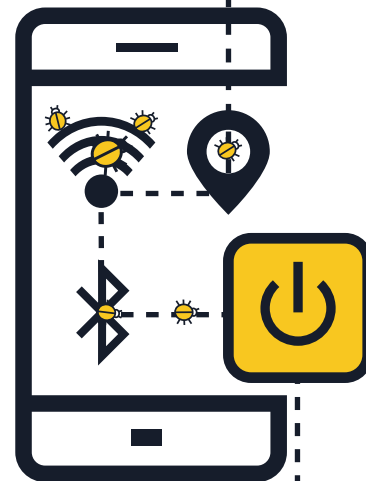


5 Izslēdziet Wi-Fi tīkla savienojumu, atrašanās vietas noteikšanas pakalpojumus un Bluetooth, kad tie netiek izmantoti

■ **Atslēdziet Wi-Fi tīkla savienojumu, ja to neizmantojat** — ja savienojums nav drošs, Jūsu informācijai var piekļūt kibernetiziedznieki. 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 iepriekš iestatīti 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, spieģelprogrammatūras un ļaunprātīgas lietotnes un pasargā no tām, kā arī citas privātuma aizsardzības un zādzību novēršanas funkcijas.

