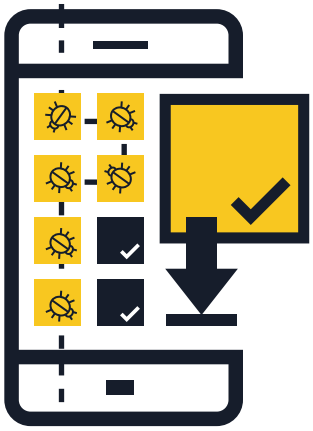
# MOBILNA ŠKODLJIVA KODA

## UPORABNI NASVETI ZA VAŠO ZAŠČITO



## 1 Aplikacije namestite samo iz virov, ki jim zaupate

- **Kupujte v preverjenih trgovinah z aplikacijami.** — Pred prenosom aplikacije preverite verodostojnost same aplikacije in njenih izdajateljev. Bodite previdni pri linkih oziroma spletnih povezavah, ki jih prejmete v elektronskih in tekstovnih sporočilih, saj vas lahko napeljejo k namestitvi aplikacij dvomljivega ali neznanega vira.
- **Preglejte mnenja in ocene drugih uporabnikov,** če so na voljo.
- **Preberite navodila, ki se nanašajo na dovoljenja aplikacij.** — Preverite, do katerih vrst podatkov lahko aplikacija dostopa in ali lahko deli vaše informacije z zunanjimi osebami. Če se vam pogoji zdijo sumljivi ali se z njimi ne strinjate, aplikacije ne prenesite.

## 2 Ne kliknite linkov oziroma spletnih povezav ali priponk v nezaželenih elektronskih ali tekstovnih sporočilih.


- **Ne zaupajte linkom oziroma spletnim povezavam v nezaželenih elektronskih ali tekstovnih sporočilih** (SMS in MMS). – Izbrišite jih takoj, ko jih prejmete.
- **Dobro preverite skrajšane naslove URL in kode QR.** — Lahko vas preusmerijo na nepreverjena spletna mesta ali neposredno prenesejo zlonamerno programsko opremo na vašo napravo. Preden kliknete, uporabite stran za preverjanje naslova URL, da potrdite, ali je spletni naslov verodostojen. Pred odčitavanjem kode QR izberite bralnik kod QR s preverjanjem spletnih naslovov in uporabite mobilno varnostno programsko opremo, ki vas opozori na nepreverjene in tvegane linke oziroma spletne povezave.

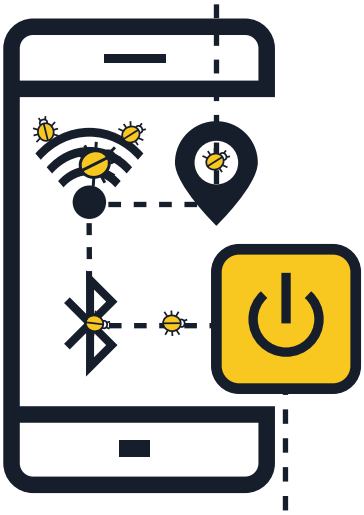
## 3 Po opravljenem plačilu se odjavite s spletnega mesta

- **Uporabniških imen in gesel nikoli ne shranite v svoj mobilni brskalnik ali aplikacijo.** — Če telefon ali tablični računalnik izgubite ali vam ga kdo ukrade, se lahko vsakdo prijavi v vaše račune. Po zaključku transakcije se najprej odjavite s spletnega mesta in šele nato zaprite brskalnik.
- **Ne uporabljajte spletne banke ali nakupujte po spletu prek javnih omrežij Wi-Fi.** — Spletno bančništvo in transakcije opravljajte samo v zaupanja vrednih omrežjih, ki jih poznate in jim zaupate.
- **Dobro preverite URL spletnega mesta.** — Zagotovite, da je spletni naslov pravilen, preden se prijavite ali pošiljate občutljive informacije. Premislite o prenosu uradne aplikacije svoje banke in tako zagotovite, da se boste vedno povezali na pravo spletno mesto.

## 4 Posodabljajte operacijski sistem in aplikacije

- **Prenesite posodobitve programske opreme za operacijski sistem svoje mobilne naprave, takoj ko vas naprava pozove, da to storite.** — Najnovejše posodobitve vam bodo zagotovile, da bo vaša naprava varna in bo bolje delovala.

## 5 Izklopite Wi-Fi, lokacijske storitve in povezavo Bluetooth, ko jih ne uporabljate



■ **Izklopite Wi-Fi, če ga ne uporabljate.** — Spletni kriminalci lahko dostopajo do vaših informacij, če povezava ni varna. Če je možno, namesto dostopnih točk uporabite podatkovno povezavo 3G ali 4G. Prav tako se lahko odločite za storitev navideznega zasebnega omrežja (VPN), da vaši podatki med prenosom ostanejo šifrirani.

■ **Ne dovolite, da bi aplikacije uporabljale vaše lokacijske storitve, razen če jih morajo.** — Te informacije so lahko uporabljene za skupno rabo ali pa razkrite in uporabljene za vsiljevanje oglasov na podlagi vašega prebivališča.

■ **Izklopite povezavo Bluetooth, ko je ne potrebujete.** — Zagotovite, da je povsem izklopljena, ne pa samo v nevidnem načinu. Privzete nastavitve so pogosto prednastavljene tako, da drugim omogočajo povezavo na vašo napravo brez vašega vedenja. Zlonamerni uporabniki bi lahko kopirali vaše datoteke, dostopali do drugih povezanih naprav ali celo pridobili oddaljen dostop do vašega telefona za klicanje in pošiljanje tekstovnih sporočil, zaradi česar bi lahko vi dobili visok račun.

## 6 Izogibajte se posredovanju osebnih podatkov

■ **Nikoli ne odgovarjajte z osebnimi podatki** na tekstovna ali elektronska sporočila, v katerih pošiljatelj trdi, da prihaja z vaše banke ali drugega zakonitega poslovnega subjekta. Namesto tega se obrnite neposredno na podjetje, da potrdite njihov zahtevek.

■ **Redno preverjajte svoje mobilne račune, da boste lahko opazili morebitne sumljive stroške.** — Če ugotovite, da imate stroške, ki jih niste povzročili vi, se takoj obrnite na ponudnika storitev.

## 7 Na svoji napravi ne izvajajte t. i. jailbreakinga

■ »Jailbreaking« je postopek odstranjevanja varnostnih omejitev, ki jih je uvedel prodajalec operacijskega sistema, s čimer dobite popoln dostop do operacijskega sistema in funkcij. **Izvajanje »jailbreakinga« na vaši napravi lahko znatno zmanjša njeno varnost in** razkrije pomanjkljivosti varnostnega sistema, ki niso bile takoj razvidne.

## 8 Varnostno kopirajte podatke

■ **Veliko pametnih telefonov in tabličnih računalnikov ima zmožnost brezžičnega varnostnega kopiranja podatkov.** — Posvetujte se glede možnosti, ki so odvisne od operacijskega sistema naprave. Z ustvarjanjem varnostne kopije pametnega telefona ali tabličnega računalnika lahko preprosto obnovite svoje osebne podatke, če napravo izgubite, vam jo ukradejo ali se poškoduje.

## 9 Namestite aplikacijo za mobilno varnost

■ Vsi operacijski sistemi lahko dobijo virus. Če je na voljo, **uporabite rešitev mobilne varnosti,** ki zazna in preprečuje zlonamerno programsko opremo, vohunsko programsko opremo in zlonamerne aplikacije poleg drugih funkcij zagotavljanja zasebnosti in protivdornih funkcij.