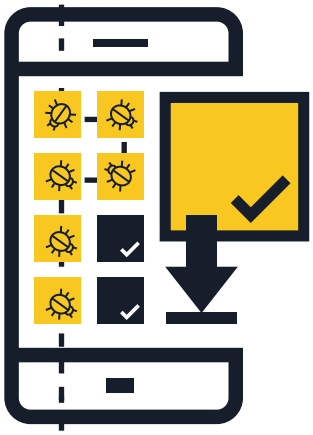
ZLONAMJERNI PROGRAMI ZA MOBILNE UREĐAJE

KORISNI SAVJETI ZA ZAŠTITU



1 Instalirajte aplikacije samo s provjerenih izvora

- **Kupujte u trgovinama aplikacija s dobrom reputacijom** — Prije preuzimanja aplikacije, istražite i aplikaciju i njene izdavače. Pazite na web-poveznice koje dobivate u porukama e-pošte i SMS porukama koje vas mogu prevariti da instalirate aplikacije treće strane ili iz nepoznatih izvora.
- **Provjerite recenzije i ocjene drugih korisnika** ako su dostupne.
- **Pročitajte dopuštenja aplikacije** — Provjerite kojim vrstama podataka aplikacija može pristupati te dijeli li vaše informacije s vanjskim stranama. Ako ste sumnjičavi oko uvjeta ili vam oni izazivaju nelagodu, nemojte preuzimati aplikaciju.

2 Nemojte klikati web-poveznice ili privitke u neželjenim porukama e-pošte ili SMS porukama

- **Nemojte vjerovati web-poveznicama u neželjenim porukama e-pošte ili u tekstualnim porukama** (SMS i MMS) — Izbrišite ih čim ih primite.
- **Dvaput provjerite skraćene URL adrese ili QR kodove** — mogli bi vas odvesti na štetna web-mjesta ili vas navesti da izravno preuzmete zlonamjerni softver na svoj uređaj. Prije klika na web-poveznicu, upotrijebite pretpregled web-mjesta URL-a kako biste potvrdili da je web-adresa legitimna. Prije skeniranja QR koda, odaberite QR čitač koji obavlja pretpregled ugrađenih web-adresa te koristi softver za sigurnost mobitela koji vas upozorava na riskantne internetske veze.

3 Odjavite se s web-mjesta nakon obavljene kupnje

- **Nikada nemojte korisnička imena i lozinke pohranjivati u mobilnom pregledniku ili u aplikacijama** — ako mobilni telefon ili tablet izgubite, svatko se može prijaviti u vaše račune. Nakon završetka transakcije, odjavite se s web-mjesta umjesto da samo zatvorite preglednik.
- **Nemojte obavljati bankovne transakcije ili internetske kupnje koristeći javne Wi-Fi veze** — Mrežno bankarstvo i transakcije koristite samo na mrežama koje poznajete i kojima vjerujete.
- **Dvaput provjerite URL web-mjesta** — provjerite je li web-adresa ispravna prije prijave ili slanja osjetljivih informacija. Preuzmite službene aplikacije banke kako biste bili sigurni da se uvijek povezujete na stvarno web-mjesto.

4 Ažurirajte operacijski sustav i aplikacije

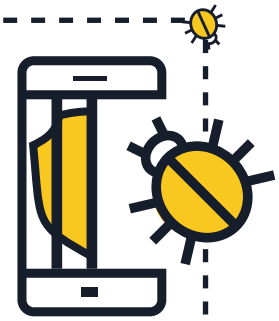
- **Preuzmite softverska ažuriranja za operacijski sustav svog mobilnog uređaja čim se to od vas zatraži** — najnovija ažuriranja omogućit će veću sigurnost vašeg uređaja i pomoći mu da radi bolje.

5 Isključite Wi-Fi, lokacijske usluge i Bluetooth kada ih ne upotrebljavate

- **Isključite Wi-Fi mrežu kada je ne upotrebljavate** — cyber kriminalci mogu pristupiti vašim podacima ako veza nije sigurna. Ako je moguće, umjesto povezivanja preko "hotspota", birajte 3G ili 4G podatkovnu vezu. Možete se odlučiti i za uslugu virtualne privatne mreže (VPN) da bi vaši podaci ostali kriptirani u prijenosu.
- **Nemojte aplikacijama dopustiti da koriste vaše lokacijske servise ako to nije nužno** — ta vrsta informacija može se dijeliti ili „procuriti" pa koristiti za guranje oglasa temeljem vaše lokacije.
- **Isključite Bluetooth kada vam nije potreban** — pazite da bude posve isključen, a ne samo u nevidljivom načinu rada. Zadane su postavke često unaprijed podešene tako da drugima dopuštaju povezivanje s vašim uređajem bez vašeg znanja. Zlonamjerni korisnici mogu potencijalno kopirati vaše datoteke, pristupiti drugim povezanim uređajima, ili čak ostvariti daljinski pristup vašem telefonu kako bi pozivali i slali tekstualne poruke, što za posljedicu ima visoke račune.

6 Izbjegavajte odavanje osobnih informacija

- **Nikad nemojte odgovarati osobnim informacijama** na tekstaulne poruke ili poruke e-pošte koje tvrde da dolaze iz vaše banke ili drugog legalnog poslovnog subjekta. Umjesto toga izravno kontaktirajte taj poslovni subjekt i potvrdite njihov zahtjev.
- **Redovno pregledavajte svoje račune za mobitel kako biste utvrdili sve sumnjive troškove** — ako otkrijete troškove koje niste počinili, odmah se obratite svojem davatelju usluga.



7 Nemojte „otvarati" ('jailbreak' postupak) svoj uređaj

- „Otvaranje" je postupak uklanjanja sigurnosnih ograničenja koja nameće davatelj operacijskog sustava kako bi se dobio potpun pristup operacijskom sustavu i značajkama. — **Otvaranje uređaja može značajno oslabiti njegovu sigurnost i** otvoriti sigurnosne rupe koje možda nisu bile vidljive.

8 Stvarajte sigurnosne kopije svojih podataka

- **Mnogi pametni telefoni i tableti imaju mogućnost bežičnog stvaranja sigurnosnih kopija** — provjerite mogućnosti ovisno o operacijskom sustavu svojeg uređaja. Stvarajući sigurnosnu kopiju za svoj pametni telefon ili tablet možete jednostavno povratiti osobne podatke ako se uređaj ikada izgubi, ukrade ili ošteti.

9 Instalirajte aplikaciju za mobilnu sigurnost

- Svi operacijski sustavi podložni su riziku od zaraze. Ako je dostupno, **koristite rješenje za mobilnu sigurnost** koje otkriva i sprječava zlonamjerne programe, špijunski softver i zlonamjerne aplikacije, uz druge značajke zaštite privatnosti i zaštite od krađe.

EUROPOL EC3 European Cybercrime Centre

ERSTE Bank

#MobileMalware