SAMO IGRA?

Instalirajte aplikacije samo sa službenih trgovina aplikacijama.

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

PROČITAJTE DOPUŠTENJA APLIKACIJE

Provjerite kojim vrstama podataka aplikacija može pristupati te dijeli li vaše informacije s vanjskim stranama. Jesu li aplikaciji potrebna sva ta dopuštenja? Ako nisu, nemojte je preuzeti.

INSTALIRAJTE APLIKACIJU ZA MOBILNU SIGURNOST

Ona će pregledati sve aplikacije na vašem uređaju i svaku novu koju naknadno instalirate te vas obavijestiti ako pronađe zlonamjerni softver.

EUROPOL EC3 | European Cybercrime Centre

REPUBLIKA HRVATSKA MUP

HRVATSKA UDRUGA BANAKA GIU

#MobileMalware

ZLONAMJERNI SOFTVER
ZA MOBILNO BANKARSTVO

ZLONAMJERNI SOFTVER MOŽE VAS KOŠTATI

Zlonamjerni softver za mobilno bankarstvo napravljen je za krađu financijskih informacija pohranjenih na vašem uređaju.

KAKO SE ŠIRI?

- Posjećivanjem zlonamjernih web-mjesta
- Preuzimanjem zlonamjernih aplikacija
- Krađom identiteta

KOJI SU RIZICI?

- Snimanje osobnih informacija za potvrdu autentičnosti
- Neovlašteno podizanje gotovine

ŠTO MOŽETE UČINITI?

- Preuzmite službenu mobilnu aplikaciju svoje banke i pazite da svaki puta posjećujete stvarnu web-lokaciju banke. (https://)
- Nemojte dopustiti da vas web-stranica ili aplikacija za bankarstvo automatski prijavljuju.
- Ni sa kim nemojte dijeliti ili otkrivati broj bankovne kartice ili lozinku.
- Ako je dostupno, instalirajte aplikaciju za mobilnu sigurnost koja će vas upozoriti na svaku sumnjivu aktivnost.
- Ako izgubite mobilni telefon ili promijenite broj, obratite se banci kako bi oni mogli ažurirati vaše informacije.
- Informacije o svojem računu nemojte dijeliti putem tekstualne poruke ili poruke e-pošte.
- Kada se povezujete s bankovnom web-stranicom ili aplikacijom, uvijek koristite sigurnu Wi-Fi mrežu. Nemojte to nikada činiti s otvorene Wi-Fi mreže!
- Često provjeravajte svoje financijske izvatke.

EUROPOL EC3 European Cybercrime Centre

HRVATSKA UDRUGA BANAKA

#MobileMalware

MOBILNI SOFTVER
KOJI TRAŽI OTKUPNINU

POZDRAVITE SE S OSOBNIM DATOTEKAMA

Softver koji traži otkup drži vaš uređaj i podatke kao taoce i postavlja cijenu. Ova vrsta zlonamjernog softvera zaključava zaslon vašeg uređaja i sprječava pristup nekim datotekama i značajkama.

KAKO SE ŠIRI?

Posjetom ugroženim web-mjestima.

Preuzimanjem lažnih verzija legitimnih aplikacija.

Klikom na zlonamjerne web-poveznice i privitke ugrađene u poruke e-pošte koje kradu identitet.

KOJI SU RIZICI?

Morate uređaj vratiti na tvorničke postavke i tako izgubiti sve podatke.

Napadač može dobiti potpun pristup vašem uređaju i podijeliti vaše podatke s trećim stranama.

ŠTO MOŽETE UČINITI?

Često stvarajte sigurnosne kopije podataka i ažurirajte aplikacije i operativni sustav.

Izbjegavajte kupnju u trgovinama aplikacija treće strane.

Ako je dostupno, instalirajte aplikaciju za mobilnu sigurnost koja će vas upozoriti ako vam je uređaj ugrožen.

Čuvajte se poruka e-pošte i web-mjesta koja izgledaju sumnjivo ili djeluju predobro da bi bila istinita.

Nikome nemojte davati administratorske ovlasti.

Nemojte plaćati otkupninu. Financirat ćete kriminalce i ohrabriti ih da nastave sa svojim protuzakonitim aktivnostima.

EUROPOL EC3 European Cybercrime Centre

HRVATSKA UDRUGA GIU BANAKA

#MobileMalware

WI-FI PRIJETNJE

BESPLATNA WI-FI MREŽA? MOGLI BISTE JE SKUPO PLATITI

Povezivanje putem javne Wi-Fi mreže ili "hotspot-a" može ugroziti sigurnost vašeg mobilnog uređaja i informacija.

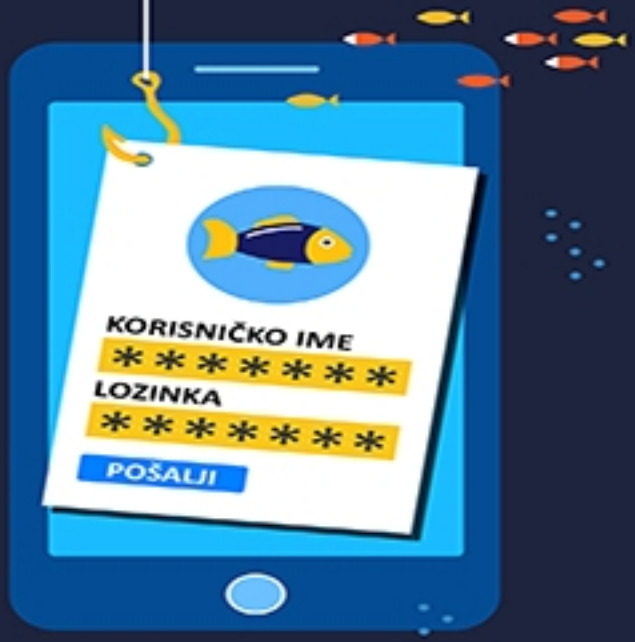
EUROPOL
EC3 European Cybercrime Centre

#MobileMalware

PRIJETNJE S WEBA

DVAPUT PROVJERITE PRIJE NEGO KLIKNETE

Mogli biste izgubiti novac, osobne informacije pa čak i pohranjene podatke ako uređaj prestane raditi.
Ne dajte se navući!



KAKO SE TO MOŽE DOGODITI?

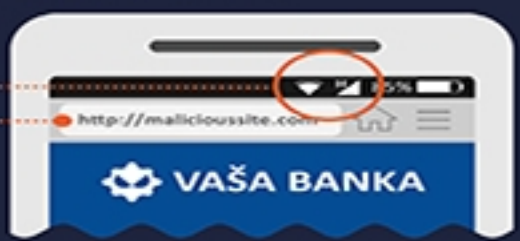
NAPADI KRAĐOM IDENTITETA: Prijevare korisnika da im oda osobne informacije pretvarajući se da su entitet od povjerenja. Šire se porukama e-pošte, SMS porukama ili platformama društvenih mreža.

PREGLEDAVANJE WEBA: Vaš se uređaj može zaraziti jednostavnim posjetom nesigurnom web-mjestu.

PREUZIMANJE DATOTEKA: Zlonamjerne web-poveznice i privici mogu biti ugrađeni u poruku e-pošte.

ZAŠTO JE UČINKOVITO?

Mobilni uređaji **NEPREKIDNO** su **SPOJENI** na internet.



SMANJENA VELIČINA ZASLONA UREĐAJA općenito je ograničenje. Mobilni preglednici prikazuju URL adrese na ograničenom prostoru zaslona, zbog čega je teško vidjeti je li domena stvarna.

Korisnik **IMPLICITNO VJERUJE** u osobnu prirodu mobilnog uređaja.

ŠTO MOŽETE UČINITI?

Budite sumnjičavi ako dobijete SMS poruku ili poziv od tvrtke koja traži vaše osobne informacije. Možete potvrditi legalnost poruke/poziva izravnim pozivom tvrtki na službeni broj.

https://

Kada pregledavate web s mobilnog uređaja, pazite da je vaša veza sigurna zahvaljujući HTTPS protokolu. Uvijek provjerite nalazi li se na početku URL adrese.

Nikad nemojte klikati web-poveznicu/privitak u neželjenoj poruci e-pošte ili SMS poruci. Odmah ih izbrišite.

^BE:%}
W@RY
*)Z#$=

Budite na oprezu ako završite na web-mjestu na kojem je vidljiva loša gramatika, pravopis ili niska razlučivost.

Ako je dostupno, instalirajte aplikaciju za mobilnu sigurnost koja će vas upozoriti na svaku sumnjivu aktivnost.

EUROPOL EC3 European Cybercrime Centre

HRVATSKA UDRUGA BANAKA

#MobileMalware

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.

ZLONAMJERNI PROGRAMI ZA MOBILNE UREĐAJE

KORISNI SAVJETI ZA TVRTKE

1 Obavijestite zaposlenike o mobilnim rizicima

- Mobilni rad zamućuje granicu između poslovne i osobne upotrebe. Tvrtke mogu pretrpjeti značajnu štetu napadom koji je inicijalno bio usmjeren na mobilni uređaj pojedinca. Mobilni uređaj je računalo i potrebno ga je zaštititi kao što štitite računala.

2 Uvedite korporativnu politiku 'donesi svoj uređaj' (Bring-Your-Own-Device, BYOD)

- Zaposlenici koji koriste svoje mobilne uređaje da bi pristupali korporativnim podacima i sustavima (čak i ako je riječ samo o bazama podataka e-pošte, kalendaru ili kontaktima), moraju slijediti pravila tvrtke. Pažljivo odaberite tehnologije koje ćete koristiti za upravljanje mobilnim uređajima i njihovo osiguravanje i uputite zaposlenike da budu oprezni.

3 Uključite pravila mobilne sigurnosti u ukupni sigurnosni okvir

- Ako uređaj nije sukladan sigurnosnim pravilima, ne bi mu se smjelo dopustiti spajanje s korporativnom mrežom te pristup korporativnim podacima. Tvrtke bi trebale implementirati rješenja za upravljanje mobilnim uređajima (MDM) ili upravljanje mobilnošću tvrtke (EMM).
- Uz to sve, ključno je instalirati rješenje za obranu od mobilnih prijetnji. To će osigurati povećanu vidljivost i kontekstualnu svijest o aplikacijama, mreži te prijetnjama na razini operacijskog sustava.

4 Budite oprezni pri korištenju javnih Wi-Fi mreža kod pristupa podacima tvrtke

- Općenito govoreći, javne Wi-Fi mreže nisu sigurne. Ako zaposlenik pristupa korporativnim podacima koristeći javnu Wi-Fi mrežu u zračnoj luci ili u kafiću, podaci mogu biti izloženi zlonamjernim korisnicima. Savjetuje se da tvrtke razviju pravila „učinkovitog korištenja" kad je o tome riječ.

ZLONAMJERNI SOFTVER
ZA MOBILNO BANKARSTVO

ZLONAMJERNI SOFTVER MOŽE VAS KOŠTATI

Zlonamjerni softver za mobilno bankarstvo napravljen je za krađu financijskih informacija pohranjenih na vašem uređaju.

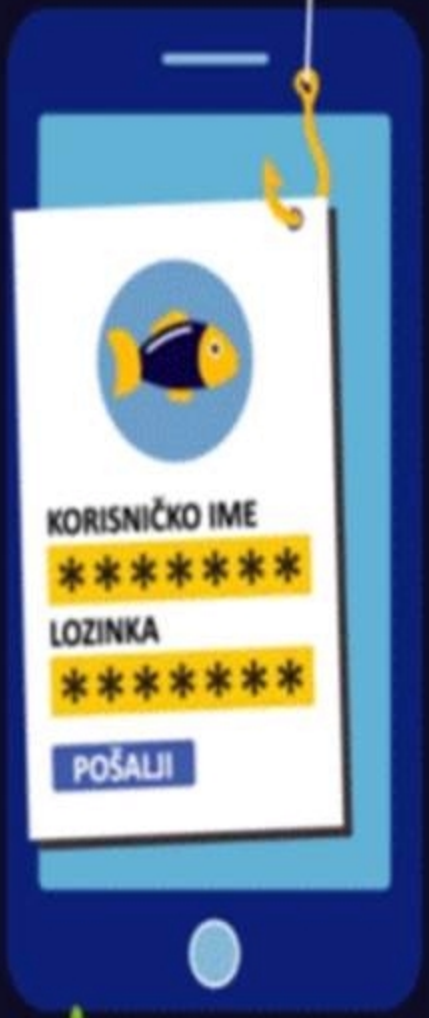
EUROPOL
EC3 | European Cybercrime Centre

#MobileMalware

PHISHING / SMISHING

DVAPUT PROVJERITE PRIJE NEGO KLIKNETE

Uvijek budite oprezni kada vas netko traži osobne informacije porukom e-pošte, SMS porukom ili telefonskim pozivom. Ne dajte se navući!



EUROPOL
EC3 | European Cybercrime Centre

#MobileMalware

SCORE 00002000 PLAYER 1 MALWARE INVADERS

APLIKACIJE

SAMO IGRA?

Instalirajte aplikacije samo sa službenih trgovina aplikacijama.

EUROPOL
EC3 | European Cybercrime Centre

#MobileMalware

MOBILNI SOFTVER KOJI TRAŽI OTKUPNINU

POZDRAVITE SE S OSOBNIM DATOTEKAMA

Ne dopustite da softver koji traži otkupninu drži vaš uređaj kao taoca.

EUROPOL
EC3 | European Cybercrime Centre

#MobileMalware