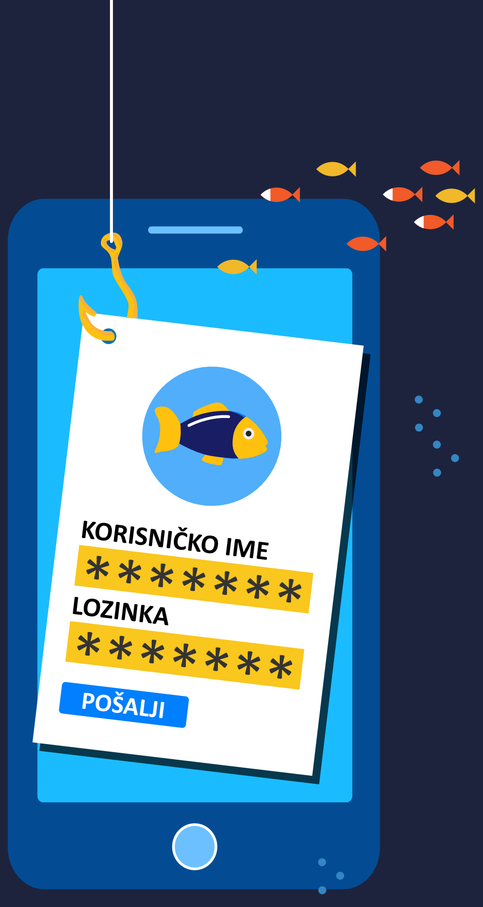
PRIJETNJE S WEBA

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

REPUBLIKA HRVATSKA MINISTARSTVO UNUTARNJIH POSLOVA MUP

HRVATSKA UDRUGA BANAKA GIU

#MobileMalware