SPLETNE NEVARNOSTI

DVAKRAT POGLEJTE, PREDEN KLIKNETE

Če naprava preneha delovati, lahko izgubite denar, osebne in celo shranjene podatke. Ne pustite se zavesti!

KAKO SE LAHKO TO ZGODI?

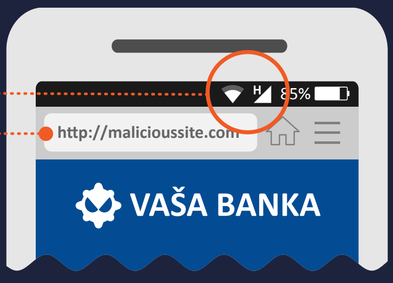
NAPADI SPLETNEGA RIBARJENJA: Prelisičijo uporabnike, da jim posredujejo osebne podatke, tako da se predstavijo kot zaupanja vreden subjekt. Širijo se po elektronskih in tekstovnih sporočilih ali okoljih družbenih in medijskih portalov.

BRSKANJE PO SPLETNIH MESTIH: Vaša mobilna naprava se lahko okuži, ko obišče nepreverjeno spletno mesto.

PRENOS DATOTEK: Zlonamerne povezave in priponke so lahko neposredno vključene v elektronsko sporočilo.

ZAKAJ JE TO UČINKOVITO?

Mobilne naprave so NENEHNO POVEZANE s spletom.



ZMANJŠANA VELIKOST ZASLONA NAPRAVE je splošna omejitev. Mobilni brskalniki prikažejo URL-je na omejenem prostoru zaslona, zato težko vidimo, ali je domena verodostojna.

IMPLICITNO ZAUPANJE UPORABNIKOV v zasebnost mobilne naprave.

KAJ LAHKO STORITE?

Bodite nezaupljivi, če prejmete SMS-sporočilo ali telefonski klic iz podjetja, ki od vas zahteva osebne podatke. Da je sporočilo/klic verodostojen, lahko preverite tako, da pokličete podjetje ali njihovo uradno številko.

https://

Med brskanjem po spletu na mobilni napravi se prepričajte, da je povezava zavarovana prek HTTPS. To lahko vedno preverite na začetku naslova URL.

Nikoli ne kliknite povezave/priponke v nezaželenem elektronskem sporočilu ali SMS-sporočilu. Takoj ga izbrišite.

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

Bodite previdni, če se znajdete na spletnem mestu s slabo slovnico, pravopisnimi napakami ali nizko ločljivostjo.

Če je na voljo aplikacija za zagotavljanja mobilne varnosti, ki vas bo opozorila na kakršno koli sumljivo aktivnost, jo namestite.

EUROPOL EC3 European Cybercrime Centre

www.varninainternetu.si

#MobileMalware