# 6 NASVETOV ZA ZAŠČITO PRED PHISHING NAPADI

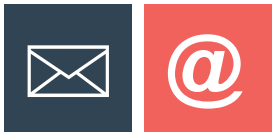
Ne glede na to, ali delate iz pisarne ali na daljavo, ste lahko vedno tarča napada v obliki socialnega inženiringa. Lažno predstavljanje (angl. phishing) je stara taktika, ki pa je še danes zelo učinkovita.

Temelji na zavajanju uporabnikov k razkritju podatkov, kot so poverilnice, podatki o kreditnih karticah in podobno, zaradi česar uporabniki mislijo, da gre za verodostojne subjekte. Lažno predstavljanje se lahko izvaja prek e-pošte, telefona, SMS-sporočil ali drugih kanalov.

**Dobra novica je, da lahko s pravim znanjem sebe in svoje podjetje zaščitimo pred lažnim predstavljanjem. Za vas smo pripravili 6 nasvetov, ki jih morate upoštevati pri vsakodnevni uporabi e-pošte in spleta:**

## 1 *E-pošta*

Ne odpirajte nezaželene e-pošte in ne odgovarjajte nanjo. Če slučajno prejmete e-pošto s priponko ali besedilno sporočilo s povezavo, ne storite ničesar, dokler ne preverite legitimnosti pošiljatelja. Ne klikajte na nobene povezave in ne uporabljajte podatkov za stik, ki so navedeni v e-pošti ali besedilu.



## 2 *Datoteke*

Prenašajte samo tiste datoteke in aplikacije, ki prihajajo iz zanesljivih in zaupanja vrednih virov. Enako velja za vtičnike brskalnikov.

## 3 *Prošnje*

Ne sprejemajte prošenj za prijateljstva, če pošiljatelja ne poznate osebno.


## 4 Klic

Klic prekinite takoj, če kdo zahteva podatke o osebnem računu prek telefona, na primer številko kreditnih kartic ali kakršne koli zaupne podatke.

## 5 Povezave

Ne klikajte na nobeno povezavo, ki jo vidite, zlasti če pride po naključni e-pošti, preko takojšnjih sporočilih ali SMS-sporočil. Vedno preletite povezave in se prepričajte, da vodijo do zanesljivega vira. Bodite pozorni na tipkarske napake v povezavah, na primer **twiter.com** namesto **twitter.com.**



## 6 Opozorila

Kadar koli se pojavi opozorilo sistema ali brskalnika, ga pozorno preberite in ustrezno ukrepajte.