

# Prepoznaj **phishing** u 6 koraka

**Phishing** - prijevara u kojoj napadač lažnim predstavljanjem i naizgled legitimnim zahtjevom pokušava potencijalnu žrtvu natjerati da učini nešto u njihovu korist.

**Najčešći ciljevi** - krađa osobnih podataka, ostvarivanje nedozvoljenog pristupa podacima, ostvarivanje financijske koristi i širenje zlonamjernog softvera.

## 01

### Lažno predstavljanje

Napadači vole imitirati institucije, sustave i usluge.

**Polje pošiljatelja može biti lažirano!**

Provjeri adresu s koje je poruka poslana i usporedi ju s kontakt informacijama navedenim na službenim stranicama.

## 02

### Nudi ti se novac ili neka druga primamljiva ponuda

Oprezno s ponudama koje izgledaju predobro da bi bile istinite. Provjeri ih na drugim mjestima i potražite komentare korisnika.

## 03

### Moraš kliknuti poveznicu ili skenirati QR kôd

Napadač će te pokušati navesti na zlonamjernu web stranicu na kojoj će te tražiti unos osobnih podataka (npr. **podataka bankovne kartice**).

Iako stranica može izgledati legitimno, ona je vjerojatno napravljena s ciljem krađe osobnih podataka.

## 04

### Izazivaju u tebi snažne osjećaje i tjeraju te na brzu reakciju

Izazivanjem snažnih emocija (npr. straha) i davanjem kratkog vremena za reakciju, napadači smanjuju sposobnost tvog kritičkog razmišljanja i tako te tjeraju na grešku.

## 05

### Sumnjivi privitak

Privitak može sadržavati **zlonamjerni kôd**. Ako nisi očekivao privitak u poruci, provjeri ostale elemente e-pošte (polje pošiljatelja, pravopis, naslov, potpis, naslov privitka i sl.).

## 06

### Traže uplatu novca ili kriptovaluta

Ne uplaćuj novac i kriptovalute osobama koje su te kontaktirale putem e-pošte, poziva ili poruke.