

# PREPOZNAJ LAŽNU ELEKTRONIČKU POŠTU



Što je *Phishing*? – Vrsta napada metodama socijalnog inženjeringa koja putem lažnih poruka navodi korisnike na preuzimanje zlonamjernih sadržaja ili odavanje osjetljivih podataka i informacija.

## POVEZNICE KOJE SE NALAZE U ELEKTRONIČKOJ POŠTI SU NAJOPASNJIJI DIO ZLONAMJERNIH PORUKA

One često sadrže lažne nazive stranica slične stvarnima kao i velik broj slova i znakova.

## POŠILJATELJI SU ČESTO PRIKAZANI LAŽNIM IMENOM KOJE JE SLIČNO STVARNOM

Promjenom samo jednog slova ili znaka kao što su to slovo O i brojka 0 korisnik vjerojatno neće primijetiti kako se radi o lažnom nazivu.

## ZASTRAŠIVANJE ILI POZIVANJE KORISNIKA NA AKCIJU U ODREĐENOM ROKU

Ovo su taktike koje koriste napadači kako bi vas naveli na poduzimanje aktivnosti.



Sistemska Podrška <support@mycrossoft.com.hr>

Vaš softver je pred istekom valjanosti

To  
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Poštovani,

Vaša verzija operativnog sustava Microsoft Office je pred istekom i moći ćete je koristiti još samo **3 dana**.

Kako bi ste zadržali pristup svojim podacima i nastavili koristiti Office paket provjerite postupak nadogradnje opisan na slijedećoj poveznici <https://mycrossoft.com.hr/office?rid=NWuxZ5C>

Lijepi pozdrav,

Support Mycrossoft

## ŠTO UČINITI KAD UOČIMO SUMNJIVU PORUKU?



1. POSTUPITI SUKLADNO  
INTERNIM PRAVILIMA I  
PROCEDURAMA TIJELA



2. PRIJAVITI KORISNIČKOJ  
PODRŠCI POJAVU PHISHING  
PORUKE



3. PRATITI NEUOBIČAJENE  
AKTIVNOSTI NA RAČUNALU I  
SUSTAVU



# PHISHING

**Što je Phishing?** – Vrsta napada metodama socijalnog inženjeringa koja putem lažnih poruka navodi korisnike na preuzimanje zlonamjernih sadržaja ili odavanje osjetljivih podataka i informacija.



## VRSTE PHISHING NAPADA



### PHISHING

Napadi na veliki broj adresa elektroničke pošte potencijalnih meta



### SPEAR PHISHING

Napadi prema precizno ciljanim pojedincima



### WHALING

Napadi prema precizno ciljanim pojedincima na upravljačkoj poziciji u organizaciji

## NA ŠTO OBRATITI POZORNOST?



PROVJERITE IME POŠILJATELJA I ADRESU ELEKTRONIČKE POŠTE



GRAMATIČKE GREŠKE I POGREŠNA UPOTREBA PADEŽA



TRAŽE VAS DA UNESETE OSOBNE PODATKE



PRIJETE VAM ILI ZAHTIJEVAJU HITNU AKCIJU

## ŠTO UČINITI KAD UOČIMO SUMNJIVU PORUKU?



1. POSTUPITI SUKLADNO INTERNIM PRAVILIMA I PROCEDURAMA TIJELA



2. PRIJAVITI KORISNIČKOJ PODRŠCI POJAVU PHISHING PORUKE



3. PRATITI NEUOBIČAJENE AKTIVNOSTI NA RAČUNALU I SUSTAVU

