Savjeti kako se zaštititi od zlonamjernog softvera

Microsoft

U posljednjem periodu smo svjedoci velikog porasta broja računala naših korisnika koja su izložena cyber prijetnjama te su inficirana virusima. S obzirom na to, odlučili smo poraditi na podizanju svijesti o odgovornom ponašanju pri korištenju računala, a posebice e-maila.

Za početak - **pojmovi**

Zlonamjerni softver koji može inficirati naše računalo zovemo ***malware***. *Malware* koji dobijemo e-mailom obično predstavlja tzv. *phishing* prijetnju. (dolazi od engleske riječi *fishing* – pecanje, analogija na bacanje udice i mamca na koji se korisnik može "upecati").

ŠTO MOŽETE NAPRAVITI KAKO BISTE SE ZAŠTITITI OD CYBER NAPADA:

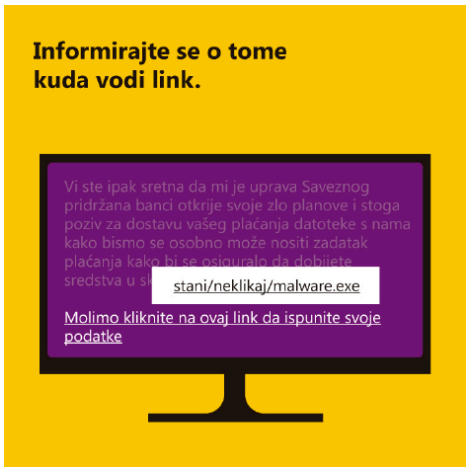
- Preuzmite i instalirajte antivirusni program i provjereni softver protiv malwarea
- Antivirusni i antispyware softver preuzimajte iz provjerenih izvora
- Ne otvarajte spam e-poruke, ne klikajte na sumnjiva web odredišta
- Redovito instalirajte sigurnosne nadogradnje za antivirusne i antispyware programe, preglednike, operativne sustave, programe za obradu teksta i drugo
- Deinstalirajte programe koje više ne koristite
- Budite oprezni s oglasima koji zvuče predobro da bi bili istiniti
- Osmislite snažne lozinke, sastavljene od kombinacije slova, brojeva i simbola
- Ne dijelite svoje lozinke, ne koristite iste lozinke na svim web odredištima i servisima
- Izradite različite lozinke za router i bežični ključ za kućne bežične mreže
- Ne spajajte nepoznate USB-ove na računalo
- Oprezno s otvaranjem privitaka i poveznica u e-pošti, programima za chat i društvenim mrežama poput Facebooka
- Programe preuzimajte samo s provjerenih web odredišta
- Budite na oprezu kad vam besplatno ponude glazbu, igre, video i tome slično

PHISHING

Phishing predstavlja krađu identiteta putem e-maila i/ili lažne web stranice s ciljem zloupotrebe osobnih informacija. *Phising* napad se manifestira u više oblika od linkova unutar e-maila, preko web stranica do telefonskih poziva.

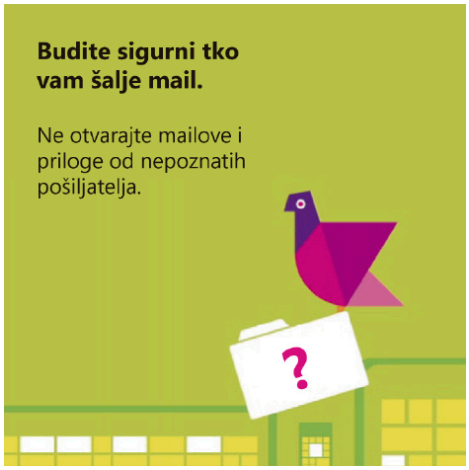
Neki od trikova koje kriminalci upotrebljavaju su:

LAŽNE WEB STRANICE



Ako dobijete sumnjivu poruku putem e-pošte sa zahtjevom da klinknete na link, postavite pokazivač miša iznad linka (ali **BEZ KLIKANJA**!). Ako URL ne odgovara opisanom u tzv. *hover* balončiću – nikako ne klikajte na link nego obavijestite svoje administratore!

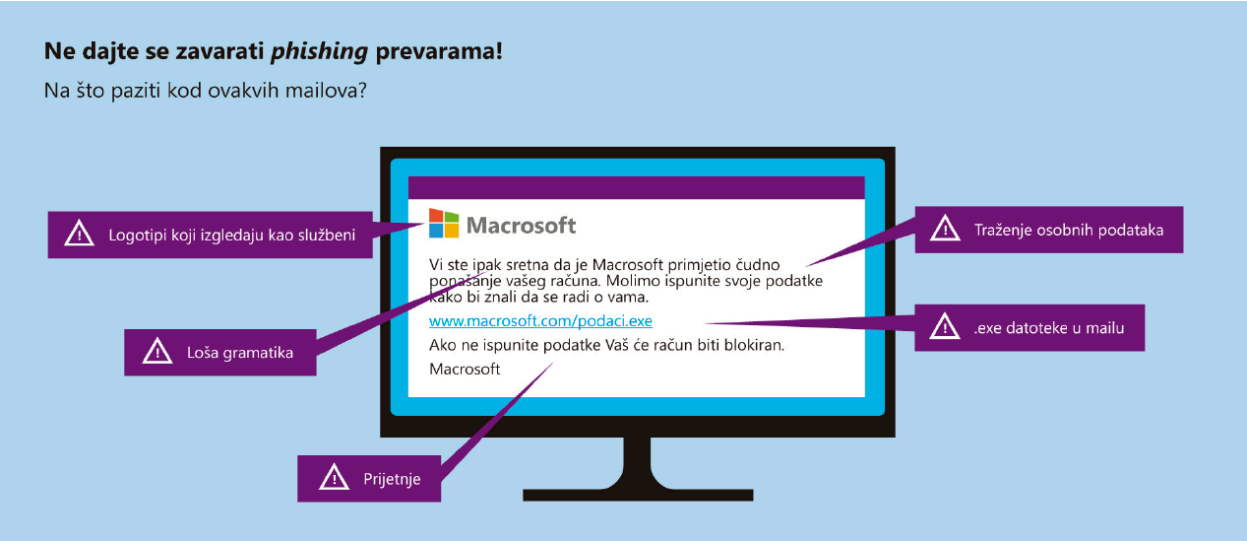
PRIJETNJE



Ako dobijete obavijest o zatvaranju vašeg računa u banci, najčešće se radi o *cyber* kriminalu. Također, obično se u poruci traži da poduzmete neke aktivnosti kako vam računa ne bi bio zatvoren. U slučaju dobijanja takve poruke, budite oprezni i obavijestite vaše administratore!

SPOOFING

Tzv. *Spoofing* (podvala) predstavlja prijetnje putem kojih se koriste grafike koje iznimno vjerno predstavljaju vizualni identitet poznatih web stranica, internetskog bankarstva ili čak poznatih svjetskih korporacija. Korisnik obično dobija poruku putem koje se traže osobni podaci, a zauzvrat obećava transferiranje novca na račun korisnika ili dobijanje novčane nagrade od raznih korporacija, npr. Microsofta ili Facebooka. To jednostavno nikada nije istina te stoga **ne nasjedajte**!



RANSOMWARE

Ransomware onemogućava korištenje računala. U tom slučaju vaši podaci i datoteke bit će nedostupni, a računalo neće biti u funkciji sve dok kreatoru *malwarea* ne uplatite novac. U nastavku ćemo pojasniti što je *ransomware*, što on čini, te dati savjete kako se od njega zaštititi i oporaviti u slučaju inficiranja vašeg računala.

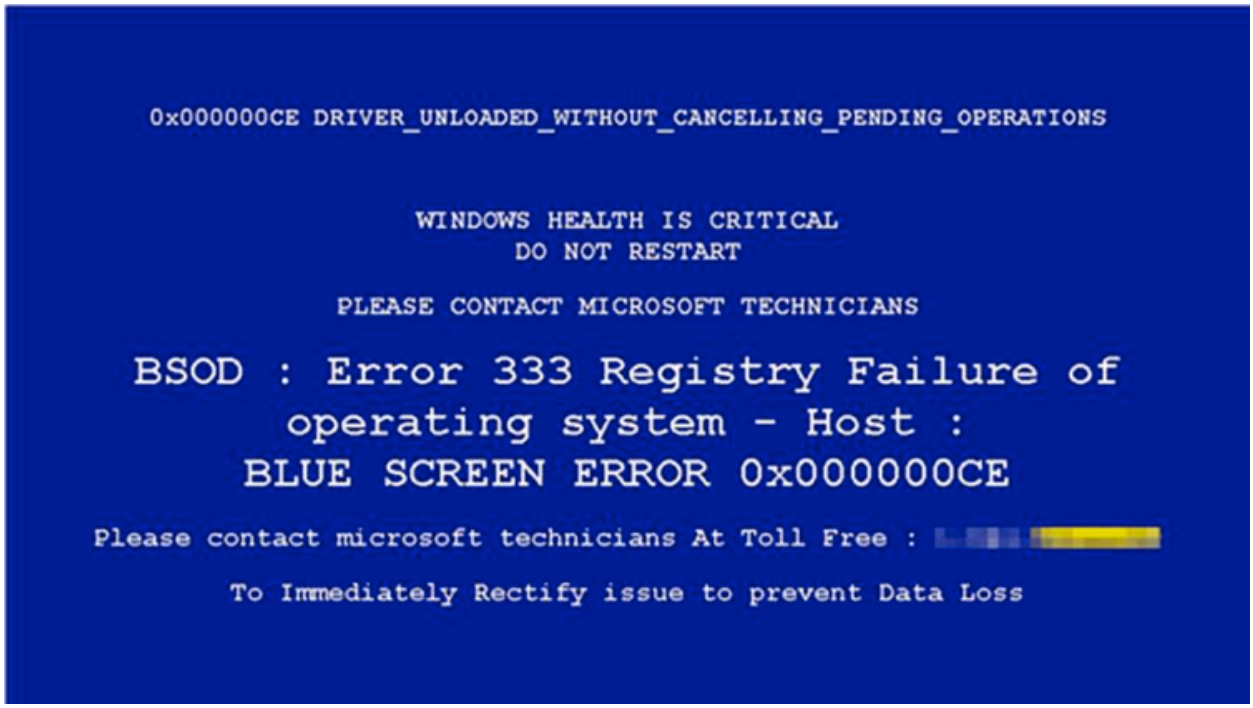
ŠTO RADI RANSOMWARE?

Postoje različite vrste *ransomwarea*, a zajedničko je da će vas svaki od njih spriječiti u normalnom radu s računalom te će tražiti da odradite određenu radnju kako biste ponovno mogli koristiti svoje računalo.

Cyber kriminalci mogu ciljati sve skupine korisnika računala, bilo da se radio kućnom računalu, krajnjim točkama u poslovnim mrežama, poslužiteljima vladinih tijela i agencija te davateljima usluga zdravstvene zaštite.

RANSOMWARE MOŽE:

- Spriječiti pristupanje/pokretanje Windowsa
- Šifrirati datoteke, tako da ih više ne možete koristiti
- Zaustaviti pokretanje/izvršavanje određenih aplikacija (uključujući i vaš web preglednik).



Ransomware će zahtijevati uplatu novca (*otkupninu*) kako biste ponovo dobili pristup računalu ili vašim datotekama. Također, uvidjeli smo kako se od žrtava cyber napada traži popunjavanje anketa putem kojih cyber kriminalci dobivaju podatke koji im omogućuju još preciznije napade.

Ono što je također problematično je činjenica kako ne postoji jamstvo ponovnog omogućavanja pristupa vašem računalu ili datotekama nakon uplate.

RANSOMWARE U POSLOVNIM OKRUŽENJIMA

Broj žrtava u poslovnom okruženju je u porastu. Napadači, posebno istražuju i ciljaju svoju žrtvu (pomoću *phishinga* ili krađe identiteta) kako bi dobili pristup poslovnoj mreži.

Zbog šifriranja datoteka, praktički je nemoguće putem obrnutog inženjeringa dešifrirati datoteku bez originalnog ključa za šifriranje – koji posjeduje napadač. Stoga, jedina prava zaštita od ove pošasti je *backup* (odnosno sigurnosna kopija) podataka na fizički odvojenom mediju (bilo na drugom uređaju poput vanjskog čvrstog diska ili drugog računala bilo na servisu za pohranu podataka u oblaku kao što je OneDrive for Business).

U određenom postotku, alati objavljeni od strane raznih tvrtki koje se bave sigurnošću računala mogu dekriptirati vaše datoteke koje su inficirane *ransomwareom*. FireEye i Fox-IT samo su neki primjeri takvih alata koji pomažu kod datoteka šifriranih *Crilock ransomwareom*. Tim Rains, direktor za sigurnost u Microsoftu, objavio je blog „Ransomware: Razumijevanje rizika"* u travnju 2016. godine koji pruža uvid u statističke pojedinosti i prijedloge poduzećima i IT profesionalcima vezano uz prevenciju. Naš „Threat Intelligence Report: Ransomware"** također uključuje prijedloge za sprječavanje i i oporavak kao i statistike te više detalja vezanih uz ovu temu.

* https://blogs.microsoft.com/microsoftsecure/2016/04/22/ransomware-understanding-the-risk/

** https://www.microsoft.com/security/portal/enterprise/threatreports.aspx

Umjesto **završetka**

Računalna sigurnost predstavlja holističku disciplinu koja obuhvaća brigu o svim mogućim vektorima napada na računala i informatičku imovinu. Odgovorno ponašanje pojedinca, usklađeno s pravilima o poslovnom korištenju opreme i softvera treba biti zadaća svakoga od nas jer je to jedini način za sigurni razvoj poslovanja tvrtke ili organizacije kao i sprječavanje većih poslovnih gubitaka nastalih kao rezultat realiziranih sigurnosnih prijetnji.

Najčešće potencijalne prijetnje koje dolaze elektroničkom poštom, a predstavljaju samo dio sveukupnih prijetnji kojima su naša računala i sustavi svakodnevno izloženi, su:

- Posjećivanje neprovjerenih i kompromitiranih web stranica
- Instalacija raznih *shareware* softvera izdanih od strane neprovjerenih proizvođača
- Korištenje prijenosnih memorijskih ključeva („USB stickova“) i kartica, korištenje ne-originalnih CD-ova/DVD-ova
- Te niz drugih aktivnosti koje predstavljaju ozbiljno kršenje internih poslovnih pravilnika

Informacijska sigurnost i borba protiv *malwarea* naša je obveza i neizbježan dio razvoja društva. Ovim putem vas želimo potaknuti da ovu knjižicu proslijedite svojim poznanicima, obitelji i poslovnim partnerima koji bi se također mogli naći na meti *cyber* napada. Želimo podići svijest o važnosti odgovornog ponašanja pojedinaca u online okruženju kako bismo spriječili sve učestalije *cyber* napade i smanjili njihovu uspješnost.

Srdačan pozdrav,
MICROSOFT HRVATSKA d.o.o.

JESTE LI ZNALI?

Digital Crimes Unit (DCU) Microsoftov je međunarodni tim pravnih i tehničkih stručnjaka čiji je cilj zaustaviti ili onemogućiti *cyber* kriminal i prijetnje računalnoj sigurnosti. U suradnji sa stručnjacima za *cyber* kriminal iz različitih industrija DCU uklanja *cyber* prijetnje klijentima, poslovanju Microsofta kao i u kompletnom digitalnom poslovnom okruženju.

Istovremeno, tim radi na zaštiti korisnika i tvrtki od *cyber* kriminala u punom opsegu, uključujući prijestupe povezane sa zlonamjernim softverom (engl. *malicious software*) i one koji koriste tehnologiju te su usmjereni na djecu i starije osobe. DCU primjenjuje alate za forenziku i praćenje kako bi preduhitrili sofisticirane *cyber* kriminalce koji stalno razvijaju nove metode digitalnog kriminala i piratstva.