**Što je prijetnja za korisnika?**
Prijetnja za korisnika su razne tipovi datoteka koje nenamjerno možemo pokupiti na internetu. A koji se najčešće skrivaju iza dobronamjernih stranica.

Među njih spadaju:
•    Virusi
•    Crvi
•    Trojanski konj
•    Adware
•    Spyware
•    Daileri
•    Višestruka ugroza (eng. blended threat)

**Virusi:**
Program ili dio kôda koji je bez znanja korisnika učitan u računalo korisnika i koji se izvršava bez njegovog znanja, odnosno svjesnog pristanka.

**Crvi:**
Program ili algoritam koji se sam replicira na računalnoj mreži i pri tome obično čini neku štetu.

Trojanski konj:
Kolokvijalno se još naziva i trojan ili trojanac, potencijalno je opasan program (obično otvara "vrata" za neovlašten ulaz na računalo) i koji se predstavlja kao obični, neopasni program. Za razliku od crva, trojanci se sami ne repliciraju. Zlonamjerni programi koji se prema korisniku predstavljaju kao "jako korisni" programi, a u stvari zlorabe korisnikovo povjerenje kako bi od njega dobili određene podatke koje nebi trebao znati nitko osim korisnika (lozinke, podatke o korisniku, ...)

**Adware:**
Program koji automatski prikazuje ili učitava oglase i/ili promidžbene poruke nakon što se instalira na računalo ili za vrijeme korištenja (programi koji korisnika zatrpavaju reklamnim materijalima, najčešće u obliku skočnih (pop-up) prozora).  Neki adware programi pripadaju ujedno i grupi spyware programa.

**Spyware:**
Program koji je bez svjesnog pristanka korisnika instaliran na računalo i koji presreće ili čak djelomično preuzima nadzor nad interakcijama korisnika i računala. Tako prikupljene podatke spyware može proslijediti trećoj osobi.

**Daileri:**
Progami koji promijene korisničke postavke za spajanje na Internet preko dial-up veze te se korisnik više ne spaja preko legalnog davatelja usluge već preko ilegalne daleko skuplje veze te tako nabijaju telefonski račun.

Višestruka ugroza (eng. blended threat):
Iskorištavanje ranjivosti računala korištenjem kombinacije virusa, crva i trojanaca.

**Kako se zaštititi?**

Zaštiti se možemo raznim programima ali ćemo najviše pridonjeti zaštiti razmišljajući svojom glavom. Instalirajući neki antivirusni program i redovito ga updatetati. Izbjegavati sigurnosne rupe pravilnim instaliranjem programa i aktiviranjem vatrozoida. Upotrijebiti zdravu pamet svaki put prije no što kliknemo na Download ili umetnemo DVD ili CD sumnjivog porijekla u računalo. Ne otvarati e-mail poruke nepoznatih ljudi, posebno ako imaju privitke ( sa dvostrukim ekstenzijama, ili izvršnim ekstenzijama). Redovito arhivirati podatke da bi se umanjio učinak eventualnog gubitka podataka.

**Vrste zaštite:**

Antivirusna zaštita
Imajte na računalu uvijek instaliran i aktivan antivirusni program. Antiviruse koji nemaju mogućnost automatske nadogradnje preko weba i koji nemaju stalno aktivnu zaštitu i provjeru datoteka kojima se pristupa tijekom rada na računalu, nemojte uopće uzimati u razmatranje. No nemojte se nikako pouzdati samo u antivirusni program jer su virusi uvijek korak ispred! Znači, prvo se pojavi virus, a tek nakon toga definicija (nadogradnja) antivirusnog programa koja omogućava da ga antivirusni program prepozna. U tom razdoblju vaše računalo je nezaštićeno od tog virusa i jedina zaštita je korisnikovo iskustvo kojim može prepoznati sumnjive programe ili datoteke!Postoje besplatni i komercijalni antivirusi.

Besplatni su:
•   [Avast! Home Edition](http://www.avast.com/free-antivirus-download)
•   [Avira](http://www.avira.com/en/pages/index.php)
•   [AVG Free Edition](http://free.avg.com/ww-en/homepage)

Komercijalni su:
•   [ESET NOD 32 Antivirus](http://www.eset.com/)
•   [Kaspersky Anti-Virus](http://www.kaspersky.com/af/globalstore?thru=reseller%3Dgoogle_gbsn_k%26gclid%3DCOP9nMPuk6ACFQgeZwod_AsNdQ)
•   [Symantec Norton-AntiVirus](http://www.symantec.com/index.jsp)
•   [F-Secure](http://www.f-secure.com/en_EMEA/products/)

**Antispyware  zaštita**
Pod spyware mislimo na programe koji se nasele na korisničko računalo ali ne rade nikakvu štetu u smislu brisanja datoteka ili slično, već korisnika ometaju u radu iskakanjem reklamnih prozora, pokušajima automatskog spajanja na net, u krajnjem slučaju i slanja korisnikovih podataka na udaljena web odredišta i slično.
Ovi programi nisu tako skriveni i moguće je da ih korisnik i sam instalira privučen reklamom a ne znajući njihovu pravu namjeru. Ti programi mogu promijeniti i početnu stranicu web preglednika mijenjajući je za svoju, promijeniti grafičko sučelje računala, desktop pozadinu, što i nije tako opasno ali korisnika tjera na utrošak vremena za vraćanje u početno stanje.

Preporuka je koristit neke od navedenih:
•   [Malwarebytes Anti-Malware](http://www.malwarebytes.org/mbam.php)
•   [SUPERAntiSpyware Free Edition](http://www.superantispyware.com/index.html)
•   [Spybot – Search&Destroy](http://www.safer-networking.org/en/index.html)

**Firewall (vatrozid)**
Firewall je program koji prati promet preko mrežnog sučelja računala (mrežna kartica, bežična mreža, ...). Nažalost, za korištenje firewalla potrebno je malo više znanja o računalima jer loše podešenim firewallom možete onemogućiti pristup na mrežu ili pojedinim programima ili cijelom računalu. U principu, ako nemate dovoljno iskustva sa firewallom, a ipak ga želite koristiti, najbolje je da ga nakon instalacije koristite u "learning modu" jer će vas u tom slučaju firewall obavještavati porukom o svakom programu koji želi komunicirati s Internetom te vas pitati želite li dopustiti spajanje. Već iz ovog kratkog opisa je vidljivo da vam je potrebno znanje što je koji program, što radi te je potrebno i nešto znanja iz mrežnog područja, portovima i protokolima.

Osim njih još je dobro znati:
•   Datoteke preuzimati samo s onih internet mjesta što zajamčeno poduzimaju mjere antivirusne provjere sadržaja koje nude na preuzimanje.

•    Svaku prijenosni medij CD, DVD, USB stick, prijenosni hard disk s podacima koje ste dobili iz neprovjerenog izvora valja podvrći testiranju na viruse. Prije učitavanja sadržaja u računalo, obvezno je “propustiti” kroz antivirusni program.

•    Svaku datoteku koju dobivate putem mreže, bez obzira od koga, odmah po prihvaćanju valja testirati na viruse.

•    Nikada ne treba otvarati datoteke primljene elektroničkom poštom od nepoznatog pošiljatelja, odnosno iz neznanog izvora. Širenje virusa elektroničkom poštom najčešći je oblik infekcije.

•    Prije preuzimanja datoteka iz Interneta dobro je kopirati (memorirati) veličinu (dimenzije) važnih sistemskih datoteka i datum njihove posljednje promjene. Ako se nakon preuzimanja datoteke ti podaci primijene, to je ozbiljna indikacija na moguću zarazu virusom.

•    Obično je dobro dezaktivirati makro instrukcije u Word i Excel datotekama prije njihova korištenja i testiranja na viruse. Makro instrukcije su zapravo “miniprogrami” kakve virusi “vole” napadati, pa su čest izvor zaraze.

•    Kada ste “na Mreži”, što češće aktivirajte “tragače” za virusima. Ne treba tražiti jako siguran povod ili čekati da se virus sam “javi”– nastojite biti korak ispred njega.

•    Učinite da se tragači za virusima i antivirusni programi aktiviraju sami pri svakom preuzimanju bilo kakvog sadržaja s Interneta, što je kod većine takvih programa moguće izborom opcije „Autodetect“.

•    Redovito ažurirajte antivirusne programe. Najveća je nevolja s virusima ta što se stalno javljaju novi!

**Internet i e-mail prijevare**

Kako se zaštititi od internet prijevare?
Kako naučiti razlikovati pravi od lažnog e-maila?
Kako se zaštititi od internetskih prijevara?

Kao i uvijek najbolji način žaštite je znanje i inteligencija. Ukoliko naiđete na sumnjivu internet stranicu ili dobijete sumnjivi e-mail dobro ih proučite i ako niste sigurni provjerite kod nekog tko zna. Ukoliko ne poznajete takvu osobu možete se obratiti svom internet provideru.
Obično najlakši način prepoznavanja lažne stranice je link. Nedavno ste mogli dobiti jedan takav lažni mail od "PayPal" tvrtke gdje se odmah po linku vidjelo da je lažni.
Link na koji se trebalo kliknuti je naravno bio zakamufliran tako da izgleda kao da je došao od tvrtke PayPal. Zakamuflirani link je link koji nije cijeli nego npr. piše "Dispute Transaction" tako da ne vidite pravi link a kada kliknete na njega odvede vas na stranicu koja je lažna i izgleda kao original od PayPal tvrtke no URL nije npr.[https://www.paypal.com](https://www.paypal.com/) (koji je originalni link od PayPal-a) nego<http://www.greg.co.kr/www.paypal.com/webscr.php?cmd=_login-run>.
Srednji dio linka gdje pise www.paypal.com je trebao zavarati posjetitelja i ostaviti dojam da je to originalna PayPal stranica.
Kada bi otvorili tu stranicu izgledala bi indentično kao PayPal stranica no kada bi unjeli podatke svoje kreditne kartice ostali bi bez svog novca.
PayPal je inače omiljena meta takvih mailova jer se PayPal bavi novčanim transakcijama i jako puno ljudi ga koristi.
Tehnički način zaštite je da koristite sigurniji web browser i e-mail client a to je skoro svaki osim Internet Explorera (osim možda verzije 8). Neki od browsera koji su sigurniji i kvalitetniji od Internet Explorer-a su Mozilla Firefox, Opera.  Firefox je trenutno najpopularniji i ima puno dodataka koji vam mogu olakšati život.
Kvalitetan i popularan e-mail client je Mozilla Thunderbird. Kao i Internet Explorer tako je i Outlook Express mail client nekvalitetan i pun siguronosnih propusta. Ne brinite prilikom instalacije Thunderbirda možete sačuvati sve svoje mailove iz Outlook Expressa.

**Phishing e-mail:**

Phishing e-mail kao što mu i ime kaže pokušava upecati nepažljive ljude tj. njihove kreditne kartice.
Postoje razne varijante tekstualnog sadržaja no svima su iste dvije stvari, ili se radi o lažnom računu za recimo PayPal, Amazon, Apple, ebay ili neku drugu tvrtku i vi trebate potvrditi kupnju putem web formulara koji se nalazi na lažnoj a ne pravoj adresi ili vam u poruci stoji kako trebate obnoviti svoj password za neku stranicu recimo PayPal, Amazon, Apple, ebay i kad to napravite netko treči dobije vaše accaunt podatke i kupuje a vama stižu računi.

Lažne internetske tvrtke

Ovaj način prijevare je sličan kao i e-mail pishing. Dobit ćete e-mail u kojem piše da neka tvrtka prodaje nešto, obično software po znatno jeftinijim cijenama.
Kad odete na njenu stranicu izgledati će kao neka obična firma samo će proizvodi biti 70% jeftiniji.
Realno je moguće da netko prodaje proizvod cca 20-30% jeftinije ali ne i 70 ili više posto.
Kada kod njih kupite proizvod najvjerojatnije nećete dobiti ništa ili u najboljem slučaju sprženi cd.

**Lutrijski dobitak**

 Kako se ljudi u ovakvim slučajevima ustvari pokušavaju prevariti. Naime, osoba primi e-mail o dobitku i molbu/uputu da pošiljatelju, najčešće u Veliku Britaniju ili Španjolsku, pošalje svoje osobne podatke, odnosno kopiju putovnice ili vozačke dozvole, adresu, broj telefona, kopiju računa kako bi se mogao uplatiti dobitak i slično.
Ukoliko "sretni dobitnik" pošalje podatke, ponovno dobiva poruku, a ovaj put mu se sugerira da se javi nekoj od europskih komisija za dobitke od igara na sreću, vezano uz, naravno, odobrenje za isplatu dobitka. "Sretni dobitnik" je i taj put zamoljen poslati osobne podatke, jednake onima koje je već poslao lutriji kod koje je ostvaren dobitak.
Nakon što "dobitnik" još jedan put pošalje tražene podatke, željno iščekujući svoj dobitak, tzv. komisija traži plaćanje naknade, nakon čega će konačno isplatiti dobitak.
Dogodi li se da "dobitnik" plati traženu naknadu, prevaranti su "na konju", jer prijevara se u tome i sastoji. Drugim riječima, nakon što tzv. dobitnik pošalje određenu svotu novca, svaki kontakt s druge strane prestaje, jer su uspjeli u svojoj namjeri, odnosno navukli su nekoga da im plati određenu svotu.
Znajući da se brojka ovakvih poruka zaprimljenih u jednome danu u cijelom svijetu kreće u tisućama, može se pretpostaviti kolika je njihova dobit.
No, teško im je stati na kraj, jer uvijek barataju lažnim podacima, a imena osoba i kuća koje organiziraju lutriju vrlo se brzo mijenjaju.
Najbolja zaštita je ne nasjedati na takve laskave poruke, a ako se ipak dogodi da pošaljete podatke, tu stanite, jer je najvažnije ne slati novac za tzv. naknadu.

**Krađa identiteta**

U slučajevima kada osoba pošalje svoje podatke, najčešće se događa da je nakon nekog vremena počinju mučiti sumnje je li to legalno, hoće li joj netko zloupotrebljavati račun ili krivotvoriti podatke.
Opasnosti takve vrste postoje, no, realno, vrlo su male, budući je puno jednostavnije navući tzv. dobitnika da nešto plati, nego se mučiti krivotvorenjem podataka, i to na temelju fotokopiranih dokumenata.
Ipak, ponekad i mala šansa opasnost može učiniti prevelikom. Naime, temeljem podataka koje osoba dostavi (osobni podaci, adresa stanovanja i radnog mjesta, informacije o užoj obitelji i sl.) mogu se krivotvoriti dokumenti i na taj način "ukrasti identitet" donedavno sretnog dobitnika.
Sjetimo se ljudi i umirovljenica" koji su došli pod sudski progon jer su kriminalci s njihovim identitetom manipulirali na svjetskim burzama.
Policija savjetuje da se u samom startu brišu takve poruke i na taj način pomogne u onemogućavanju ovakvih oblika prijevare. Također, vaši osobni podaci su samo vaši te ih nemojte olako slati nepoznatim osobama, pogotovo putem interneta.

Informacije i primjeri preuzeti sa BOL-Foruma!
bug.hr/forum