

Opasnosti na internetu

"Radoznalost uvlači ljude u prijevaru."

Frank Stallone

U početku do 1990tih godina su internet koristile samo znanstvene ustanove i sveučilišta tako da nije bilo opasnosti na internetu. Kada su se u korištenje interneta uključila i poduzeća stvari su se promijenile. Praktično se svo društvo iz realnog svijeta preslikalo na virtualni svijet pa i kriminal, pornografija, lažna prodaja, prodaja oružja,...

U ovom poglavlju opisat ćemo opasnosti koje možemo očekivati pri korištenju internetskih aplikacija.

Internetska prijevara (engl. scam) jest zlouporaba u kojoj je neka osoba u zabludi i ne sumnja da je riječ o prijevari. Osobi se pružaju lažni podaci kako bi prevaranti ostvarili zaradu ili došli do osjetljivih podataka.

Hoax (engl. obmana) - prijevara kojom se zastrašivanjem ili nagovaranjem pokušava pridobiti korisnika da je proširi!



Slika 51 Karikatura zastrašivanja

Najčešći oblici hoaxa:

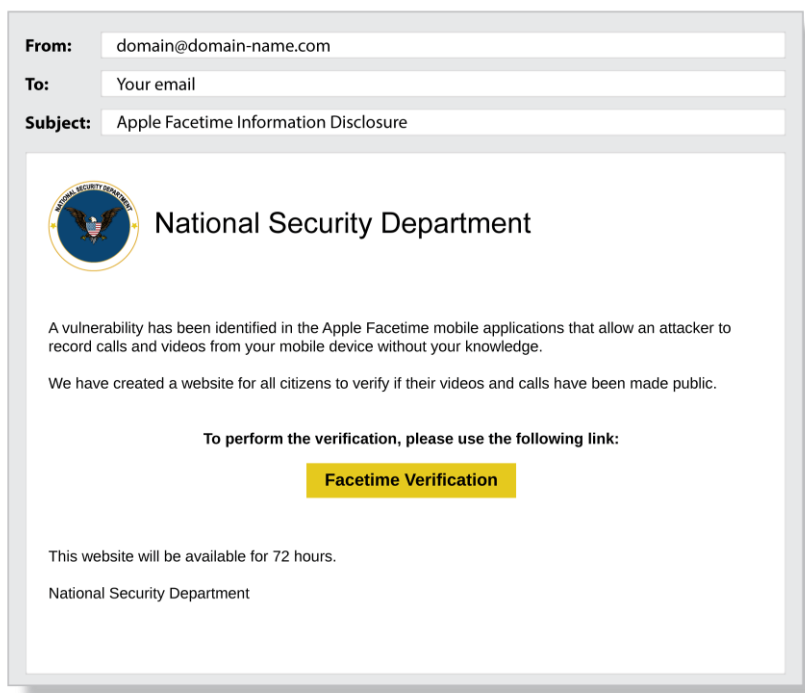
poruke upozorenja o štetnim programima, virusima i sl.

lanci sreće u kojima se prijete da će nam se nešto dogoditi ako ih prekinemo

poruke o nemoćnim osobama kojima treba pomoći (bolesna djeca, roditelji traže svoju djecu...)

poruke koje narušavaju ugled osobe ili organizacije (lažne izjave, tračevi i sl.).

Phishing (oblik engleske riječi za pecanje, fishing) - način prijevare kojom netko želi "upecati" naše osobne podatke.



Slika 52 Primjer „phishinga“

Ima različitih oblika phishinga kao na slici gore zahtjev da se verificiramo zbog opasnosti kao na slici gore, ili izbrisat će se vaš račun elektroničke pošte ako ne pošaljete svoje podatke ili slijediti poveznicu. Obično je dizajn poruke sličan stvarnoj stranici međutim ako pogledate adresu sa koje je poslana poruka vidite da nije povezana sa naslovom stvarne institucije.

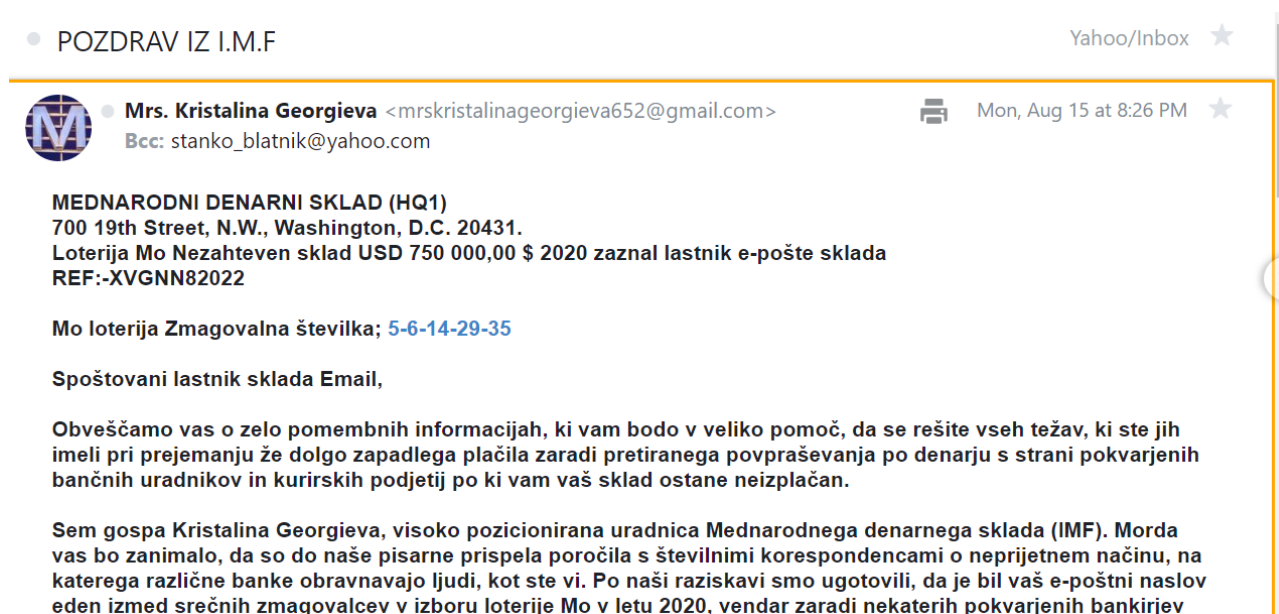
Česti pokušaji su lažna obećanja da ste dobili novčanu nagradu. Mogu vam nuditi da dobijete odštetu, jer ste se liječili lijekom koji ima neželjene posljedice kao na slici 53



Slika 53 Primjer elektroničke poruke sa ponudo odštete za liječenje.

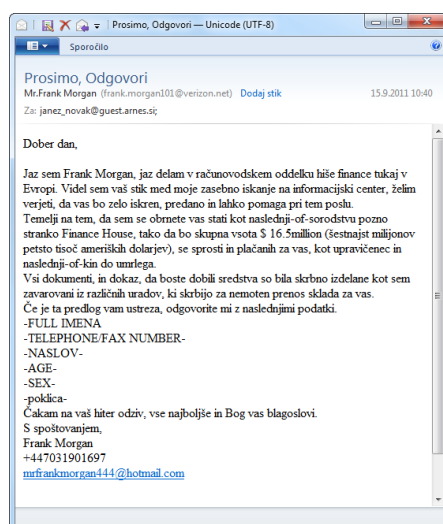
Ako pogledate naslov elektroničke pošte sa kojeg je poslana pošta vidite da je čudan kao i sama ponuda.

Druga mogućnost je da dobijemo poruku u kojoj nam javljaju da smo dobili na lutriji. Kada pažljivije na tekst vidjet ćete da je to loš prijevod vjerojatno sa engleskom. Takve poruke odmah izbrišite.



Slika 54 Primjer elektroničke pošte o dobitku na lutriji

Nigerijska prijevara obično započinje slanjem masovnih poruka putem e-pošte i uljudno se predstavlja, obično kao bogati poslovni čovjek ili državni službenik, govoreći mu odakle dolazi (obično iz Nigerije) i opisuje svoj problem. Osoba želi osobne podatke žrtve i bankovni račun, jer ima veliku svotu novca koju želi prenijeti iz svoje zemlje u inozemstvo, pa nudi i visoku nagradu. Ako primatelj odgovori, odgovara da je potrebno prethodno platiti troškove otvaranja računa i neke druge troškove, a ti su troškovi zanemarivi u odnosu na obećanu nagradu. Zahtijeva prijenos putem platnog sustava Western Union, koji se ne može pratiti. Nakon prijenosa osoba prekida komunikaciju sa žrtvom.

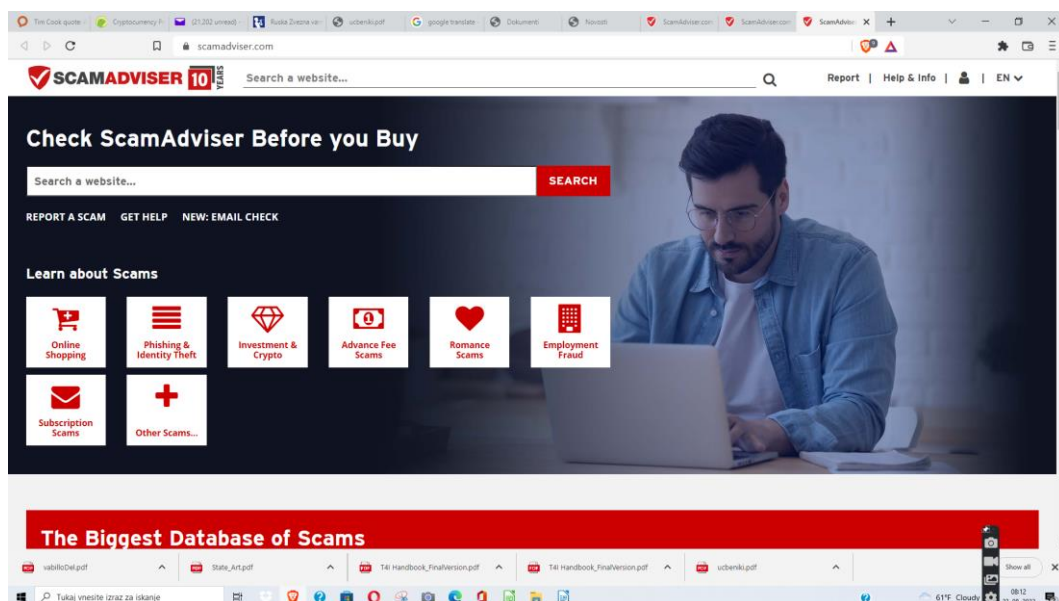


Slika 55 Primjer nigerijske prijevare

Na slici 53 je prikazano pismo tipično za nigerijske prijevare. Vidi se da je jezik loš i nastao automatskim prevođenjem. Ako to povežete sa nerealnom ponudom možete biti sigurni da vas pošiljalac želi prevariti.

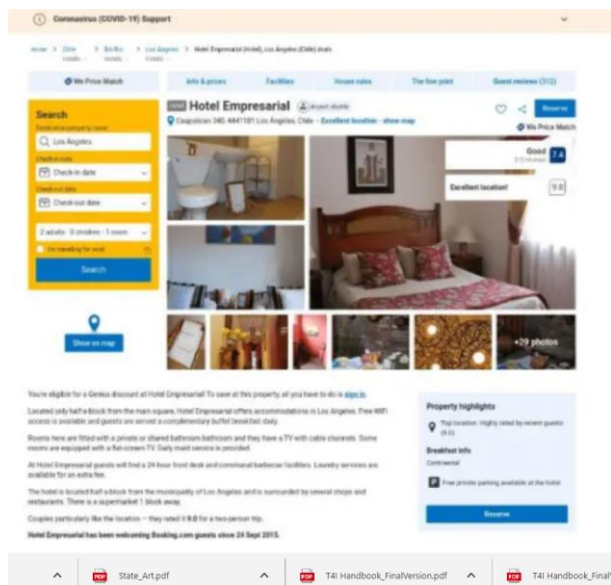
Prilikom kupovine na webu vas isto mogu prevariti. Posebno treba paziti ako naletite na internetsku trgovinu koja vam proizvode nudi po izuzetno niskim cijenama. Prvo što morate uraditi u tom slučaju provjerite web stranicu sa koje želite kupovati. Postoje više web stranica na kojima je moguće provjeriti da li je sigurno kupovati u određenoj internetskoj trgovini. Na slici 56 je

početna stranica www.scamadviser.com. Dobro bi bilo ukoliko bi provjerili prije svake internetske kupovine na internetskim trgovinama na kojima još niste kupovali da li je kupovina sigurna.



Slika 56 Početna stranica www.scamadviser.com

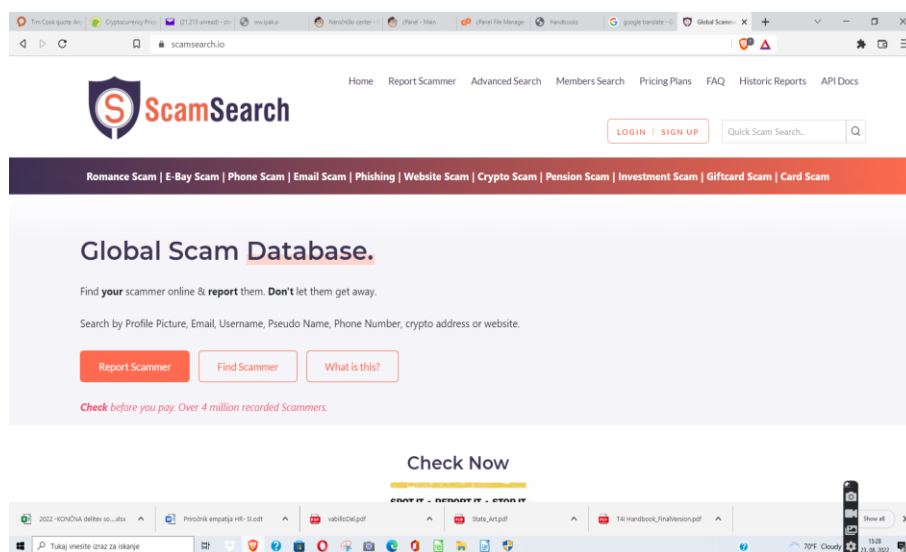
Postoje i lažne trgovine čiji su web stranice slične poznatim internetskim poduzećima. Tako je na



Slika 58 Lažna web stranica Bookinga

slici 58 prikazana lažna web stranica www.booking.com . Ako na takvoj stranici rezervirate sobu bićete neprijatno iznenađeni kada dođete na svoje odredište.

Zato je potrebno u slučajevima kada vam se ponuda učini veoma ugodna provjeriti da nije u pitanju određena prijevara. Pažljivo pogledate internetsku adresu tog „ugodnog” ponuditelja usluge i provjerite tu adresu na www.scamadviser.com ili <https://scamsearch.io/>



Slika 59 Početna web stranica „Scamsearch”

Ukoliko ste žrtva takve prijevara odmah kontaktirajte svoju banku kako biste nadoknadili gubitak i prijavite prijavu na nekoj od web stranica koje prate internetske prijevara.

U svakom slučaju ako ne kupujete kod provjerenih internetskih poduzeća kao što su www.amazon.com, www.ebay.com budite oprezni da izbjegnute nepotrebne gubitke.

Preko elektronske pošte dolazi velik broj poruka koje nas ne zanimaju, a mogu biti štetne jer se upotrebljavaju za ranije opisane prijevara ili prenos virusa. Mada ponuditelji elektronske pošte pokušavaju da ih odstrane u „spam” mapu ne odstranjuju sve štetne e-poruke.

Posebno su opasne poruke koje u privitku sadrže viruse. Virusi se razlikuju od ostalih programa, njima imena završavaju nastavcima EXE, COM, PIF, SCR, VBS, SHS, CHM ili BAT. Oni mogu imati i

neki od poznatih nastavaka npr. DOC, PDF, HTM, HTML, TXT, JPG, GIF... no iza tih nastavaka imaju i nastavke navedene u prethodnoj rečenici. Programe koji imaju nastavke EXE, COM, PIF, SCR, VBS, SHS, CHM ili BAT nikada nemojte pokretati a da prije toga ne skenirate najnovijom verzijom antivirusnog programa.

Pošto većina spamova dolazi preko e-pošte da bi se zaštitili od opasnosti pri pregledu iste pazite na slijedeće

1. Provjerite pošiljatelja e-pošte prije otvaranja. Ukoliko niste sigurni u pošiljatelja nemojte otvarati sadržaj e-pošte. Čak i ako imate antivirus program, nemojte klikati na poveznice i nemojte otvarati priložene datoteke.
2. Koristite najnoviju verziju antivirusnog programa. Omogućite automatsko ažuriranje softvera, jedino ažurirani sigurnosni program može zaštititi vaše računalo.
3. Nikada ne odgovarajte na poruku za koju ste sigurni ili ju smatrate neželjenom porukom. Odmah obrišite takvu poruku.
4. Provjerite sigurnost URL-a bez klikanja na njega. Ako u e-poruci primite sumnjivi URL pređite mišem preko njega te pogledajte donji lijevi kut vašeg web pretraživača. Trebao bi se prikazati pravi URL do kojeg ćete bit preusmjereni. Ako izgleda sumnjivo ili završava na .exe, .js or .zip, nemojte kliknuti na njega.
5. Loš stil pisanja - Prvo što možete primijetiti je predmet i tekst poruke. Najčešće su pisani na engleskom jeziku. Također poruka može biti na vrlo lošem hrvatskom jeziku koje je najčešće automatski prevedena s engleskog jezika na nekom od on-line prevoditelja.
6. Ukoliko se u e-poruci vrši pritisak da preuzmete nešto ili kliknete na neku poveznicu vjerojatno se radi o virusu.

Hi User,

The version of your email is outdated, Failure to upgrade to the newest mail version might result in a permanent closure of your account.

Note: This is mandatory to continue the use of your mailbox

Click [HERE](#) to UPGRADE

**Thanks,
Yahoo Admin**

Slika 60 Primjer e-poruke u kojoj se traži da se klikne na poveznicu

Pored gore opisanih prijevara na webu je prisutno (kao i realnom svijetu): Nasilje na internetu - prijetnje ili ucjenjujući poruke, uznemiravanje, vrijeđanje, širenje neistina, objavljivanje privatnih podataka, montaže, seksualno uznemiravanje i slično.- Tome su prije svega izložena djeca .

Kako se je upotreba digitalnih tehnologija u svakodnevnom životu izuzetno proširila povećao se broj osoba koje su o njima ovisne. To postaje sve veći problem posebno kod mlađih osoba i njegovom rješavanju odnosno traženju pametnog odnosa između realnog i virtualnog svijeta će postati sve više aktualno. Zbog toga je pri poučavanju digitalnih vještina tome posvetiti odgovarajuću pažnju.