Nevarnosti na internetu

"Radovednost vodi ljudi v goljufije."

Frank Stallone

Na začetku, do devetdesetih let prejšnjega stoletja, so internet uporabljale le znanstvene ustanove in univerze, tako da nevarnosti na internetu ni bilo. Ko so podjetja začela uporabljati internet, so se stvari spremenile. Praktično vsa družba iz realnega sveta je bila kopirana v virtualni svet, vključno s kriminalom, pornografijo, lažno prodajo, prodajo orožja, ...

V tem poglavju bomo opisali nevarnosti, ki jih lahko pričakujemo pri uporabi internetnih aplikacij.

Internetna goljufija (eng. scam) je zloraba, pri kateri se oseba zmoti in ne sumi, da gre za goljufijo. Osebi se posredujejo lažni podatki, da goljufi zaslužijo denar ali pridobijo dostop do občutljivih informacij.

Hoax (prevara v angleščini) – goljufija, ki skuša prepričati uporabnika, da jo razširi z ustrahovanjem ali prepričevanjem!

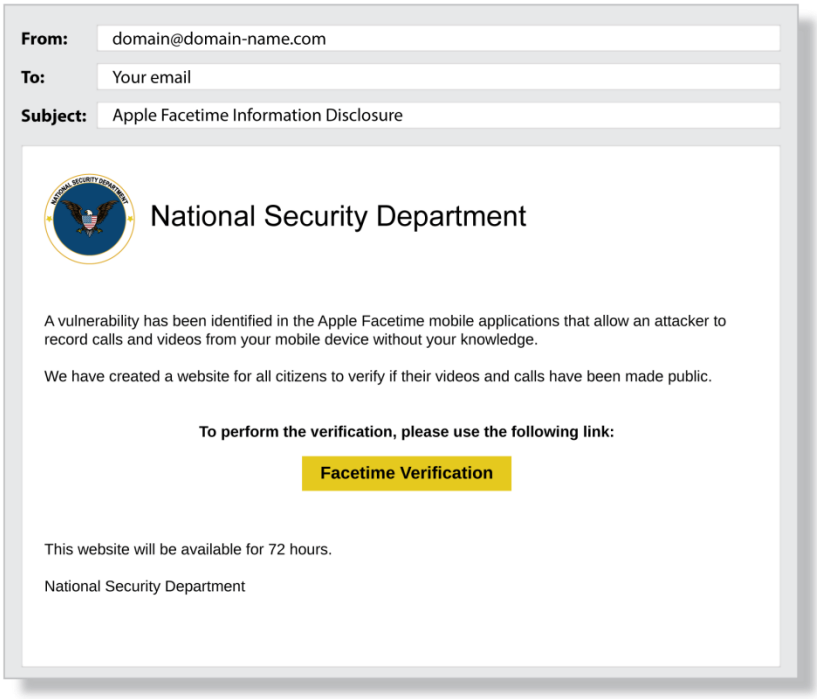
Slika 51 Karikatura ustrahovanja

Najpogostejše oblike potegavščin:

- opozorilna sporočila o škodljivih programih, virusih itd.

- verige sreče, v katerih grozi, da se nam bo nekaj zgodilo, če jih pretrgamo
- sporočila o osebah,, ki potrebujejo pomoč (bolni otroci, starši, ki iščejo svoje otroke...)
- sporočila, ki škodijo ugledu osebe ali organizacije (lažne izjave, trači ipd.).

Phishing (oblika angleške besede za ribolov) – metoda goljufije, s katero želi nekdo »izloviti« naše osebne podatke.

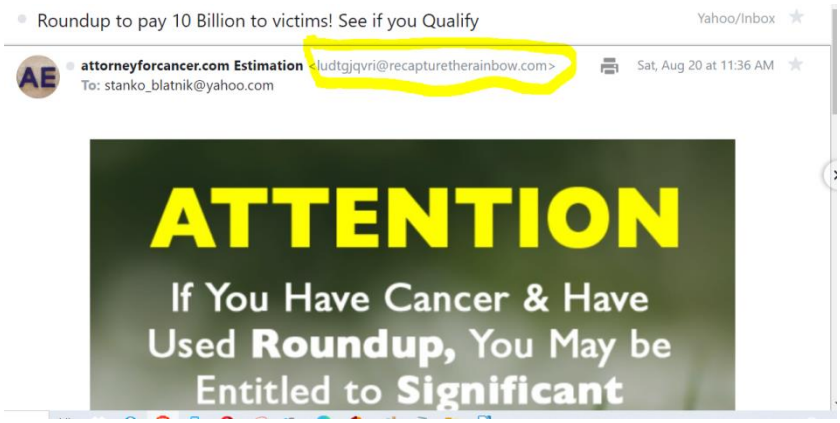


Slika 52 Primer "phishinga"

Obstajajo različne oblike lažnega predstavljanja, kot je na sliki nad zahtevo za preverjanje zaradi nevarnosti, kot je na zgornji sliki, ali pa bo vaš e-poštni račun izbrisan, če ne pošljete svojih podatkov ali sledite povezavi. Običajno je oblika sporočila podobna dejanski strani,

vendar če pogledate naslov, s katerega je bilo sporočilo poslano, boste videli, da ni povezan z naslovom dejanske ustanove.

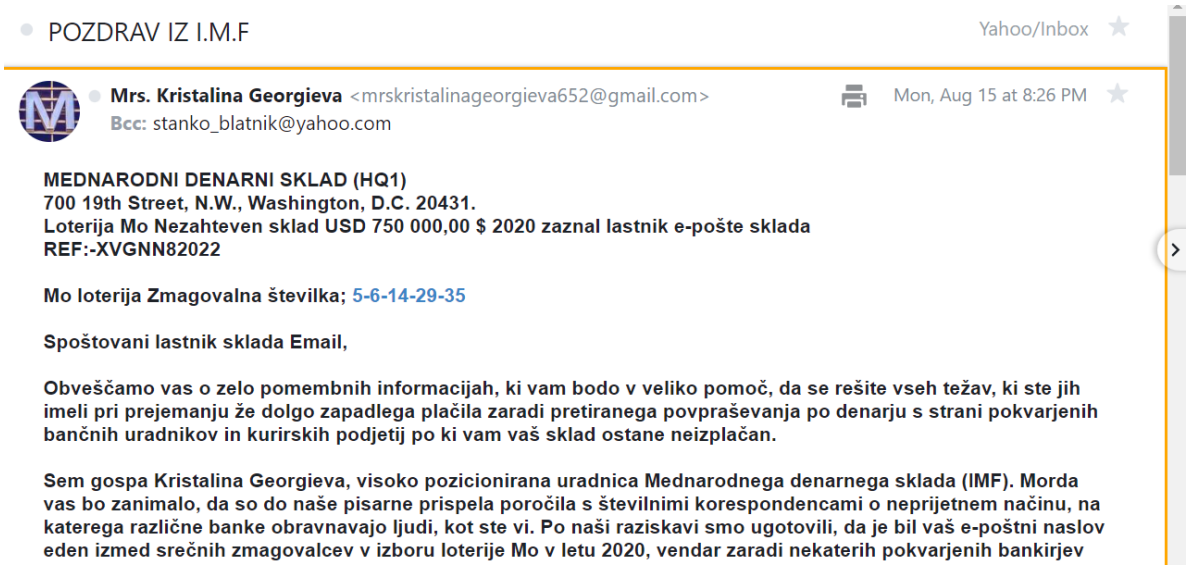
Pogosti poskusi so lažne obljube, da ste prejeli denarno nagrado. Lahko vam ponudim odškodnino, ker ste bili zdravljeni z zdravilom, ki ima neželene posledice kot na sliki 53



Slika 53 Primer elektronskega sporočila s ponudbo nadomestila za zdravljenje.

Če pogledate e-poštni naslov, s katerega je bilo e-sporočilo poslano, boste videli, da je enako nenavaden kot ponudba sama.

Druga možnost je, da prejmemo sporočilo, ki nas obvešča, da smo zadeli na loteriji. Ko boste besedilo bolje pogledali, boste videli, da gre za slab prevod, verjetno iz angleščine. Takšna sporočila takoj izbrišite.


POZDRAV IZ I.M.F

Yahoo/Inbox

Mrs. Kristalina Georgieva <mrskristalinageorgieva652@gmail.com>
Bcc: stanko_blatnik@yahoo.com

Mon, Aug 15 at 8:26 PM

MEDNARODNI DENARNI SKLAD (HQ1)
700 19th Street, N.W., Washington, D.C. 20431.
Loterija Mo Nezahteven sklad USD 750 000,00 $ 2020 zaznal lastnik e-pošte sklada
REF:-XVGNN82022

Mo loterija Zmagovalna številka; 5-6-14-29-35

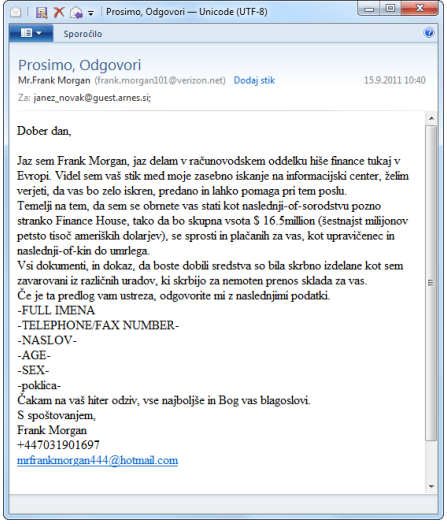
Spoštovani lastnik sklada Email,

Obveščamo vas o zelo pomembnih informacijah, ki vam bodo v veliko pomoč, da se rešite vseh težav, ki ste jih imeli pri prejemanju že dolgo zapadlega plačila zaradi pretiranega povpraševanja po denarju s strani pokvarjenih bančnih uradnikov in kurirskih podjetij po ki vam vaš sklad ostane neizplačan.

Sem gospa Kristalina Georgieva, visoko pozicionirana uradnica Mednarodnega denarnega sklada (IMF). Morda vas bo zanimalo, da so do naše pisarne prispela poročila s številnimi korespondencami o neprijetnem načinu, na katerega različne banke obravnavajo ljudi, kot ste vi. Po naši raziskavi smo ugotovili, da je bil vaš e-poštni naslov eden izmed srečnih zmagovalcev v izboru loterije Mo v letu 2020, vendar zaradi nekaterih pokvarjenih bankirjev

Slika 54 Primer elektronskega sporočila o dobitku na loteriji

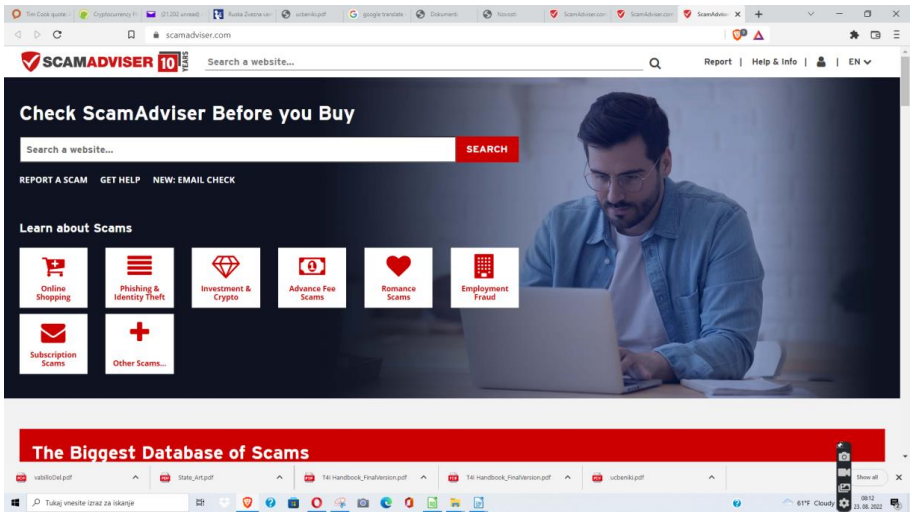
Nigerijska prevara se običajno začne z množičnim e-poštnim sporočilom in se vljudno predstavi, običajno kot premožen poslovnež ali državni uradnik, pri čemer mu pove, od kod prihaja (običajno Nigerija), in opiše svojo težavo. Oseba želi oškodovančeve osebne podatke in bančni račun, saj ima veliko količino denarja, ki ga želi nakazati iz svoje države v tujino, zato ponuja visoko nagrado. Če prejemnik odgovori, odgovori, da je treba vnaprej plačati stroške odprtja računa in nekatere druge stroške, ti stroški pa so zanemarljivi glede na obljubljeno nagrado. Zahteva prenos prek plačilnega sistema Western Union, ki mu ni mogoče slediti. Po prenosu oseba preneha komunicirati z žrtvijo.



Slika 55 Primer nigerijske prevare

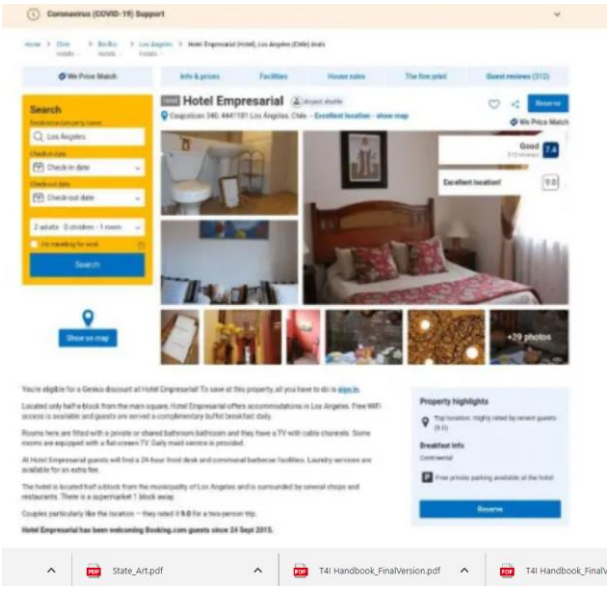
Slika 55 prikazuje pismo, značilno za nigerijske prevare. Vidi se, da je jezik slab in je nastal s samodejnim prevajanjem. Če to združite z nerealno ponudbo, ste lahko prepričani, da vas želi pošiljatelj prevarati.

Pri spletnem nakupovanju vas lahko tudi zavedejo. Še posebej pazite, če naletite na spletno trgovino, ki vam ponuja izdelke po izjemno nizkih cenah. Prva stvar, ki jo morate storiti v tem primeru, je preveriti spletno mesto, na katerem želite kupiti. Obstaja več spletnih strani, kjer je mogoče preveriti, ali je v določeni spletni trgovini varno nakupovati. To je na sliki 56domača stran www.scamadviser.com. Dobro bi bilo, če bi pred vsakim spletnim nakupom v spletnih trgovinah, kjer še niste nakupovali, preverili, ali je nakup varen.



Slika 56 Domača stran www.scamadviser.com

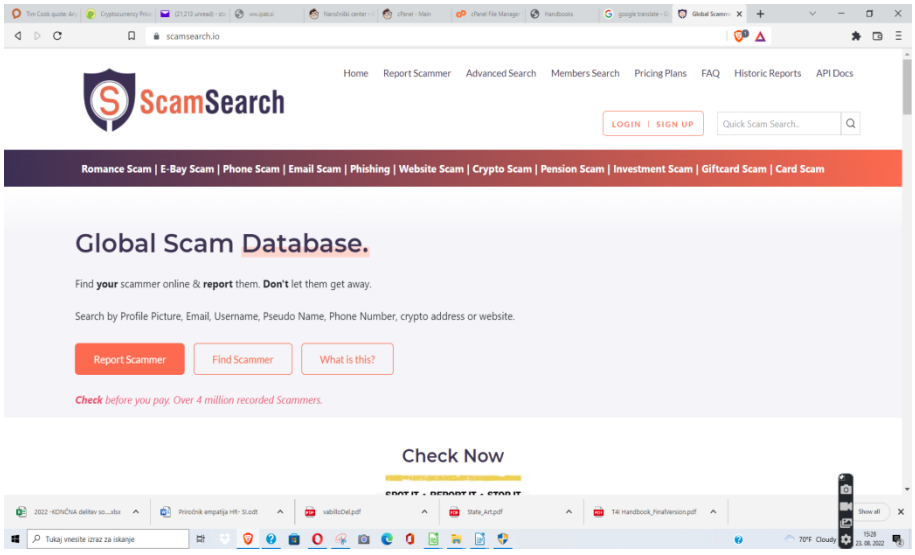
Obstajajo tudi lažne trgovine, katerih spletne strani so podobne znanim spletnim podjetjem. Tako je



Slika 58 Lažna stran Bookinga

Slika 58 prikazuje lažno spletno stran www.booking.com. Če na takem mestu rezervirate sobo, boste ob prihodu na cilj neprijetno presenečeni.

Zato je treba v primerih, ko se vam zdi ponudba zelo prijetna, preveriti, da ne gre za pravo goljufijo. Pozorno si oglejte spletni naslov tega "prijaznega" ponudnika storitev in preverite ta naslov na www.scamadviser.com ali https://scamsearch.io/



Slika 59 Domača stran »Scamsearch«.

Če ste žrtev takšne goljufije, se nemudoma obrnite na svojo banko za nadomestilo izgube in prijavite goljufijo na enem od spletnih mest, ki spremljajo internetne goljufije.

V vsakem primeru, če ne kupujete pri zaupanja vrednih spletnih podjetjih, kot sta www.amazon.com, www.ebay.com, bodite previdni, da se izognete nepotrebnim izgubam.

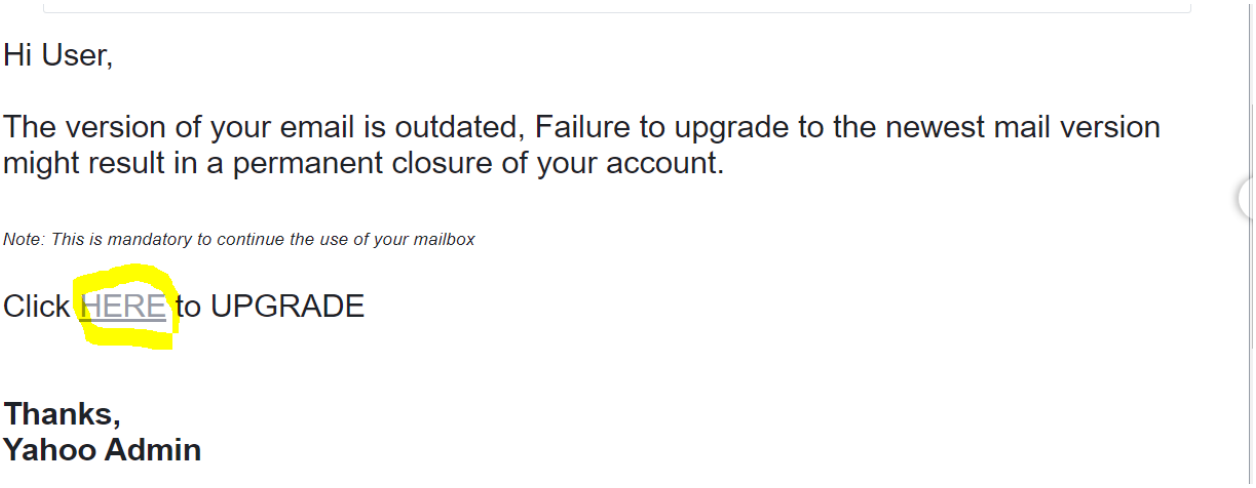
Preko elektronske pošte prihaja veliko število sporočil, ki nas ne zanimajo in so lahko škodljiva, ker se uporabljajo za prej opisane goljufije ali prenos virusov. Čeprav jih ponudniki e-pošte poskušajo odstraniti v mapo »spam«, ne odstranijo vseh škodljivih e-poštnih sporočil.

Še posebej nevarna so sporočila, ki v priponki vsebujejo viruse. Virusi se razlikujejo od drugih programov, njihova imena se končajo z EXE, COM, PIF, SCR, VBS, SHS, CHM ali BAT. Lahko imajo tudi nekatere od znanih končnic, na primer DOC, PDF, HTM, HTML, TXT, JPG, GIF ... vendar imajo za temi končnicami še končnice, omenjene v prejšnjem stavku. Nikoli ne zaženite programov s končnicami EXE, COM, PIF, SCR, VBS, SHS, CHM ali BAT, ne da bi jih predhodno pregledali z najnovejšo različico protivirusnega programa.

Ker večina neželene pošte prihaja prek e-pošte, bodite pozorni na naslednje, da se zaščitite pred nevarnostmi pri ogledu:

1. Preverite pošiljatelja elektronske pošte, preden jo odprete. Če niste prepričani o pošiljatelju, ne odpirajte vsebine e-pošte. Tudi če imate protivirusni program, ne klikajte povezav in ne odpirajte priloženih datotek.
2. Uporabite najnovejšo različico protivirusnega programa. Omogočite samodejne posodobitve programske opreme, le posodobljen varnostni program lahko zaščiti vaš računalnik.
3. Nikoli ne odgovarjajte na sporočilo, za katerega ste prepričani ali ga smatrate za vsiljeno pošto. Takšno sporočilo takoj izbrišite.

4. Preverite varnost URL-ja, ne da bi ga kliknili. Če v e-pošti prejmete sumljiv URL, premaknite miško nad njim in poglejte v spodnji levi kot spletnega brskalnika. Prikazovati mora pravilen URL, na katerega boste preusmerjeni. Če je videti sumljivo ali se konča z .exe, .js ali .zip, ga ne kliknite.
5. Slab stil pisanja – najprej opazite zadevo in besedilo sporočila. Večinoma so napisani v angleščini. Prav tako je lahko sporočilo v zelo slabi slovenščini, ki jo običajno iz angleščine samodejno prevede kateri od spletnih prevajalcev. Če vas e-pošta sili, da nekaj prenesete ali kliknete na povezavo, je verjetno virus.
6. Če vas e-pošta pritiska, da nekaj prenesete ali kliknete na povezavo, je verjetno virus.


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 Primer e-poštnega sporočila, ki zahteva klik na povezavo

Poleg zgoraj opisanih goljufij je na spletu (pa tudi v resničnem svetu) prisotno: Nasilje na spletu - grozilna ali izsiljevalska sporočila, nadlegovanje, žalitve, širjenje neresnic, objava zasebnih podatkov, montaže, spolno nadlegovanje. , in podobno Temu so izpostavljeni predvsem otroci.

Ker se je uporaba digitalnih tehnologij v vsakdanjem življenju izjemno razširila, se je povečalo tudi število ljudi, ki so od njih odvisni. To postaja vse večji problem predvsem med mlajšimi,

njegovo reševanje oziroma iskanje pametnega razmerja med realnim in virtualnim svetom pa bo vse bolj aktualno. Zato je pomembno, da mu pri poučevanju digitalnih veščin posvetimo ustrezno pozornost.