VARSTVO PRED SPLETNIMI PREVARAMI

MIRKO JAVERŠEK
Šolski center Kranj, Kranj, Slovenija
mirko.javersek@sckr.si

Družbena odgovornost, kritično mišljenje ter kreativnost so temeljne agende v postmodernem svetu. Družbeno odgovornost lahko razširimo tudi na širše – spletno okolje. Tako smo vsak trenutek izpostavljeni novim tehnološkim izumom in napravam, pa tudi nenehno novim načinom uporabe tehnologije, na prvi pogled učinkovitejše. Bolj podroben pogled, pa ob navidezni večji storilnosti pokaže, da se počasi oddaljujemo in odtujujemo od bistva. Obdaja nas tehnologija, ki jo včasih tudi ne znamo uporabljati na ustrezen način. Raznovrstna družbena omrežja, spletni forumi ter vedno nove ob aplikacija predstavljajo vir in novo okolje za profesionalno delo in tudi preživljanje prostega časa. Ta nova okolja pa nosijo s seboj tudi precejšnja varnostna tveganja. Internet predstavlja zelo uporabno in skorajda nujno orodje za urejanje, deljenje ter dostop do podatkov za vsakršne namene. Tako moramo danes, bolj kot kdaj koli, poznati njegovo delovanje in pasti, ki prežijo na nas. Sobivanje z novimi načini uporabe tehnologije postaja zahtevnejše.

DOI
https://doi.org/10.18690/um.fov.2.2025.27

ISBN
978-961-286-963-2

Ključne besede:
kritično mišljenje,
kreativnost,
internet,
družbena omrežja,
varnostna tveganja

Univerzitetna založba Univerze v Mariboru

DOI
https://doi.org/
10.18690/um.fov.2.2025.27

ISBN
978-961-286-963-2

Keywords:
critical mind,
creativity,
internet,
social media,
security risk

PROTECTION AGAINST ONLINE SCAMS

MIRKO JAVERŠEK
School Centre Kranj, Kranj, Slovenia
mirko.javersek@sckr.si

Nature conservation and environmental protection are fundamental agendas in our postmodern world. The security of the environment can also be extended to the wider online environment. Thus, every moment we are exposed to new technological inventions and devices, as well as constantly new ways of using technology, at first glance more efficient. A more detailed look, however, with apparent greater productivity, shows that we are slowly drifting away and alienating ourselves from the essence. We are surrounded by technology, which sometimes we don't even know how to use properly. Various social networks, online forums and new applications are a source and a new environment for professional work and leisure. These new environments also carry significant security risks. The Internet represents a very useful and almost necessary tool for editing, sharing and accessing data for any purpose. So today, more than ever, we need to know its operation and the pitfalls that lie in wait for us. Coexistence with new ways of using technology is becoming more challenging. Let's look back to the bottom line and sharpen our perspective on the fact that we are in fact leading by example. In the eyes of male and female colleagues, male and female students, male and female students, we are not what we say, but what we live. Thus, in addition to nature conservation and environmental protection, we must also keep in mind the protection of the online environment.

University of Maribor Press

1 Uvod

Živimo v hitro razvijajočem se svetu, kjer smo vsak trenutek izpostavljeni novim tehnološkim izumom in napravam, poleg tega pa tudi nenehno novim načinom uporabe tehnologije. V življenju smo že od začetka obdani s tehnologijo, ki jo včasih tudi ne znamo uporabljati na ustrezen oziroma pravilen način. Razna družbena omrežja, spletni forumi ter nove aplikacija predstavljajo novi vir in novo okolje za preživljanje prostega časa, vendar ta okolja nosijo s seboj tudi določena varnostna tveganja.

Internet predstavlja zelo uporabno in skorajda nujno orodje za urejanje, deljenje ter dostop podatkov za vsakršne namene, zato pa moramo danes bolj kot kdaj koli poznati njegovo delovanje in pasti, ki se tam pojavljajo.

Glede varnosti je potrebno omeniti pomembne dejavnike, ki pomagajo do regulacije objave osebnih podatkov, varnosti pred zlonamernimi kodami ter lažnimi objavami na internetu, tj. preventiva in seznanjanja uporabnikov interneta o tveganjih javne objave podatkov, medijske pismenosti ter splošne seznanitve z zlonamernimi kodami kot način, da pridemo do kritičnih in zdravih uporabnikov interneta.

V zadnjih letih čas, ki ga preživimo na spletu, konstantno narašča, prav tako pa tudi narašča število ljudi, ki do spleta dostopa. Današnjo generacijo predvsem pa otroke in mladino lahko poimenujemo tudi digitalna generacija, saj odraščajo s tehnologijo in so v stiku z njo praktično vsakodnevno že od malih nog. Današnji uporabniki interneta tako predstavljajo zelo pomembne medijske uporabnike, predvsem zato, ker bodo s tehnologijo v stiku vse življenje. Včasih smo si želeli nove igrače (lego kocke), danes pa nov zmogljiv mobilni telefon ali celo kaj več v zvezi z digitalizacijo. Pri oblikovanju teh navad igra ozaveščanje pred nevarnostjo zelo močno vlogo, saj se moramo zavedati nevarnosti internetne tehnologija z namenom, da jo bomo lahko varno in odgovorno uporabljali (Grilc, 2017).

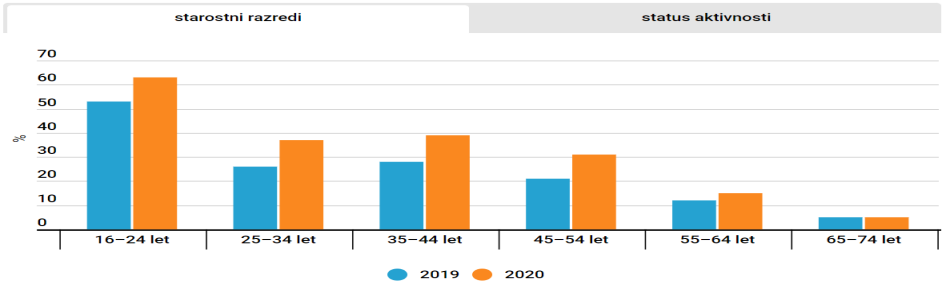
Uporaba informacijsko-komunikacijske tehnologije (IKT) že nekaj časa predstavlja osrednji element sodobne družbe, zato bi bilo potrebno uporabnike te tehnologije že od malih nog poučiti pravilno uporabljati. Ali to dejansko počnemo? Osnovno znanje mladi dobijo v šoli, npr. uporaba orodij Microsoft Office, e-poštnega

nabiralnika, brskanje po spletu, itd, vendar bi morali mlade že od začetka poučiti o varnosti podatkov, zlonamernih kodah ter lažnih novicah.

2 Statistika uporabe interneta

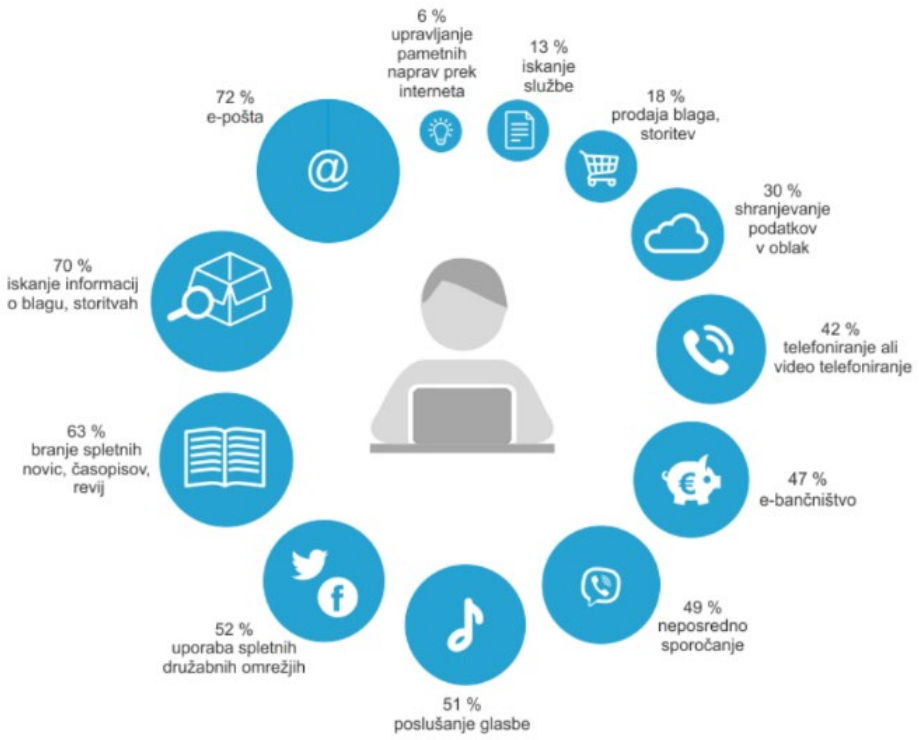
Po podatkih Statističnega urada Slovenije (SURS) ima v Sloveniji v letu 2023 dostop do interneta 93% delež gospodinjstev (osebe med 16 in 74 letom), 71% delež e-kupcev (osebe stare od 16 do 74 let ki so v zadnjih 12 mesecih nekaj naročil ali kupili preko spleta) ter 85% delež oseb (osebe med 16 in 74 letom), ki uporabljajo internet vsak dan ali skoraj vsak dan (SURS 2021).

Po podatkih SURS 2021 jih 27% starih od 16 do 74 let ni vedlo da imajo na svojem pametnem telefonu nameščen varnosti program, 4% pa jih je na svojem pametnem telefonu zaradi zlonamerne kode ali drugih vrst sovražnih programov izgubile informacije, dokumente, slike ali druge podatke (SURS 2021).



Slika 1: Delež oseb, starih 16–74 let, ki so se izobraževale prek interneta, Slovenija, 2019–2020
Vir: SURS, 2021

Slika 2: Koliko rednih uporabnikov interneta je v posamezni starostni skupini
Vir: SURS, 2021



Slika 3: Delež uporabnikov interneta (16 -74) po namenih uporabe interneta
Vir: SURS, 2021

3 Zlonamerna koda

Zlonamerna koda je izraz, ki se uporablja za opis katere koli kode v katerem koli delu programskega sistema ali skripte, ki naj bi povzročil neželene učinke, varnostne kršitve ali škodo na sistemu. Zlonamerna koda je varnostna grožnja aplikacije, ki je ni mogoče učinkovito nadzorovati samo s konvencionalno protivirusno programsko opremo. Zlonamerne kode opisujejo široko kategorijo sistemskih varnostnih izrazov, ki vključujejo napadne skripte, viruse, črve, trojanske konje, trojanska vrata in zlonamerno aktivno vsebino (VERACODE, 2021).

Zlonamerna koda lahko vključuje tudi časovne bombe, kriptografsko kodiranje podatkov, namerno uhajanje informacij in podatkov, rootkite in tehnike za preprečevanje odpravljanje napak. Te ciljne grožnje z zlonamerno kodo so skrite v

programski opremi, da se izognejo odkrivanju s tradicionalnimi varnostnimi tehnologijami.

Ko je zlonamerna koda v vašem okolju (računalniku, pametnemu telefonu, itd.), ta vstopi v omrežje in se širi. Zlonamerna koda lahko povzroči preobremenitev omrežja in poštnega strežnika s pošiljanjem e-poštnih sporočil, krajo podatkov in gesel, brisanje datotek in dokumentov, itd (Tekavec, 2021). Ločimo več vrst zlonamernih kod, ki jih predstavljam v nadaljevanju

3.1 Virus

Je vrsta zlonamerne programske opreme, ki se širi tako, da vstavi svojo kopijo v drug program in postane del drugega programa. Širi se z enega računalnika na drugega in med potovanjem pušča okužbe. Resnost virusov se lahko razlikuje vse od povzročanja zmerno nadležnih učinkov pa vse do škodovanja podatkov ali programske opreme. Skoraj vsi virusi so priloženi izvedljivi datoteki (.exe), kar pomeni da virus morda obstaja v sistemu, vendar ne bo aktiven ali se ne bo mogel širiti dokler uporabnik ne zažene ali odpre te izvedljive datoteke. Običajno gostiteljski program še naprej deluje, ko ga okuži virus zato ga je težko odkriti na golo oko. Virusi se širijo, ko se programska oprema ali dokument, ki vsebuje virus prenese iz enega računalnika na drugega z uporabo omrežja, diska, skupne rabe datotek ali okuženih e-poštnih prilog.

Najhujši računalniški virusi v zgodovini (Gerencer, 2020):

1. Mydoom – 38 milijard dolarjev v letu 2004
2. Sobig – 30 milijard dolarjev v leti 2003
3. Klez – 19.8 milijard dolarjev v leti 2001
4. ILOVEYOU – 15 milijard dolarjev v letu 2000
5. WannaCry – 4 milijarde dolarjev v letu 2017
6. Zeus – 3 milijarde dolarjev v letu 2007
7. Code Red – 2.4 milijarde dolarjev v letu 2001
8. Slammer 1.2 milijarde dolarjev v letu 2003
9. CryptoLocker - 665 milijonov dolarjev v letu 2013
10. Sasser – 500 milijonov dolarjev v letu 2004

3.2 Izsiljevalska programske koda (ang. Ransomware)

Ransomware je vrsta zlonamerne programske kode ki grozi, da bo objavila podatke žrtve ali pa trajno blokirala dostop do njih, ter šifrira razne diske, datoteke in mape, razen če je plačana odkupnina. Medtem ko lahko neka preprosta izsiljevalska programska oprema zaklene sistem na način, ki ga poznavalcem ni težko spremeniti, lahko tudi naprednejša koda popolnoma zaklene/šifrira dostop do nekih podatkov, ki jih brez ključa ni možno odkleniti. Velikokrat tudi po prejemu plačila ne dešifrirajo datotek, map ali diskov (Janhar, 2021).

Primer: CryptoLocker je bil eden najbolj donosnih pri izsiljevalskih programskih kodah. Med septembrom in decembrom 2013 je okužil več kot 250.000 sistemov in je ustvarjalec zaslužil več kot 4 milijone dolarjev preden je bil leta 2014 odstranjen.

Slika 4: Primer izsiljevanja
Vir: Canva

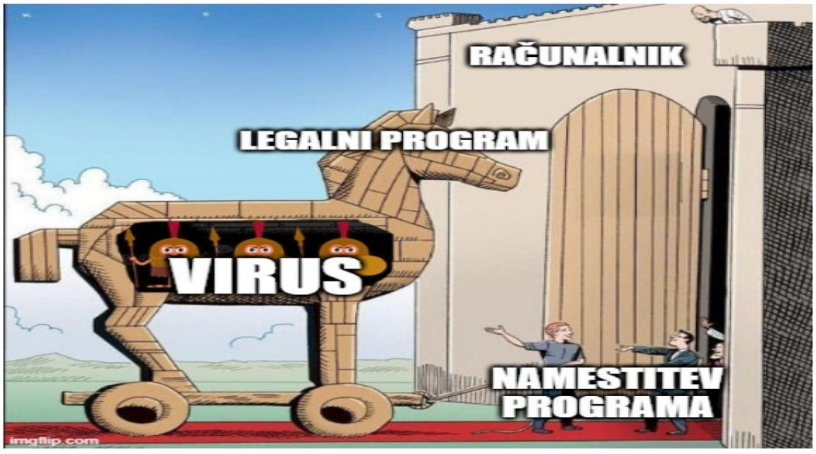
3.3 Črv (Worms)

So podobni računalniškemu virusu, ker se tudi razmnožujejo in lahko povzročajo enako vrsto škode. V nasprotju z virusi, ki zahtevajo širjenje okužene gostitelje datoteke, so črvi samostojna programska oprema in za širjenje ne potrebujejo

gostiteljskega programa ali človeške pomoči. Za širjenje izkoriščajo ranljivost sistema ali pa uporabljajo nekakšen socialni inženiring, da uporabnike ukanejo/zavedejo da jih poženejo. Črv vstopi v računalnik skozi ranljivost v sistemu in izkoristi funkcije prenosa datotek ali informacij v sistemu, kar mu omogoča potovanje brez pomoči. Naprednejši črvi uporabljajo tehnologijo šifriranja, brisanja ali kodiranja opreme, z namenom da škodijo svojim tarčam.

3.4 Trojanski konj

Je vrsta zlonamerne koda, ki je dobila ime po lesenem konju, so ga Grki uporabili za infiltriranje v Trojo. To je škodljiva programske oprema, ki na površini izgleda legitimna. Uporabniki so običajno zavedeni, da ga naložijo in izvedejo v svojih sistemih. Ko je naložen, lahko doseže poljubno število napadov na uporabnika, vse od draženja uporabnika (po skakanje oken ali spreminjanje namizij) pa vse do večjega škodovanja (brisanje datotek, krajo podatkov ali aktiviranje in širjenje druge zlonamerne programske opreme kot so virusi). Znano je tudi da trojanski konj ustvarja stranska vhodna vrata (ang. Backdoor), ki omogočijo dostop do sistema. Za razliko od virusov in črvov se trojanski konj sami ne razmnožujejo, tako da okužijo druge datoteke. Širijo se preko uporabniške interakcije kot je odpiranje e-pošte ali zagon nekih datotek, ki smo jih prenesli preko interneta.



Slika 5: Primer delovanja trojanskega konja
Vir: Canva

3.6 Stranska vhodna vrata (Backdoor)

Nedokumentiran način dostopa do sistema, ki zaobide običajne mehanizme preverjanja prisotnosti. Nekatera stranska vhodna vrata namesti tisti programer ki je ustvaril nek program, druga pa so nameščena s sistemsko ogroženostjo, kot je virus, črv ali trojanski konj. Napadalci običajno uporabljajo stranska vrata za lažji dostop do sistema, z namenom pridobivanja datotek, podatkov in informacij (Janhar, 2021).

3.6 Vohunska programska oprema (Spyware)

Vohunska programska oprema je splošno ime celo paleto programske opreme, ki nadzira uporabnikove aktivnosti, zbira informacije kot so pritisnjene tipke, snema zaslone in datotečne mape, vse to pa lahko shranjuje ali pošilja na oddaljeno lokacijo, seveda brez uporabnikovega privoljenja in zavedanja. Za razliko od računalniških virov in črvov, se vohunska programska oprema ne razmnožuje avtomatični, vendar pa vseeno izkorišča računalniške sisteme za komercialno korist. Znano je, da večina spletni strani, ki omogočajo prenašanje programov in datotek, poleg želenih datotek namesti tudi spyware. Nameščena je lahko na prikrite načine kot trojanski konj, del virusa in črva ali prenesen na skrit način.

3.7 Rootkit

Je zlonamerna koda, ki je izrecno narejena z namenom preminjanja procesov v operacijskem sistemu s čimer bi dosegel nestandardno delovanje. Rootkit spada med najbolj napredne tipe zlonamerne kode, ki so zgrajeni za delovanje v popolni prikritosti. Njihovo odkritje in odstranjevanje močno otežuje dejstvo, da se maskirajo in skrijejo med preostale neškodljive procese, ki potekajo na računalniku. Kljub temu, da jih ni popolnoma mogoče odkriti, pa je za navadnega uporabnika skoraj nemogoče, da jih odstrani, saj pri tem velikokrat ne uspe tudi za to specializiranim protivirusnim programom.

4 Obramba pred zlonamerno kodo

4.1 Protivirusni programi

Dobri protivirusni programi so nosilni stebri obrambe našega računalnika, saj se tega zavedajo tudi proizvajalci teh protivirusnih programov. Ponujajo nam zaščito pred virusi, črvi, trojanskimi konji in številnimi drugimi grožnjam.
So tri temeljne protivirusne tehnike:

1. Specifične metode odkrivanja
2. Tovrstne metode iščejo in identificirajo specifične tipe virusov. Ko je odkrita nova zlonamerna koda, jo strokovnjaki analizirajo, razstavijo njeno kodo in jo tako skušajo spoznati ter ugotoviti, kako jo v prihodnje prepoznati ter izbrisati. Glede na zapletenost zlonamerne kode je to lahko zelo dolg in zapleten proces.
3. Splošne metode odkrivanja virusa
4. Pri tej metodi se ne išče točno določene kode, ampak zgolj sumljivo aktivnost in nepooblaščene modifikacije procesov v računalniškem sistemu.
5. Preventivne metode
6. Tovrstne metode ustvarijo računalniško okolje, kjer zlonamerna koda »okleva« preden vstopi v sistem, ali pa se po vstopu ne more izvršiti. Večina teh tehnik vsebuje uporabo zdravega razuma.

4.2 Požarni zid

So poleg protivirusnih programov steber obrambe našega sistema pred zlonamerno kodo in vdori. Požarni zid bi lahko definirali kot nekakšen filter, ki identificira poskuse različnih aplikacij, ko le-te poskušajo preko spleta dostopati do našega računalnika. Pri požarnem zidu velja tudi obratno, in sicer nas obvešča o aplikacijah nameščenih na našem sistemu, ko skušajo dostopati do spleta. Se pravi, požarni zid nas ščiti pred potencialnimi zlonamernimi kodami, ko ta skuša dostopati do našega računalnika.

Poznamo požarne zidove:

1. Požarni zidovi s filtriranjem paketov
2. Je najbolj osnoven tip in filtrira le omrežni in transportni nivo. Deluje tako da sprejme paket in na podlagi nastavitev določi ustrezno dejanje in to dejanje izvrši na paketu.
3. Požarni zidovi, ki pregledajo celoten paket
4. Isto kot zgoraj, dodatno pa še nadzirajo stanje prispelih paketov.
5. Požarni zid na aplikacijskem nivoju
6. Ta tip lahko filtrira promet na omrežnem, transportnem in aplikacijskem nivoju.
7. Krožni požarni zidovi s prehodom
8. Je najmanj uporabljan in ne omogoča nikakršne večje zaščite, le da skrije omrežje ali posamezen računalnik na požarnim zidom.

5 Socialni inženiring

Pri socialnem inženiringu lahko po domačne povemo, da gre za prevaro s katero prevaranti pridejo do določenih zaupnih podatkov. Je ne tehnični vdor, ki se pretežno zanaša na človeške interakcije in pogosto vključuje prevare ljudi z namenom zaobiti varnostne postopke. Širša definicija je »tehnika, s katero ciljne osebe (žrtve) z uporabo poznavanja psihologije ljudi, delovanja računalniških sistemov in terminologije ter z uporabo majhnih in verjetnih laži pripravimo do tega, da ravnajo (ali pa opustijo neko ravnanje), ki v običajnih okoliščinah ko imamo opravke s tujci oz. nepoznanimi osebami, ne bi nikoli« (Pagon, 2021).

Pri socialnem inženiringu pride do tega da individualne osebe uporabljajo vpliv in prepričljivost za prevaro ljudi tako, da jih prepriča, da je socialni inženir nekdo, ki to ni oz. jih prevara z manipulacijo (Suša, 2009).

Razlika med hekerjem ter socialnim inženirjem je torej v tem, da socialni inženir ne potrebuje nujno vrhunskega računalniškega znanja, pač pa mora biti le prepričljiv in dobro poznati psihologijo človeka. Ta način kraje podatkov in ostalih nelegalnih početih je mnogo hitreje in cenejše od hekerskega vdiranja v sistem, vendar je za osebe in podjetja, ki pa hočejo svoje podatke zaščiti veliko bolje nevaren.

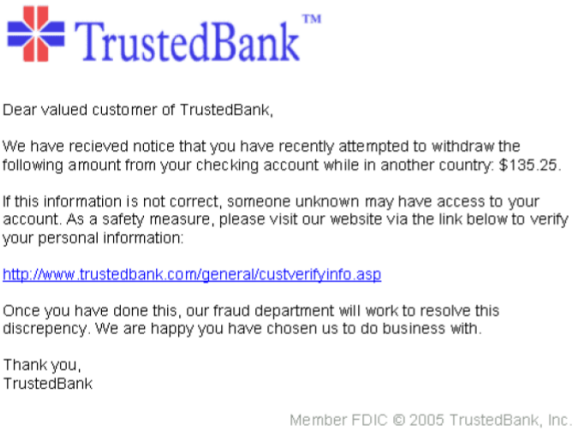
Pri socialnem inženiringu nam namreč bolj malo pomaga zaščitna tehnologija kot so protivirusni programi, požarni zidovi, posodobljeni računalniški sistemi, itd. Tukaj sta poglavitni zaščiti pazljivost in zdrava pamet vsakega posameznika. Poznamo več vrst socialnega inženiringa. Dominirajo v nadaljevanju opisane oblike.

5.1 Ribarjenje (Phishing)

Je najpogostejša vrste socialnega inženiringa na internetu. Ribarjenje je kraja podatkov s pomočjo ponarejenih elektronskih sporočil in spletnih strani. Najpogosteje ponarejene so strani finančnih organizacij, strani spletnih prodajaln oz. »oglasnikov« in ponudnikov internetnih storitev. Vse pogosteje pa so tarča ribarjenja socialna omrežja kot so Facebook, Twitter, Reddit, itd (Suša, 2009)..

Ribarjenje poteka nekako tako:

1. Prevarant najprej izbere organizacijo, za katero se bo izdajal in nato izdelal podobno oziroma identično stran
2. Ko je stran izdelana, potrebuje uporabnike, ki jih bodo nasedli
3. Potencialnim uporabnikom pošlje veliko e-sporočil
4. Pri sporočilu prevarant navede, da je prišlo do procesne napake in je potrebno ali resetirati geslo ali uporabniško ime.



Slika 6: Primer ribarjenja
Vir: Canva

Kako preprečiti ribarjenje:

1. Naučiti identificirati potencialne prevare
2. Preveriti vir prejetih sporočil – Pokličemo banko direktno in povprašamo
3. Nikoli ne klikamo na povezave v e-poštah

5.2 Pharming

Je zelo podobna prevari phishing, vendar se razlikuje v tem da jo je težje odkriti. Phraming je »preusmerjanje z legitimnih strani na nelegitimne z namenom pridobitve zasebnih podatkov«. Kako deluje? Domenski strežnik (DNS) je strežnik, ki poskrbi, da posamezniku da odpiranje neke strani kot je npr. www.ff.uni-lj.si ni potrebno v brskalnik vpisovati IP naslov te strani ki je npr, 193.2.106.66 (izmišljeno), pač pa le domeno, ki si jo je veliko lažje zapomniti. Se pravi DNS strežnih usmerja internetne domene na pravi IP naslov. Pharming pa spremeni DNS strežnik, ter nas usmerja na svoj (nepravi) IP naslov. Pharming napadov je več in sicer, sprememba host datotek na posameznem računalniku ali pa spremembe na routerjih oz. usmerjevalnikih. To se običajno izvede preko trojanskega konja.

5.3 Napad s posrednikom (man in the middle MITM)

Še bolj napreden napad kot je pharming je napad s posrednikom. Gre za napad kjer napadalec prestreza komunikacijo med dvema sistemoma kot na primer med uporabnikom in spletno banko. Tak način je težje prepoznati, saj vse strani delujejo normalno kot prej, ugotoviti da nam nekdo prisluškuje pa je zalo težko. Zaščita pred tem napadom je upraba vatnih povezav. Verjetno najboljša zaščita pa je uporaba dvofaktorne avtentikacije preko drugega komunikacijskega kanala (Telefon ali aplikacija).

5.4 Smishing

Podobna oblika kot ribarjenje vendar je preko SMS sporočil. Prejemnik dobi sporočilo na mobilni telefon od banke, spletne prodajalne ali druge finančne ustanove, kjer zahtevajo potrditev določenih podatkov, tako da kliknete na določeno povezavo ali pokličete na določeno telefonsko številko. Na ta način prevaranti

pridobijo zasebne podatke. Smishing je prevara, ki naj bi bila v porastu, prevaranti pa se je poslužujejo predvsem zato, ker smo uporabniki postali sumničavi na zahteve bank po elektronski pošti.

5.5 Vishing

Temelji na telefoniji preko interneta. Oblikovan je tako, da na več tisoč telefonskih številk pošljejo posneto telefonsko sporočilo različnih organizacij, ki zahtevajo določeno akcijo. Tako na primer zahtevajo, naj uporabnik pokliče klicni center, saj so zaznali, da je bila njihova kreditna kartica zlorabljena. Uporabnika nato v telefonskem pogovoru zaprosijo za številko kreditne kartice in kodo, da bi preverili, če je šlo res za napako, ter mu nato sporočijo, da je vse v redu.

5.6 Nigerijska pisma

So prevara preko e-pošt, v katerih se nekdo pretvarja, da je npr. sin nekega predsednika, uslužbenca, poslovneža, včasih tudi da so neka oddaljena žlahta, itd. V tej e-pošti pojasnjuje, da ima na račun večjo količino denarja, ki jo mora spraviti iz države oz. ne more dostopati do nje. Za pomoč prosi nas, v zameno pa nam obljubi določen odstotek nakazane vsote. Ko žrtev izkaže voljo za sodelovanje, mu običajno naročijo, naj nakažejo nekaj malega denarja za ureditev papirjev, itd. Zadeva se ponovno zatakne in si izmislijo drug izgovor, zakaj denarja ni še na računu in da ponovno potrebuje denar. To se ponovi večkrat, dokler prevarani ugotovi, da je vse skupaj prevara.

5.7 Zaščita pred socialnim inženiringom

Ultimativne zaščite pred socialnim inženiringom ni. Lahko le zmanjšujemo ali omilimo posledice. In če je prav človek tisti, ki je najšibkejši člen v tem sistemu obrambe, saj ha je zlahka prevarati, si lahko predstavljamo, da je ključni faktor obrambe izobrazba ljudi v smislu zavedanja tovrstnih prevar. Tak problem najlažje rešimo z informativnimi varnostnimi tečaji. Ljudi moramo naučiti postopkov in standardov, kako v takih primerih ukrepati.

Tovrstne napade lahko preprečimo (Pagon, 2021):

1. Z izobrazbo in poznavanjem problema. Z različnimi tipi prevar se tudi obramba od razlikuje od primera do primera.
2. Nikoli ne klikajte na priponke ali povezave v e-pošti – Če dobite neko e-pošto se izogibajte odpiranju priponk ali klikanju na neke povezave
3. Če dobite takšno e-sporočilo ja najbolje v primeru, da morate spremeniti geslo zaradi varnosti, obiskati spletno stran direktno preko brskalnika in ne preko povezav, ki so pritrjene na e- poštah.
4. Znano je, da podjetja nikoli od vas ne bodo zahtevala gesel. Se pravi če vas nekdo sprašuje po geslu potem takoj veste, da gre za prevaro
5. Uporaba programov za preprečevanje neželene e-pošte.

6 Gesla

Gesla preprečujejo nepooblaščeno uporabo osebnih podatkov, e-pošte, sporočil, klicev, spletne banke in družbenih omrežij. Glavna težava pri geslih je, da uporabnik pri oblikovanju gesel niso inovativni. Pogosto se gesla tako enostavna, da je le vprašanje časa, kdaj bodo nepridipravi vdrli v naše profile.

6.1 Velikost gesla

Pomembno je omeniti tudi Moorov zakon. Moč GPU in CPU se vsake dve leti podvoji, zato je tudi vedno lažje vdreti v gesla. To pomeni da če danes potrebujemo 120 let za vdor gesla, bomo čez 18 mesecev potrebovali 60 let in čez 26 mesecev bi potrebovali 30 let. Priporočljivo je da se gesla najmanj menjajo vsakih 30-90 dni, največ pa vsakih 1-2 leti

6.2 Varovanje gesel

NordPass je izvedel raziskavo v kateri je navedel, da naj bi si v povprečju individualna oseba morala zapomniti 100 različnih gesel (Rowe, 2021). Za individualno osebo je, da si mora zapomniti že 20-30 gesel preveliko, še posebej v današnjem času, ko je priporočljivo, da so gesla dolga in vsebujejo vsaj en znak, eno veliko črko in eno številko poleg tega pa naj nebi uporabljali osebnih podatkov pri geslih ter naj jih nebi ponavljalo za druge uporabniške račune.

	8 znakov	10 znakov	12 znakov
Samo male črke	Takoj	Takoj	Nekaj tednov
+ 1 velika črka	pol ure	1 mesec	5 let
+ 1 številka	eno uro	6 let	2 tisoč let
+ 1 simbol	en dan	50 let	63 tisoč let

Slika 7: Obseg gesla
Vir: Lasten

Slaba gesla:

- enaka gesla za več storitev
- zaporedje znakov (12345678 ali qwert ali asdfgh)
- izražanje čustev v geslih (»ljubimte«, »ljubezen«, »sranje«)
- ime kot geslo (cocacola, linkedin, facebook)

Dobra gesla:

+ za vsako spletno stran drugo geslo
+ vsaj 8 znakov dolga gesla
+ kombinacija malih, velikih črk, ter številk in znakov
+ izogibanje splošnih imen
+ izogibanje uporabe osebnih podatkov (imena, datum rojstva)
+ redno spreminjajte gesla

Glede na to, da si moramo v današnjem času zapomniti toliko različnih in dolgih gesel, je priporočljiva uporaba programov kateri nam omogočajo shranjevanje teh gesel, pri tem pa je program sam zaščiten z zelo dolgim geslom ter dvojno faktorsko avtentikacijo (2FA).

7 Deepfake

Je digitalni ponaredek, ustvarjen s pomočjo globokega učenja. Deepfake lahko ustvari popolnoma novo ali manipulira že obstoječo vsebino, prav tako pa video, zvok (avdio), fotografije – grafiko in tekst. Lahko se uporablja za očrnitev ugleda izbranih žrtev, lažno oponašanje določenega politika ali funkcionarja za izsiljevanje, ter za kibernetske kriminalne operacije (Zadravec, 2020).

Manipulirana vsebina je za družbo problematična že z vidika manipuliranja samega in njegovih posledic. V družbi je velik poudarek na vplivu deepfake-ov na političnem in demokratičnem področju, vendar nebi smel biti zapostavljen na posameznika, predvsem zasebnika. Ko je javnost, preko deepfake.ov, opremljena s tehnologijo zavajanja, lahko uspešno zavaja druge, zato so na udaru vsa področja družbenega zasebnemu kot tudi poslovnemu ugledu posameznika in institucij. Znotraj družbe negativne posledice deepfak-ov občutijo tudi organizacije. Mnogo podjetij in organizacij lahko postane tarča raznih prevar in goljufij. Deepfake-i so lahko tudi grozeči zaradi izsiljevanja podjetij in organizacij preko algoritmov (Zadravec, 2020).

8 Zaključek

Spletni socialni inženiring, zlonamerne kode, manipuliranje podatkov ter slaba ozaveščenost ljudi glavni vir pridobivanja podatkov posameznikov ter podjetij in organizacij, in je vse pogostejša. Poznani so številni primeri zlonamernih napadov, a je kljub temu zaskrbljujoče dejstvo, da je osveščenost še vedno prenizka.

Zavedati se moramo, da se tehnologija posodablja in izboljšuje iz dneva v dan je vsem tem spremembam težko slediti. Zaradi tega se morajo ljudje, ki so v dobi tehnologije in ki odraščajo v dobi tehnologije zavedati, da niso nedotakljivi

Samoozaveščanje bi se moralo pričeti že pri starših, da bi lahko to informacijsko znanje prenašali na svoje otroke, saj jim le-ti najbolje zaupajo že od ranih let. Poleg tega pa bi morali izobraževanje, vsaj v osnovni meri, izvajati tudi v šolah. Danes se skoraj vse modernizira, ljudje opravijo veliko dela na pletu in pametnih napravah in prav zaradi tega bi jim morali pojasniti nevarnosti in posledice.

Res je, da vseh napadov ne bomo uspeli preprečiti, saj se dogajajo iz dneva v dan z novimi tehnikami. Lahko pa opozorimo in poučimo o najbolj pogostih napakah in tako preprečimo nepotrebne žrtve. Poleg tega jim bo redno ozaveščanje o spletnem socialnem inženiringu, zlonamernih kodah ter lažnimi informacijami predstavilo nove tehnike napadov, ki se razvijajo iz dneva v dan in bodo tako nanj bolj pozorni.

Literatura

Gerencer, T. (2020, November 4). The Top 10 Worst Computer Viruses in History. Pridobljeno na https://www.hp.com/us-en/shop/tech-takes/top-ten-worstcomputer-viruses-in-history dne 10.8.2024

Grilc, T. (2017). (Ne)varnost mladih na spletu. Pridobljeno na http://dk.fdv.uni-lj.si/diplomska_dela_1/pdfs/mb11_grilc-tim.pdf dne 10.8.2024

Horvat, J. (2018). Zloraba kombinacije obratnega inženirstva, prikrivanja, ukan in varnostnih ranljivosti. Pridobljeno na http://eprints.fri.uni-lj.si/4203/1/63140081-JAN_HROVAT-Zloraba_kombinacije_obratnega_in%C5%BEenirstva%2C_prikrivanja%2C_ukan_in_varnostnih_ranljivosti.pdf dne 10.8.2024

Janhar, N. (2021). Razkrivanje zlonamerne zmaličene kode. Pridobljeno na https://repozitorij.uni-lj.si/Dokument.php?id=140399&lang=slv dne 10.8.2024

Kolbezen, D. (2018, Junij). Privilegirani uporabniki in varna uporaba gesel. Pridobljeno na http://revis.openscience.si/Dokument.php?id=4738 dne 10.8.2024

Pagon, U. (2021, Junij). Zavedanje mladostnikov glede nevarnosti spletnega socialnega inženiringa. Pridobljeno na https://dk.um.si/Dokument.php?id=150543 dne 10.8.2024

Rowe, A. (2021, November). Study Reveals Average Person Has 100 Passwords. Pridobljeno na https://tech.co/password-managers/how-many-passwords-average-person dne 10.8.2024

Suša, M. (2009). Socialni inženiring na internetu. Pridobljeno na http://dk.fdv.uni-lj.si/diplomska_dela_1/pdfs/mb11_susa-milos.pdf dne 10.8.2024

SURS (2022). Uporaba ITK v gospodinjstvih. Pridobljeno na https://www.stat.si/StatWeb/Field/Index/2989 dne 10.8.2024

SURS (2022). Varnost pri uporabi interneta med prvim valom epidemije covida-19. Pridobljeno na https://www.stat.si/StatWeb/News/Index/9359 dne 10.8.2024

Tekavec, P. (2021, September). Zlonamerna koda kot grožnja informacijski varnosti. Pridobljeno na https://dk.um.si/Dokument.php?id=25293 dne 10.8.2024

Tertinek, T., M. (2020). Lažne novice in njihovo omejevanje. Pridobljeno na https://dk.um.si/Dokument.php?id=146165 dne 10.8.2024

Zadravec, J. (2020, September). Deepfake ali globoki ponaredki in njihov vpliv na medije ter družbo. Pridobljeno na https://dk.um.si/Dokument.php?id=146927 dne 10.8.2024

Žbogar, M. (2009, Julij). Zasebnost in internet. Pridobljeno na https://dk.um.si/Dokument.php?id=12392 dne 10.8.2024