

VARNOST V DIGITALNEM SVETU

**Praktične rešitve za starejše z
analizo študij primerov
kibernetske kriminalitete**



VSEBINA:

1. POGLAVJE

KIBERNETSKI NAPADI IN INTERNETNA VARNOST

- Napad prek omrežij Wi-Fi (zasebnih in javnih)
- Napadi prek e-pošte
- Napadi na šibka gesla
- Phishing ("Ribarjenje")
- Zlonamerna programska oprema in računalniški virusi

2. POGLAVJE

FINANČNE IN NALOŽBENE PREVARE

- Finančne in naložbene manipulacije
- Navidezni altruizem: dobrodelna prevara
- Mamljive iluzije: izmišljene nagrad, loterije in nagradne igre
- Prevare z digitalnimi valutami
- Mednarodne finančne prevare

3. POGLAVJE

SOCIALNA MANIPULACIJA IN ČUSTVENA PREVARA

- Prevare v odnosih - romantične prevare
- SMS prevare - Smishing
- Telefonske prevare starejših - Vishing
- Prevare, ki izkoriščajo čustvene družinske vezi
- Prevare, ki vključujejo medicinske izdelke

4. POGLAVJE

PREVARE PRI SPLETNIH TRANSAKCIJAH

- Prevare pri potovanjih in nakupu vozovnic
- Prevare z naročninami
- Prevare pri ustvarjanju lažnih spletnih trgovin
- Prevarantski nakupi prek spletnih oglasov (nakup)
- Prevarantski nakupi prek spletnih oglasnikov (prodaja)

5. POGLAVJE

MANIPULACIJA IDENTITETE IN IZKORIŠČANJE JAVNEGA ZAUPANJA

- Obtožbe o vpletenosti v kazniva dejanja
- Manipulacije pri prevarah z lažnim predstavljanjem javnih institucij
- Manipulacija s tehnologijo deepfake
- Storitvene prevare z lažnim predstavljanjem državnih institucij
- Prevara z lažnimi računi



Sodobna tehnologija postaja vse bolj vpeta v naša življenja, kar poudarja ključen pomen varnosti v virtualnem svetu. To vprašanje je še posebej pomembno za starejše, ki pogosto niso vešči sodobnih tehnologij in so bolj izpostavljeni kibernetским grožnjam. E-knjiga »Varnost v digitalnem svetu. Praktične rešitve za starejše z analizo študij primerov kibernetiske kriminalitete« ponuja potrebno znanje in orodja, ki starejšim pomagajo pri zaščiti pred grožnjami na internetu.

Ta e-knjiga je bila ustvarjena kot del projekta "Cyber Safe Senior" številka 2023-1-PL01-KA220-ADU-000160325, ki ga financira Evropska unija. Namen tega projekta je ozaveščanje starejših o pravilih internetne varnosti in razvoj njihovih digitalnih veščin. Kot odziv na vse večje povpraševanje po izobraževanju o varni rabi interneta projekt ponuja praktične nasvete, študije primerov in analize, ki starejšim pomagajo pri izogibanju nevarnostim in odzivanju v izrednih razmerah.

E-knjiga vsebuje poglavja o različnih vidikih kibernetiske varnosti, kot so kibernetiski napadi, finančne prevare, družbena manipulacija, prevare pri spletnih transakcijah in kraja identitete. Vsako poglavje vsebuje študije primerov, ki ponazarjajo delovanje kibernetiskih kriminalcev in kažejo, kako se pred njimi učinkovito ubraniti. Zaradi praktičnih nasvetov je ta e-knjiga dragocen vir znanja za starejše, ki želijo varno uporabljati sodobne tehnologije.



V okviru projekta smo pripravili edinstvena gradiva, ki poleg dragocenega znanja pritegnejo in zanimajo uporabnike. Eden ključnih elementov so profesionalno pripravljene video posnetki – pet dinamičnih, vizualno privlačnih videov, ki na dostopen način ponazarjajo realne situacije, potencialne grožnje in ustrezne odzive na nevarnosti. Videi so namenjeni izobraževanju s praktičnimi primeri, zaradi česar je podane informacije lažje razumeti in si jih zapomniti.

Pripravili smo tudi interaktivni paket kvizov, ki so bili razviti na način, ki ni samo poučen, ampak tudi zanimiv in zabaven, tako da lahko udeleženci preverjajo svoje znanje in se ob tem zabavajo. Takšna oblika vključevanja prejemnikov ne le poveča privlačnost sporočila, temveč tudi njegovo učinkovitost, saj zagotavlja, da bo pridobljeno znanje dlje časa ostalo v njihovi zavesti.

Elementi, ki združujejo izobraževanje in zabavo, naredijo projekt ne le dragocen, ampak tudi privlačen in prijeten za vsakega prejemnika.



VIDEOPOSNETKI:

Čustvena manipulacija – dobrodelna prevara

Finančna manipulacija

Razbijanje gesel

Lažno predstavljanje in deepfake

Pasti spletnega nakupovanja

KVIZI:

SMS-prevare: Kako dobro se lahko zaščitite?

E-poštni napadi, prevare z lažnim predstavljanjem, tveganja uporabe šibkih gesel ter zlonamerna programska oprema in računalniški virusi.

Lažno predstavljanje in tehnologije deepfake.

Nakup in prodaja prek spleta: ali lahko opazite grožnje?

Finančna manipulacija in izkoriščanje čustev starejših.

1. POGLAVJE

KIBERNETSKI NAPADI IN INTERNETNA VARNOST

V današnjem digitalnem svetu so starejši vedno bolj ranljivi za kibernetiske napade, ki ogrožajo njihovo spletno varnost. V tem poglavju bomo razpravljali o metodah napada in varnostnih ukrepih, ki lahko starejšim pomagajo, da se zaščitijo pred grožnjami.

Napadi na Wi-Fi vključujejo zasebna in javna omrežja, ki jih kriminalci lahko uporabijo za prestrezanje podatkov. Pomembno je razumeti tveganja uporabe javnih dostopnih točk in znati prepoznati varna omrežja Wi-Fi.

E-poštni napadi, kot je lažno predstavljanje, pošiljajo lažna sporočila, ki so videti kot da prihajajo od zaupanja vrednih institucij z namenom, da bi pridobili osebne podatke. Šibka gesla pa so še ena težava, ki lahko olajša dostop do zasebnih računov.

Zlonamerna programska oprema in virusi predstavljajo resno nevarnost, saj se lahko infiltrirajo v naprave in ukradejo podatke. Razpravljali bomo o zaščitnih metodah, kot so redne posodobitve, protivirusna programska oprema in izogibanje sumljivim povezavam.

Osredotočili se bomo na praktične nasvete in strategije, ki bodo starejšim pomagali razumeti tovrstna tveganja in se jim izogniti ter zaščititi njihove podatke in zasebnost na spletu.

Napad prek omrežij Wi-Fi (zasebnih in javnih)

— ZNAČILNOSTI NEVARNOSTI:

Javna omrežja Wi-Fi omogočajo brezplačen dostop do interneta in so zelo priročna. Na voljo so na številnih javnih mestih, vključno s knjižnicami, kavarnami, letališči, restavracijami in hoteli. Vendar odprta omrežja Wi-Fi že dolgo veljajo za tvegano spletno okolje za vaše podatke. Čeprav nobeno omrežje Wi-Fi ni popolnoma varno, je varnost vaših zasebnih podatkov v veliki meri odvisna od vrste omrežja Wi-Fi. Napadi na omrežja Wi-Fi, tako zasebna kot javna, so lahko različnih oblik.

Tu je pet vrst takih napadov:

Pri napadu MitM (*Man-in-the-Middle*) napadalec prestreže komunikacijo med dvema napravama v omrežju Wi-Fi tako, da se izdaja za eno od strank. S tem lahko brez vednosti uporabnikov pridobi podatke, kot so prijave, gesla ali bančne informacije.

Pri napadu *Evil Twin* (*Zlobni dvojček*) napadalec ustvari lažno omrežje Wi-Fi, ki je na prvi pogled videti enako legitimnemu omrežju. Uporabniki, ki mislijo, da se povezujejo s pravim omrežjem, se povežejo z lažnim omrežjem in napadalcu omogočijo prestrazanje vseh posredovanih podatkov.

Napad tipa
"Človek
vmes" (Man-
in-the-
Middle)

Napad tipa
"Zlobni
dvojček"
(Evil Twin)

Napad prek omrežij Wi-Fi (zasebnih in javnih)



ZNAČILNOSTI NEVARNOSTI:

Napad tipa "Z grobo silo" na geslo za Wi-Fi (Brute Force Attack)

Napadalec poskuša uganiti geslo za Wi-Fi s pomočjo programov, ki sistematično testirajo različne kombinacije znakov. Če je geslo šibko ali preenostavno, je ta napad lahko učinkovit in omogoča nepooblaščen dostop do omrežja.

Napad tipa "Vohanja paketov" (Packet Sniffing)

Pri tem napadu napadalec uporablja posebno programsko opremo za zajemanje in analizo podatkovnih paketov, poslanih prek omrežja Wi-Fi. Tudi v zavarovanem omrežju, če podatki niso pravilno šifrirani, jih je mogoče prebrati in uporabiti.

Napad tipa "Zavrnitev storitve" (Denial of Service)

Pri napadu DoS (Denial of Service) napadalec pošlje veliko število neveljavnih zahtev ali lažnih signalov za razveljavitev dostopne točke Wi-Fi, kar povzroči prezasedenost omrežja. To lahko začasno onemogoči ali prekine omrežje, kar uporabnikom prepreči uporabo povezave.

Napad prek omrežij Wi-Fi (zasebnih in javnih)



POSLEDICE:

Uporaba javnega in brezplačnega dostopa do interneta prinaša številne nevarnosti, ki lahko ogrozijo občutljive podatke in spletno varnost. Pomembno je vedeti, kakšna so tveganja pri uporabi javnih omrežij Wi-Fi.

Posledice različnih vrst napadov na Wi-Fi omrežje:

01 Človek vmes (MitM)

Starejši lahko postanejo žrtve kraje identitete ali izgubijo svoje prihranke, če kriminallec prestreže podatke za prijavo na bančne račune ali spletna mesta za družabna omrežja.

02 Zlobni dvojček (Evil Twin)

Uporabniki lahko nevede posredujejo svoje prijavnne podatke, številke kreditnih kartic ali druge občutljive podatke, saj mislijo, da uporabljajo varno omrežje.

Napad prek omrežij Wi-Fi (zasebnih in javnih)



POSLEDICE:

03 Surova sila (Brutte Force)

Če starejši uporabljajo preprosta ali ponavljajoča se gesla, lahko kriminalci pridobijo dostop do njihovih omrežij, kar lahko privede do kršitev zasebnosti in višje račune za internet.

04 Vohanje paketov (Packet Sniffing)

Starejši so lahko v nevarnosti, da razkrijejo zasebne informacije, kot so e-poštni naslovi, gesla in osebni podatki, če napadalci prestrežejo nešifrirane podatke.

05 Zavrnitev storitve (Denial of Service)

Napad DoS (Denial of Service) lahko prepreči starejšim dostop do interneta, kar je še posebej problematično za tiste, ki se zanašajo na tehnologijo za komunikacijo z ljubljene ali pri urejanju vsakodnevnih opravil.

Napad prek omrežij Wi-Fi (zasebnih in javnih)

— NAČINI ZAŠČITE:



Filip se je odločil, da bo večerjal v bližnji restavraciji. Z uporabo javnega Wi-Fi-ja restavracije je odprl svojo e-pošto, da bi preveril najnovejše novice. Na žalost, ker se ni zavedal nevarnosti, povezanih z javnimi omrežji Wi-Fi, svoje povezave ni zavaroval. Zaradi napada *Man-in-the-Middle* (Človek vmes) je kriminallec prestregel njegove e-poštne podatke za prijavo, kar je povzročilo nepooblaščen dostop do njegovega računa in morebitno razkritje zaupnih informacij.



Filipova zgodba ni neobičajna in se ne dogaja samo starejšim. Vendar je to mogoče popraviti. Preberite si moje nasvete.

Posledice neprepoznavanja grožnje:

1. KORAK: Napad na Wi-Fi omrežje v restavraciji na javnem mestu

Filip je v restavraciji uporabil javno Wi-Fi omrežje, da bi preveril svojo elektronsko pošto. Pomanjkanje ustreznih varnostnih ukrepov, kot je npr. dvofaktorska avtentikacije, je kriminalcu omogočilo prestrezanje podatkov za prijavo.

2. KORAK: Nepooblaščen dostop do elektronske pošte

Zaradi napada je kriminallec pridobil nepooblaščen dostop do Filipovega e-poštnega računa in pridobil občutljive podatke, kot so zasebna korespondenca, kontakti in drugi zaupni podatki.

3. KORAK: Uhajanje zaupnih informacij

Prezem e-poštnega računa lahko povzroči morebitno uhajanje Filipovih zaupnih podatkov, kar lahko ogrozi njegovo zasebnost in varnost. Kriminallec bi te podatke lahko uporabil za goljufijo, krajo identitete ali druge nezakonite dejavnosti.

4. KORAK: Čustvene posledice

Philip je doživljal stres, tesnobo in izgubo zaupanja pri uporabi javnih omrežij Wi-Fi. Poleg tega lahko potreba po spremembi gesel, nadzoru računov in ukrepanju za preprečevanje nadaljnjih napadov zahteva dodaten čas in trud.

Napad prek omrežij Wi-Fi (zasebnih in javnih)

— NAČINI ZAŠČITE:

Takšnim posledicam se lahko izognete tako, da sledite spodnjim metodam in se zaščitite pred napadi prek omrežja Wi-Fi.



Uporabite močna gesla:

Zavarujte svoje omrežje Wi-Fi z močnim, edinstvenim geslom. Zapomnite si, da ne smete uporabljati očitnih gesel, kot so ime, priimek, datum rojstva ali druge lahko uganljive kombinacije znakov.

Posodobite programsko opremo:

Redno posodablajte programsko opremo usmerjevalnika za zaščito pred znanimi varnostnimi ranljivostmi.



Napad prek omrežij Wi-Fi (zasebnih in javnih)



NAČINI ZAŠČITE:



Omogočite šifriranje:

Prepričajte se, da so vsi podatki med prenosom šifrirani, tudi v zavarovanih omrežjih Wi-Fi.

Izogibajte se javnim omrežjem Wi-Fi:

Če je le mogoče, se izogibajte uporabi javnih Wi-Fi omrežij za prenos občutljivih podatkov. Če jih morate uporabljati, uporabite virtualno zasebno omrežje (VPN).



Nadzorujte svoje omrežje:

Redno preverjajte, katere naprave so povezane z vašim omrežjem Wi-Fi, da hitro odkrijete nepooblašcene naprave.

Napadi prek e-pošte

— ZNAČILNOSTI NEVARNOSTI:

E-poštni napadi so zlonamerni poskusi pridobitve nepooblaščenega dostopa do sistemov ali informacij prek e-poštnih računov. Starejši so ranljivi za številne vrste napadov. Vredno se je seznaniti z nekaterimi najpogostejšimi.

Glavne vrste napadov na e-poštne predale:

Ribarjenje (Phishing) je običajna metoda, pri kateri goljufi pošiljajo lažna e-poštna sporočila, za katera se zdi, da prihajajo iz zaupanja vrednih virov (npr. bank, državnih uradov).

Akcija goljufov:

- Lažne povezave in priloge: goljufi pošiljajo sporočila s povezavami do lažnih spletnih mest ali prilogami, namenjenimi pridobivanju občutljivih podatkov, kot so gesla in številke kreditnih kartic.
- Ustvarjanje občutka nujnosti: e-poštna sporočila pogosto vključujejo informacije o težavah z vašim računom, potrebo po nemudoma posodobitvi vaših podatkov ali opozorila o sumljivi dejavnosti.

Harpuniranje (Spear phishing) je naprednejša oblika lažnega predstavljanja, pri kateri so napadi prilagojeni in usmerjeni na določene osebe.

Akcija goljufov:

- Personalizirana sporočila: goljufi zbirajo podatke o žrtvi iz javnih virov, kot so družbeni mediji, da ustvarijo zakonita e-poštna sporočila.
- Izdajanje za prijatelja: Ta sporočila so pogosto videti, kot da jih pošilja oseba, ki jo žrtev pozna (npr. sodelavec iz službe).

**“Ribarjenje”
(Phishing)**

**“Harpuniranje”
(Spear Phishing)**

Napadi prek e-pošte

— ZNAČILNOSTI NEVARNOSTI:

Napad "Ponarejanje e- pošte" (Email Spoofing)

Pri napadu s ponarejanjem e-pošte goljufi spremenijo glave e-pošte, da se zdi, kot da so sporočila poslana iz zaupanja vrednega vira.

Akcija prevarantov:

- Lažne glave: Goljufi spreminjajo glave sporočil, da je videti, kot da so poslana z pravega naslova, na primer od prijatelja, šefa ali zaupanja vredne ustanove.
- Prikrivanje identitete: sporočila so videti pristna, zato jih prejemniki in sistemi za zaščito pred neželeno pošto težko zaznajo.

Napad "Zlonamerne" (Malware) in "Izsiljevalske" (Ransomware) programske opreme

Kibernetski kriminalci pogosto ugrabijo e-poštne račune za distribucijo zlonamerne programske opreme.

Akcija goljufov:

- Okužene priloge: e-poštna sporočila vsebujejo priloge, ki ob odprtju namestijo zlonamerno programsko opremo v računalnik žrtve.
- Zlonamerne povezave: E-poštna sporočila lahko vsebujejo povezave do spletnih mest, ki samodejno prenesejo in namestijo zlonamerno programsko opremo v vaš računalnik.

Napad "Človek vmes" (MitM) na e-poštno komunikacijo

Napad MitM se zgodi, ko napadalec prestreže in prenaša podatke med dvema stranema brez vednosti ene in druge strani.

Akcija goljufov:

- Prestrežanje podatkov: hekerji prestrežejo komunikacijo, da pridobijo občutljive informacije, kot so prijavni podatki ali skrivnosti podjetja.
- Ponarejanje e-pošte (Spoofing): pošiljajo lahko tudi sporočila v imenu ene strani, kar omogoča manipulacijo komunikacije.

Napadi prek e-pošte



ZNAČILNOSTI NEVARNOSTI:

Prevzem e-pošte ali napadi za prevzem

Hekerji poskušajo pridobiti dostop do vašega e-poštnega računa tako, da ugibajo vaše geslo ali uporabljajo druge metode.

Akcija goljufov:

- Ugibanje gesla: Hekerji lahko uporabijo tehnike, kot je groba sila (Brute Force Attack), da uganejo vaše geslo.
- Ribarjenje (Phishing): uporabijo lahko tudi ribarjenj ali druge tehnike socialnega inženiringa, da vas zavedejo, da jim posredujete svoje prijavnne podatke.

Napadi z zbiranjem prijavnih podatkov

Hekerji pridobijo dostop do e-poštnih računov tako, da uporabnike zavedejo, da jim posredujejo podatke za prijavo.

Akcija goljufov:

- Ribarjenje (Phishing): Uporabnik prejme e-poštno sporočilo z lažno zahtevo po podatkih za prijavo.
- Družbeni vpliv: Hekerji se pretvarjajo, da so nekdo drug, ter zahtevajo uporabniško ime in geslo, pri čemer pogosto uporabljajo informacije iz družbenih medijev, da bi bila njihova zahteva bolj verodostojna.

Napadi prek e-pošte



POSLEDICE:

E-poštni napadi imajo številne resne posledice, ki lahko ogrozijo zaupne podatke in spletno varnost. Da bi se zaščitili, je pomembno, da jih prepoznate.

01 Ribarjenje (Phishing)

- Kraja identitete: starejši lahko posredujejo svoje podatke za prijavo, številke kreditnih kartic, kar vodi do kraje identitete.
- Finančna izguba: prenos podatkov lahko povzroči nepooblaščne transakcije in finančne izgube.

02 Harpuniranje (Spear Phishing)

- Kršitev zasebnosti: starejši lahko delijo zaupne informacije, misleč, da komunicirajo z nekom, ki mu zaupajo.
- Finančne in čustvene izgube: lahko jih zmanipuliramo v dejanja, ki povzročijo finančne in čustvene izgube.

03 Napadi lažnega pošiljanja e-pošte (Email Spoofing)

- Kršitev varnosti: starejši lahko ukrepajo na podlagi napačnih informacij, kar vodi do kršitev varnosti.
- Namestitev zlonamerne programske opreme: klik na povezave ali priloge lahko vodi do namestitve zlonamerne programske opreme.

Napadi prek e-pošte



POSLEDICE:

04

Distribucija zlonamerne (Malware) in izsiljevalske (Ransomware) programske opreme

- Poškodbe sistema: zlonamerna programska oprema lahko poškoduje vaš računalnik in ga naredi neuporabnega.
- Izsiljevalska programska oprema: zlonamerna programska oprema lahko šifrira datoteke v vašem računalniku in za njihovo odklepanje zahteva odkupnino.

05

Napadi "človek vmes" (MitM) na e-poštno komunikacijo

- Izguba zaupnosti: starejši lahko nevede razkrijejo zaupne informacije.
- Manipulacija: napadalci lahko zavedejo obe strani komunikacije.

06

Prevzem e-pošte ali napadi za prevzem

- Kraja identitete: hakerji lahko dostopajo do občutljivih podatkov in jih uporabijo za krajo vaše identitete.
- Pošiljanje vsiljene pošte: ogrožene račune je mogoče uporabiti za pošiljanje neželene pošte in zlonamerne programske opreme.

07

Napadi z zbiranjem prijavnih podatkov

- Izguba dostopa: starejši lahko izgubijo dostop do svojih e-poštnih računov.
- Kršitev zasebnosti: hakerji lahko pridobijo dostop do zasebnih podatkov in korespondence.

Napadi prek e-pošte



NAČINI ZAŠČITE:



Danijel redno uporablja e-pošto, da ohranja stik s svojo družino. Njegov sin, ki živi v tujini, mu pogosto pošilja novice po elektronski pošti. Nekega dne je Danijel prejel e-pošto, za katero se je zdelo, kot da jo je poslal njegov sin.

Od: tom@primer.com

Zadeva: Nove počitniške fotografije!

Zdravo oče, upam, da je s tabo vse v redu. S tabo sem želel deliti fotografije z našega zadnjega potovanja. Če si jih želiš ogledati, klikni na spodnjo povezavo.

[Oglej si fotografije]

Lep pozdrav, tvoj sin

Posledice neprepoznavanja grožnje:

1. KORAK: Klik na povezavo

Danijel, misleč, da je prejel sporočilo od sina, je kliknil na povezavo.

2. KORAK: Okužba računalnika

S klikom na povezavo se je prenesla zlonamerna programska oprema in bila nameščena v Danijelov računalnik. Takšna programska oprema lahko sledi vaši spletni dejavnosti, ukrade gesla in druge zaupne podatke.

Napadi prek e-pošte

— NAČINI ZAŠČITE:

Danijelov primer kaže, kako nevarni so lahko napadi na e-poštne predale.

Povezava v sporočilu je vodila do spletne strani, ki je samodejno prenesla in namestila zlonamerno programsko opremo v njegov računalnik.



3. KORAK: Okužba računalnika

Zlonamerna programska oprema je pridobila dostop do Danijelovih osebnih podatkov, vključno s številkami bančnih računov, gesli za različne račune in zasebnimi dokumenti.

4. KORAK: Čustveni stres

Danijel se je počutil prevaranega, hkrati pa ga je skrbelo, da se nekdo lažno predstavlja kot njegov sin. Incident mu je povzročil stres in tesnobo.

Napadi prek e-pošte



NAČINI ZAŠČITE:

Takšnim posledicam se lahko izognete tako, da sledite spodnjim ukrepom za zaščito pred e-poštnimi napadi.



Bodite previdni pri odpiranju elektronske pošte:

Danijel bi moral biti previden pri odpiranju elektronske pošte.

Akcija:

- Vedno preverite e-poštni naslov pošiljatelja, še posebej, če sporočilo vsebuje povezave ali priloge.
- Natančno preberite sporočila in bodite pozorni na neobičajne zahteve in slovnične napake.

Posodobitve protivirusne programske opreme:

Danijel bi moral zagotoviti, da ima njegov računalnik in telefon redno posodobljeno protivirusno programsko opremo.

Akcija:

- Redno posodablajte protivirusno programsko opremo in skenirajte sistem.
- Namestite najnovejše posodobitve operacijskega sistema in spletnega brskalnika.



Napadi prek e-pošte

— NAČINI ZAŠČITE:

Dvofaktorska avtentikacija (2FA):

Danijel bi moral razmisliti o aktiviranju dodatne ravni varnosti z uporabo dvofaktorske avtentikacije (2FA) na vseh pomembnih računih. Ta pristop znatno poveča stopnjo varnosti, tudi če je geslo razkrito.

Akcija:

- Dodatna raven varnosti: uporaba 2FA na vseh pomembnih računih, kar poveča vašo raven varnosti, tudi če je vaše geslo razkrito.



O aktivaciji 2FA velja razmisliti:

- pri spletni prijavi v svoj bančni račun, da si zagotovite varen dostop do svojih sredstev,
- pri prijavi v svoj e-poštni račun, v katerem so shranjeni pomembni podatki in korespondenca,
- pri dostopu do platforme družabnih medijev, zlasti kadar se uporablja za komuniciranje z družino in prijatelji ter za deljenje osebnih fotografij in informacij.

Z upoštevanjem teh preventivnih ukrepov se lahko Danijel izogne številnim potencialnim grožnjam, povezanim z napadi po elektronski pošti in drugimi oblikami kibernetске kriminalitete.

Ne pozabite na moj nasvet, saj se boste z njim počutili bolj samozavestni pri uporabi interneta ter zaščitili svoje osebne in finančne podatke pred nepooblaščenim dostopom.



Napadi na šibka gesla

— ZNAČILNOSTI NEVARNOSTI:

Napadi na šibka gesla so ena najpogostejših metod kibernetских kriminalcev.

Glavne vrste napadov na e-poštne predale:

Slovarski napad vključuje testiranje velikega števila potencialnih gesel iz vnaprej pripravljenega seznama (slovarja). Ta seznam pogosto vključuje običajne slogane in različice besed. To je učinkovita metoda, če uporabnik uporablja gesla, ki jih je enostavno predvideti, kot so "geslo", "123456" ali "qwerty".

"Napad na slovar"
(Dictionary Attack)

Pri napadu s surovo silo napadalec sistematično preizkuša vse možne kombinacije znakov, dokler ne najde pravilnega gesla. Čeprav lahko ta vrsta napada traja dolgo, je lahko učinkovita predvsem za kratka in enostavna gesla.

"Napad s surovo silo"
(Brute Force Attack)

Ta napad uporablja podatke, zbrane iz prejšnjih uhajanj informacij, kot so prijavni podatki in gesla. Napadalci poskušajo uporabiti iste kombinacije prijavnega gesla na različnih spletnih mestih, pri čemer računajo na dejstvo, da uporabniki običajno uporabljajo iste podatke za prijavo na več spletnih mestih.

"Napad s polnjenjem poverilnic"
(Credential Stuffing Attack)

Čeprav ni neposreden napad z geslom, je lažno predstavljanje tehnika, ki poskuša uporabnike pretentati, da prostovoljno razkrijejo svoje prijavne podatke. Napadalci ustvarjajo lažna spletna mesta, ki so videti identična pravim spletnim mestom (npr. bančništvo, e-pošta) in pošiljajo e-poštna sporočila, ki potencialne žrtve spodbujajo k prijavi.

"Ribarjenje"
(Phishing)

Napadi na šibka gesla



POSLEDICE:

Napadi na šibka gesla imajo številne resne posledice za starejše in lahko ogrozijo vaše občutljive podatke in vašo spletno varnost. Da bi se zaščitili, je pomembno, da jih poznate.

01 Napad na slovar (Dictionary Attack)

Starejši, ki uporabljajo zlahka predvidljiva gesla, kot sta "geslo" ali "123456", lahko postanejo žrtve tega napada. Posledično je lahko kršena njihova zasebnost in ukradeni osebni ali finančni podatki.

02 Napad s surovo silo (Brute Force Attack)

Starejši ljudje, ki uporabljajo kratka in enostavna gesla, so ranljivi za napade s surovo silo. Kriminalci lahko dostopajo do svojih računov prek omrežja Wi-Fi, kar vodi do morebitnega uhajanja podatkov in kraje identitete.

03 Napad s polnjenjem poverilnic (Credential Stuffing Attack)

Starejši, ki običajno uporabljajo iste podatke za prijavo na več spletnih mestih, so ranljivi za to vrsto napada. To lahko povzroči nepooblaščen dostop do njihovih računov na različnih spletnih platformah.

04 Ribarjenje (Phishing)

Starejši, ki se morda manj zavedajo takšnih groženj, so dovzetni za lažno predstavljanje. Kriminalci lahko uporabijo ponarejena spletna mesta ali e-pošto, da žrtve ukanijo in na ta način pridobijo podatke za prijavo v njihov račun, kar lahko povzroči krajo identitete ali finančno izgubo.

Napadi na šibka gesla



NAČINI ZAŠČITE:



Ana uporablja svoj Facebook račun za ohranjanje stika s sodelavci iz službe. Dnevno objavlja fotografije, deli pomembne dogodke in koordinira strokovne projekte. Žal je bila žrtev napada, v katerem so kibernetiski kriminalci razbili njeno geslo za Facebook in prevzeli njen račun.



Takšni primeri niso redki in ne prizadenejo le starejših, temveč tudi poklicno aktivne in tehnološko ozaveščene ljudi. Vsakdo, ne glede na starost, lahko postane žrtev kibernetiskih kriminalcev, če ne sprejme ustreznih varnostnih ukrepov na spletu.

1. KORAK: Uporaba enostavnega gesla

Ana je uporabila enostavno geslo, kot je "12345678", kar je kibernetickemu kriminalcu olajšalo izvesti napad.

2. KORAK: Nobenih unikatnih gesel

Ana je na številnih spletnih mestih uporabljala isto geslo. Njeno geslo je bilo uporabljeno na drugih spletnih mestih, kar je povzročilo uhajanje podatkov.

Napadi na šibka gesla

— NAČINE ZAŠČITE:

Takšnim posledicam se lahko izognete tako, da sledite spodnjim ukrepom za zaščito pred napadi s šibkim geslom.



Spremenite geslo v močno in unikatno geslo:

Ana bi morala takoj spremeniti svoje geslo za Facebook v močno, dolgo in unikatno geslo, ki se ne uporablja na nobeni drugi spletni strani. Geslo naj vsebuje mešanico črk, števil in posebnih znakov.

Aktivirajte dvofaktorsko avtentikacijo (2FA):

Dobro je, da na svojem Facebook računu omogočite dvofaktorsko avtentikacijo, ki bo zagotovila dodatno raven varnosti. Zahvaljujoč temu, tudi če nekdo pozna geslo, se ne bo mogel prijaviti brez drugega dejavnika preverjanja verodostojnosti (npr. koda SMS).



Preverite varnostne nastavitve:

V varnostnih nastavitvah Facebooka preverite, ali so bile dodane neznane naprave ali aplikacije, in se odjavite iz vseh naprav. Spremenite tudi varnostna vprašanja, če so bila nastavljena.

Napadi na šibka gesla



NAČINE ZAŠČITE:



Prijavite incident Facebooku:

Pravilna rešitev je, da se obrnete na Facebookovo pomoč uporabnikom in sporočite, da je bil vaš račun ogrožen. Facebook vam lahko pomaga obnoviti račun in ga zaščiti pred nadaljnjimi napadi.

Preverite druge račune:

Dobro je preveriti druge račune na spletnih mestih, kjer ste morda uporabljali isto geslo, in jih zamenjati z edinstvenimi in močnimi gesli. S tem boste preprečili nadaljnje prevzeme računov.



Izobraževanje o "ribarjenju" (phishing):

Prav tako je dobro, da se naučite prepoznati poskuse ribarjenja in se tako v prihodnje izognete tovrstnim napadom. Ana naj bo pozorna na sumljiva e-poštna sporočila in povezave ter skrbno preveri naslove URL prijavnih strani.

Phishing ("Ribarjenje")

— ZNAČILNOSTI NEVARNOSTI:

Lažno predstavljanje je oblika kibernetškega napada, pri katerem skušajo goljufi pridobiti zaupne informacije. Beseda "phishing" izhaja iz angleške besede "fishing", ki se metaforično nanaša na "ribolov" osebnih podatkov uporabnikov.

Štiri glavna načela, na katerih temelji lažno predstavljanje:

- Metoda: goljufi ustvarijo lažna spletna mesta, e-pošto ali sporočila, ki navidezno prihajajo iz zaupanja vrednih institucij (npr. bank, tehnoloških podjetij, vladnih uradov).
- Tehnika: uporabljajo logotipe, barve in komunikacijske sloge, ki posnemajo izvirne vire.
- Cilj: pridobiti zaupanje žrtve, da posreduje svoje prijavnne podatke ali druge zaupne informacije.

- Metoda: uporaba občutka nujnosti ali strahu, ki žrtev prisili k hitremu ukrepanju.
- Tehnika: pošiljanje sporočila o domnevni kršitvi računa, neporavnanim plačilu ali posebni priložnosti/ponudbi, ki zahteva takojšen odziv.
- Cilj: povečati možnost, da bo žrtev ravnala impulzivno, brez tehtnega premisleka.

**Lažno
predstavljanje
za
verodostojne
institucije**

**Ustvarjanje
nujnih in
čustvenih
sporočil**

Phishing ("Ribarjenje")



ZNAČILNOSTI NEVARNOSTI:

Uporaba lažnih povezav in prilog

- Metoda: pošiljanje sporočil s povezavami do lažnih spletnih strani ali prilog, ki vsebujejo zlonamerno programsko opremo.
- Tehnika: povezave se morda zdijo legitimne, vendar vodijo do lažnih spletnih mest, ki zbirajo prijavne podatke ali nameščajo zlonamerno programsko opremo v napravo žrtve.
- Namen: prevzem prijavnih podatkov, okužba žrtvine naprave z zlonamerno programsko opremo ali pridobivanje drugih informacije.

Socialni inženiring

- Metoda: manipulacija žrtve z uporabo tehnik psihološkega zavanja.
- Tehnika: uporaba javno dostopnih informacij, kot so podatki na družbenih medijev, za ustvarjanje prilagojenih sporočil. Prevaranti lahko opravljajo tudi telefonske klice, pri čemer se se pretvarjajo, da so delavci tehnične podpore.
- Namen: ustvariti lažen občutek varnosti in preslepiti žrtev, da razkrije zaupne informacije.

Phishing ("Ribarjenje")



POSLEDICE:

Zakaj je lažno predstavljanje (phishing) nevarno? Posledice uspešnega lažnega predstavljanja so lahko resne – od izgube denarja, kraje identitete do okužbe naprave z zlonamerno programsko opremo. Da bi se zaščitili, je pomembno, da jih poznate.

01 Lažno predstavljanje za verodostojne institucije

- **Kraja identitete:** starejši lahko nevede posredujejo osebne podatke, ki bodo nato uporabljeni za odprtje lažnih bančnih ali kreditnih računov v njihovem imenu.
- **Finančna izguba:** razkritje prijavnih podatkov za bančni račun lahko povzroči nepooblaščene transakcije in izgubo prihrankov.

02 Ustvarjanje nujnih in čustvenih sporočil

- **Nepooblaščena plačila:** starejši se lahko hitro odzovejo na lažna opozorila tako, da posredujejo svoje bančne podatke in izvedejo nepotrebna nakazila.
- **Izguba prihrankov:** skušnjava hitrih odločitev lahko privede do velike finančne izgube, zlasti če starejši goljufom posredujejo podatke o svoji kreditni kartici.
- **Povečana ranljivost:** zaradi ponavljajočih se poskusov goljufije so lahko starejši zaradi stresa in negotovosti bolj ranljivi za nadaljnje napade.

Phishing ("Ribarjenje")



POSLEDICE:

03 Uporaba lažnih povezav in prilog

- Okužba naprave: zlonamerna programska oprema lahko okuži računalnik ali pametni telefon starejšega, zaradi česar lahko izgubi nadzor nad napravo in dostop do zaupnih podatkov.
- Kraja podatkov: zlonamerna programska oprema lahko pridobi podatke za prijavo, kar goljufom omogoča dostop do bančnih računov in drugih zaupnih podatkov.
- Stroški popravila: odstranitev zlonamerne programske opreme in popravilo okužene naprave lahko vključujeta visoke stroške, na katere starejši morda niso pripravljeni.

04 Socialni inženiring

- Telefonske goljufije: starejše lahko zavedejo, da posredujejo zaupne podatke po telefonu, kar vodi do kraje identitete in finančne izgube.
- Izguba zaupanja: pogosti napadi socialnega inženiringa lahko povzročijo pomanjkanje zaupanja v legitimne institucije in ljudi, kar oteži vsakdanje življenje in finančno upravljanje.
- Čustvena manipulacija: psihološki učinki, kot so strah, stres in tesnoba, lahko negativno vplivajo na duševno zdravje starejših.

Phishing ("Ribarjenje")

— NAČINI ZAŠČITE:



Marija redno uporablja internet za stike z družino, preverjanje bančnih računov in branje novic. Nekega dne je prejela e-poštno sporočilo, za katerega se je zelo, kot da ga pošiljanja njena banka.

Od: Banka XYZ no-reply@bankxyz.com
Zadeva: Pomembno: Zahtevana je takojšnja potrditev računa!

Spoštovana gospa Marija, zaradi nedavnih poskusov nepooblaščenega dostopa do vašega računa se takoj prijavite v svoj račun, da potrdite svojo identiteto in zaščitite svoj račun. Kliknite spodnjo povezavo in sledite navodilom:

Kliknite tukaj za prijavo

Hvala za sodelovanje, Banka XYZ

Posledice neprepoznavanja grožnje:

1. KORAK: Klik na povezavo

Marija, zaskrbljena zaradi vsebine e-pošte, klikne na povezavo, ne da bi natančno preverila njeno pristnost. Povezava jo pripelje na stran, ki je videti enako kot prijavna stran njene banke.

2. KORAK: Posredovanje podatkov

Marija vnese svoje prijavne podatke na lažno spletno stran, misleč, da potrjuje svoj račun.

Phishing ("Ribarjenje")

— NAČINI ZAŠČITE:

Marijin primer ponazarja običajno metodo lažnega predstavljanja zaupanja vrednih institucij. Poglejmo si posledice, do katerih lahko pride, če Marija ne prepozna te grožnje.



3. KORAK: Dodatna priloga

E-poštno sporočilo vsebuje tudi prilogo. Marija prenese prilogo, ki vsebuje zlonamerno programsko opremo. Ko odpre datoteko, se zlonamerna programska oprema namesti v njen računalnik in goljufom omogoči oddaljeni dostop do njene naprave.

4. KORAK: Prestrežanje podatkov in kraja denarja

Ko je Marija kliknila na povezavo, so prevaranti takoj prestregli njene podatke za prijavo in pridobili dostop do Marijinega pravega bančnega računa.

5. KORAK: Stres in tesnoba

Marija je uničena zaradi izgube svojih prihrankov in se boji, da bi v prihodnosti uporabljala spletno bančništvo ali druge spletne storitve.

6. KORAK: Okužba naprave

Zlonamerna programska oprema na Marijinem računalniku omogoča goljufom, da spremljajo njene spletne dejavnosti, prevzamejo druge prijave podatke in potencialno okužijo druge datoteke.

Phishing ("Ribarjenje")

— NAČINI ZAŠČITE:

Takšnim posledicam se lahko izognete tako, da sledite spodnjim ukrepom, da se zaščitite pred prevarami z lažnim predstavljanjem.



Preverjanje e-poštnega naslova pošiljatelja in povezav:

Marija naj natančno preveri e-poštni naslov pošiljatelja in povezave v sporočilu, preden klikne.

Akcija:

- Preverjanje e-poštnega naslova: preverite, ali e-pošta prihaja iz prave domene banke.

Nastavitev dvofaktorske avtentikacije (2FA):

Marija bi morala omogočiti dvofaktorsko avtentikacijo (2FA) na svojem bančnem računu, kar doda dodatno raven varnosti. Tudi če goljufi dobijo vaše geslo, potrebujejo tudi drugi element avtentikacije (npr. kodo SMS).

Akcija:

- Aktivacija 2FA: Marija naj kontaktira svojo banko, da ji omogoči 2FA.



Phishing ("Ribarjenje")

— NAČINI ZAŠČITE:

Redno posodablajte protivirusno programsko opremo in operacijski sistem:

Marija bi morala zagotoviti redne posodobitve protivirusne programske opreme in operacijskega sistema, da bi si zagotovi zaščito pred najnovejšo zlonamerno programsko opremo in phishingom.

Akcija:

- Protivirusna programska oprema: Marija mora namestiti protivirusno programsko opremo in poskrbeti, da je vedno posodobljena, ter jo redno posodablja.



Z upoštevanjem teh varnostnih ukrepov lahko Marija zmanjša tveganje, da bi postala žrtev phishinga, ter zaščiti svoje podatke in finance. Vedno natančno preverite e-poštni naslov pošiljatelja in se izogibajte klikanju povezav ali prilog v nepričakovanih e-poštnih sporočilih.



Zlonamerna programska oprema in računalniški virusi

— ZNAČILNOSTI NEVARNOSTI:

Izraz zlonamerna programska oprema se uporablja za opis zlonamernih programov, namenjenih poškodovanju računalnika ali izvajanju neželenih dejanj s strani uporabnika računalnika. Računalniški virus je ena najresnejših groženj, s katerimi se soočajo uporabniki računalnikov. Zlonamerna programska oprema lahko povzroči ogromno škode – od kraje podatkov, upočasnitve sistema do popolnega uničenja datotek.

Vrste zlonamerne programske opreme:

Vrsta zlonamerne programske opreme, ki blokira dostop do uporabniških podatkov tako, da jih šifrira. Kibernetski kriminallec zahteva odkupnino v zameno za ključ za dešifriranje in obljublja obnovitev dostopa do podatkov. Vendar se kriminalci pogosto odpovejo dogovoru in zaupne podatke prodajo tudi po plačilu odkupnine, žrtve pa so lahko znova tarča napadov.

**Izsiljevalska
zlonamerna
oprema
(Ransomware)**

Vrsta zlonamerne programske opreme, ki se izdaja za legitimno da bi se prikrito namestila na napravo uporabnika. Ko je enkrat nameščena, omogoči napadalcem dostop do naprave, kar jim omogoča, da namestijo druge oblike zlonamerne programske opreme, vohunijo za uporabnikom in kradejo občutljive podatke. Trojanci se pogosto širijo z uporabo socialnega inženiringa, kot so lažno predstavljjanje (phishing) in ponarejene spletne strani, ki zvabijo uporabnika k prenosu škodljivih datotek.

**Trojanski konj
(Trojan)**

Zlonamerna programska oprema in računalniški virusi

— ZNAČILNOSTI NEVARNOSTI:

Črvi (Worms)

Vrsta zlonamerne programske opreme, podobna virusom, vendar za širjenje ne potrebuje interakcije uporabnika. Izkorišča ranljivosti v napravah za namestitev in repliciranje. Ko okuži napravo, poskuša vzpostaviti povezavo z drugimi napravami v istem omrežju ter išče nadaljnje ranljivosti, da se razširi nanje.

Vohunska programska oprema (Spyware)

Zlonamerna programska oprema, ki se namesti na napravo žrtve z namenom vohunjenja in zbiranja občutljivih informacij, kot so prijavni podatki in številke kreditnih kartic. Spyware je lahko priložen drugim programom, ali pa ga namestite sami, če kliknete na oglas ali prenesete brezplačno programsko opremo z nezanesljivih spletnih strani. Ko je nameščen, beleži vsako tipko, ki jo uporabnik pritisne na tipkovnici, sledi zgodovini brskanja in uporablja kamero ter mikrofona naprave za nadzorovanje uporabnika.

Zlonamerna programska oprema brez datotek (Fileless malware)

Fileless zlonamerna programska oprema je vrsta zlonamerne programske opreme, ki za okužbo naprave ne uporablja izvršljivih datotek z zlonamerno kodo. Namesto tega spremeni legitimna orodja sistema, kar omogoča izvajanje zlonamernih dejavnosti brez prenosa datotek na trdi disk. Zlonamerna koda fileless programske opreme teče neposredno v pomnilniku računalnika in uporablja obstoječa sistemska orodja za doseganje svojih ciljev.

Zlonamerna programska oprema in računalniški virusi

— ZNAČILNOSTI NEVARNOSTI:

Vrsta zlonamerne programske opreme, ki napada mobilne naprave, kot so pametni telefoni in tablični računalniki, da bi pridobila dostop do občutljivih podatkov. Naprave brez ustreznih varnostnih ukrepov so ranljive za tovrstne napade, saj pogosto nimajo privzetih varnostnih mehanizmov, vgrajenih v izvirni operacijski sistem.

Virusi so vrsta zlonamerne programske opreme, ki okužijo naprave in se razmnožujejo, da bi se razširili na druge naprave. Pogosto se prikrijejo kot zlonamerne datoteke ali aplikacije, ki jih žrtve namestijo. Napadalci pogosto poskušajo prepričati uporabnike, da prenesejo te datoteke prek phishing napadov. Ko žrtev prenese okuženo datoteko ali aplikacijo, se virus aktivira in začne razmnoževati na napravi. Pogosto spreminja datoteke, da bi se izognil zaznavi, ter okuži druge naprave. Virus lahko krade zaupne podatke, upočasni napravo, zamrzne aplikacije ter spreminja in uničuje datoteke.

**Mobilna
zlonamerna
programska
oprema**

Virusi

Zlonamerna programska oprema in računalniški virusi



POSLEDICE:

Posledice okužbe z zlonamerno programsko opremo so zelo resne. Kibernetski kriminalci so motivirani s željo po dobičku. Uporabljajo okužene naprave za izvajanje napadov, kot so pridobivanje prijavnih podatkov za bančne storitve, zbiranje osebnih podatkov za prodajo, prodaja dostopa do računalniških virov ali izsiljevanje žrtev za odkupnine.

01 Izsiljevalska programska oprema (Ransomware)

Programska oprema lahko povzroči izgubo dostopa do pomembnih podatkov starejših, kot so finančni dokumenti ali družinske fotografije. Poleg tega plačilo odkupnine ne zagotavlja obnovitve podatkov, kar lahko povzroči dodatne finančne izgube.

02 Trojanski konj (Trojan)

Programska oprema lahko povzroči krajo občutljivih informacij, kot so gesla za bančne račune ali številke kreditnih kartic, zaradi česar so starejši izpostavljeni tveganju kraje identitete in finančne izgube.

03 Vohunska programska oprema (Spyware)

Programsko opremo je mogoče uporabiti za prisluškovanje pogovorom starejših ali sledenje njihovim spletnim dejavnostim, kar krši njihovo zasebnost in lahko povzroči uporabo zbranih podatkov za namene izsiljevanja ali goljufije.

Zlonamerna programska oprema in računalniški virusi



POSLEDICE:

04 Črvi (Worms)

Programska oprema lahko poškoduje operacijski sistem naprave starejših ali kibernetiski kriminalci prevzamejo nadzor nad njo, kar lahko onemogoči uporabo naprave ali povzroči izgubo pomembnih podatkov.

05 Programska oprema brez datotek (Fileless malware)

Programska oprema lahko deluje v ozadju in neopazno spreminja nastavitve vaše naprave ali uporablja njene vire, kar lahko povzroči upočasnitev vaše naprave ali povzroči težave z njenim delovanjem.

06 Mobilna zlonamerna programska oprema

Programska oprema lahko povzroči izgubo podatkov ali kršitev zasebnosti starejših z dostopom do njihovih osebnih podatkov ali sledenjem njihove lokacije.

07 Virusi

Virusi lahko ukradejo zaupne podatke, kot so gesla, finančni podatke ali osebne podatki, s čimer kršijo zasebnost uporabnikov. Lahko se razmnožujejo in širijo na druge naprave v omrežju, kar povzroči nadaljnje okužbe in poveča obseg težave.

Zlonamerna programska oprema in računalniški virusi



NAČINI ZAŠČITE:



Aleksander je brskal po svojem e-poštnem računu. Opazil je novico, ki je ni pričakoval, in ga je začela zanimati. Kliknil je na prilogo e-sporočilu. Opazil je nekaj nenavadnega. Nekaj je začelo spreminjati datoteke na njegovem računalniku, kar je povzročilo velike motnje pri njegovem delu. Kaj se je lahko zgodilo?

Primeri, podobni Aleksandrovedu, so žal kar pogosti. Klik na sumljivo prilogo e-poštnega sporočila lahko povzroči okužbo računalnika z zlonamerno programsko opremo. Posledično lahko pride do resnih motenj v delovanju in ogrozi varnost podatkov.



1. KORAK: Klik na prilogo v elektronski pošti

Aleksander je brskal po e-pošti in nič hudega sluteč kliknil na priponko v e-pošti.

2. KORAK: Okužba naprave

Klik na lažno prilogo je njegovo napravo okužil z virusom.

3. KORAK: Replikacija/množenje virusa

Priložena zlonamerna koda se je začela hitro razmnoževati v Aleksandrovem računalniku, kar je povzročilo spremembe v datotekah in motnje pri njegovem delu.

4. KORAK: Možnost kraje podatkov

Poleg tega je virus lahko ukradel zaupne podatke iz Aleksandrove naprave, kar je povzročilo dodatne težave z varnostjo in zasebnostjo.

Zlonamerna programska oprema in računalniški virusi

— NAČINI ZAŠČITE:

Takšnim posledicam se lahko izognete tako, da sledite spodnjim ukrepom zaščite pred zlonamerno programsko opremo.



Redno posodablajte svojo programsko opremo, kadar koli so na voljo nova sporočila o domnevnih grožnjah, kar zmanjša tveganje okužbe z zlonamerno programsko opremo, ki izkorišča te ranljivosti.

Bodite previdni pri odpiranju e-poštnih prilog in prenašanju datotek, še posebej, če so od neznanih pošiljateljev ali se zdiijo sumljive.



Izogibajte se klikom na sumljive povezave ali pojavna okna, saj lahko vodijo do okužb ali kraje podatkov.

Zlonamerna programska oprema in računalniški virusi

— NAČINI ZAŠČITE:



Javna omrežja Wi-Fi uporabljajte previdno, saj so ranljiva za napade; za zaščito internetne povezave razmislite o uporabi storitve VPN. Z uporabo storitve VPN so vaši podatki med prenašanjem prek javnih omrežij šifrirani, kar pomeni, da nihče ne more videti vašega naslova IP ali prestrezati podatkov, ki jih pošiljate ali prejimate iz svoje naprave.

Uporabljajte protivirusne programe in programe proti zlonamerni programski opremi, ki pomagajo preprečiti okužbe in odstraniti zlonamerno programsko opremo, vključno z vohunsko (spyware) in zlonamerno programsko opremo za prikazovanje oglasov (adware). Protivirusni programi se večinoma osredotočajo na odkrivanje in odstranjevanje virusov, medtem ko se ti. antimalware obravnava širok spekter zlonamerne programske opreme, vključno z zlonamernimi aplikacijami, ki niso razvrščene kot virusi.



Z upoštevanjem teh priporočil se lahko Aleksander in drugi uporabniki interneta izognejo grožnjam zlonamerne programske opreme. Zapomnite si, da ne smete sprejemati prehitrih odločitev in v virtualnem svetu vedno ravnajte previdno.



Dodatno branje



NAPAD PREK OMREŽIJ WI-FI (ZASEBNIH IN JAVNIH)

- www.keepersecurity.com/pl_PL/threats/man-in-the-middle-attacks-mitm.html
- www.cdv.pl/blog/blog-ekspercki/najpopularniejsze-rodzaje-atakow-hakerskich/
- www.socialwifi.com/pl/baza-wiedzy/bezpieczenstwo-sieci/najpopularniejsze-rodzaje-atakow-na-wifi/



NAPADI PREK ELEKTRONSKE POŠTE

- www.powerdmarc.com/pl/what-are-email-based-attacks/
- <https://www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y>
- www.keepersecurity.com/blog/pl/2023/08/30/the-most-common-types-of-cyberattacks/



NAPADI NA ŠIBKA GESLA

- www.keepersecurity.com/blog/pl/2024/01/12/types-of-password-attacks/
- www.securivy.com/blog/brute-force/
- www.keepersecurity.com/pl_PL/threats/dictionary-attack.html



PHISHING ("RIBARJENJE")

- www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y
- www.orange.pl/poradnik/twoj-internet/co-to-jest-phishing-i-jak-sie-przed-nim-bronic/
- www.kwestiabezpieczenstwa.pl/phishing/



ZLONAMERNA PROGRAMSKA OPREMA IN RAČUNALNIŠKI VIRUSI

- www.keepersecurity.com/blog/pl/2024/01/24/twelve-common-types-of-malware/
- www.hackeru.pl/wirus-komputerowy/
- www.powerdmarc.com/pl/types-of-malware/

2. POGLAVJE

FINANČNE IN NALOŽBENE PREVARE

V današnjem svetu so starejši vse pogostejše žrtve finančnih prevar, ki imajo različne oblike in jih kriminalci nenehno izpopolnjujejo. Namen tega poglavja je poudariti najpogostejše vrste prevar, da bi starejšim pomagali prepoznati grožnje in zaščititi svoje prihranke.

Med najbolj razširjenimi prevarami so finančne in naložbene manipulacije, ki temeljijo na lažnih obljubah hitrega dobička, ter dobrodelne prevare, ki izkoriščajo empatijo starejših. Druga nevarnost so obljube velikih dobitkov s ponarejenimi nagradami in loterijskimi zadetki, ki zahtevajo predplačilo.

Tudi prevare, ki vključujejo digitalne valute, kot je Bitcoin, postajajo vse pogostejše in ponujajo novo pot za kriminalne dejavnosti. Pomembno je omeniti tudi nigerijske prevare – mednarodne sheme goljufij, ki temeljijo na fiktivnih transakcijah.

Razumevanje teh groženj je ključnega pomena za starejše, da zavestno zaščitijo svoje finance.

Finančne in naložbene manipulacije

— ZNAČILNOSTI NEVARNOSTI:

Finančne in naložbene manipulacije se nanašajo na zavajajoče prakse, katerih cilj je prepričati posameznike, da vložijo svoj denar v goljufive ali nezanesljive sheme. Te sheme pogosto obljublajo visoke donose, vendar na koncu povzročijo finančno izgubo za vlagatelje.

Vrste manipulacij pri finančnih naložbah:

Prevaranti s prepričljivimi taktikami vlagateljem obljublajo nenavadno visoke donose na njihove naložbe. Te obljube, ki se zdijo preveč dobre, da bi bile resnične, in so pogosto usmerjene prav na starejše, ki iščejo načine za dopolnitev dohodka ob upokojitvi.

**Lažne
obljube o
visokih
donosih**

Prevaranti pogosto uporabljajo prodajne taktike visokega pritiska, s katerimi pritiskajo na posameznike, da bi sprejeli hitre naložbene odločitve, ne da bi temeljito raziskali ali razumeli naložbene produkte. Občutek nujnosti ustvarijo z navajanjem časovno omejenih ponudb ali spodbujanjem občutka strahu, da bi zamudili donosne priložnosti.

**Pritisk za
hitro
vlaganje**

Goljufi lahko priporočijo zapletene ali nejasne naložbene produkte, ki jih vlagatelji, zlasti starejši, težko razumejo. Ti produkti lahko vključujejo visoke provizije, skrita tveganja ali pomanjkanje preglednosti glede načina uporabe naloženih sredstev.

**Zapleteni in
nejasni
naložbeni
produkti**

Finančne in naložbene manipulacije



POSLEDICE:

Finančne in naložbene manipulacije imajo lahko resne negativne učinke, kot so:

01 Finančne posledice

Če postanete žrtev finančne manipulacije, lahko izgubite težko zaslužene prihranke in naložbe. Morda boste imeli precej manj denarja, kot ste pričakovali, kar bo vplivalo na vašo sposobnost pokrivanja vsakodnevnih stroškov in uživanja v pokoju.

02 Čustveni vpliv

Če vas prevarajo finančni goljufi, se lahko počutite prevarane in razočarane. Morda vas bo sram ali nerodno, da ste nasedli goljufiji, kar lahko vpliva na vašo samozavest in samozaupanje.

03 Osebne posledice

Če postanete žrtev finančne manipulacije, lahko to zmanjša vaše zaupanje v druge, zaradi česar boste bolj previdni in skeptični do prihodnjih naložbenih priložnosti. Ta izguba zaupanja pa lahko ogrozi tudi vaše odnose in vam oteži iskanje finančnih nasvetov ali podpore.

Finančne in naložbene manipulacije

— NAČINI ZAŠČITE:



Zofka prejme e-poštno sporočilo od neznanega pošiljatelja, ki trdi, da ponuja donosno naložbeno priložnost v novo tehnološko podjetje. E-pošta obljublja visoke donose in poziva Zofko, naj hitro ukrepa in si zagotovi sodelovanje pri naložbi.

Vendar se Zofka spomni prebranega nasveta o previdnosti pri nezaželenih e-poštnih sporočilih, ki obljublajo velike dobičke.

Zofkina zgodba žal ni edini primer, ki kaže na velik pomen zaščite starejših pred finančnimi manipulacijami. Starejši se morajo zavedati različnih oblik manipulacije, s katerimi se lahko srečajo, in poznati načine, kako se jim izogniti.



1. KORAK: Preverjanje

Zofka se odloči preveriti zakonitost naložbene priložnosti, preden ukrepa.

3. KORAK: Potrditev

Še vedno skeptična se Zofka odloči neposredno stopiti v stik s podjetjem, da bi preverila naložbeno priložnost.

2. KORAK: Posvetovanje

Zofka poišče tudi nasvet pri svojem družinskem članu, ki ima izkušnje s financami.

4. KORAK: Prijava

Zofka se odloči, da bo sumljivo elektronsko pošto prijavila pristojnim organom.

Finančne in naložbene manipulacije

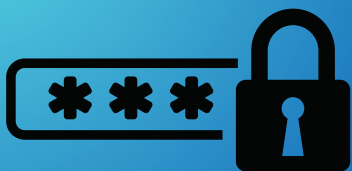


NAČINI ZAŠČITE:

Zaščita pred finančnimi in naložbenimi manipulacijami je ključnega pomena za zaščito vašega težko prisluženega denarja. Tukaj je nekaj enostavnih korakov, ki jih lahko naredite.

Previdno z e-pošto:

Če prejmete nepričakovano e-poštno sporočilo, ki obljublja velike dobičke ali nujne finančne ponudbe, bodite previdni. Vzemite si trenutek časa in preverite, ali pošiljateljev elektronski naslov ne vsebuje kakšnih čudnih znakov. Če se vam zdi, da nekaj ni v redu, ne klikajte na povezave in ne prenašajte prilog.



Okrepite gesla:

Ko nastavljate gesla za svoje spletne račune, se prepričajte, da so močna in unikatna. Uporabite kombinacijo črk, števil in simbolov ter se izogibajte uporabi informacij, ki jih je enostavno uganiti, kot je vaš rojstni dan ali ime vašega ljubljénčka.

Finančne in naložbene manipulacije



NAČINI ZAŠČITE:

Bodite pozorni na sumljive povezave in spletna mesta:

Če naletite na spletno mesto, ki se vam zdi nejasno ali neznano, ne delite osebnih ali finančnih podatkov. Za varna spletna mesta v naslovni vrstici poiščite »https://« in simbol ključavnice.



Bodite obveščeni o spletni varnosti:

Na voljo je veliko virov in izobraževalnih gradiv, ki vam bodo v pomoč pri spoznavanju pogostih prevar, ki so usmerjene na starejše.

Nenazadnje naj vas ne bo strah prositi za pomoč:

Če niste prepričani o finančni odločitvi ali sumite, da ste bili lahko tarča prevare, se za nasvet in podporo obrnite na družinske člane, prijatelje ali zaupanja vredne strokovnjake. Če menite, da ste postali žrtev finančne manipulacije, to nemudoma prijavite pristojnim organom, na primer državni agenciji za varstvo potrošnikov.



Navidezni altruizem: dobrodelna prevara

— ZNAČILNOSTI NEVARNOSTI:

Spletne goljufije z lažnimi dobrodelnimi organizacijami pogosto izkoriščajo radodarnost in sočutje ljudi, še posebej pa ciljajo na starejše, starejše od 65 let. Takšne prevare običajno vključujejo lažne dobrodelne organizacije, ki se predstavljajo kot legitimne in zbirajo denar za namišljene namene, kot so pomoč ob naravnih nesrečah, medicinske raziskave ali podpora ljudem v stiski.

Vrste manipulacij v dobrodelnih prevarah:

Prevaranti lahko uporabijo prepričljiv jezik ali čustvene pozive, da bi žrtve prisilili k hitri donaciji.

Z namenom zavajanja žrtev lahko goljufi ustvarijo lažna spletna mesta ali pošiljajo e-poštna sporočila, ki posnemajo blagovne znamke znanih dobrodelnih organizacij.

Prevaranti si lahko izmišljujejo srce parajoče zgodbe ali nudijo lažna pričevanja, da izzovejo sočutje in spodbudijo žrtve k donaciji.

Lažne dobrodelne organizacije pogosto navajajo nejasne ali zavajajoče informacije o svojem poslanstvu, ciljih in načinu uporabe donacij.

Taktika visokega pritiska

Lažno predstavljane zakonitih dobrodelnih organizacij

Lažne zgodbe in pričevanja

Pomanjkanje preglednosti

Navidezni altruizem: dobrodelna prevara



POSLEDICE:

V primeru, da postanejo žrtve dobrodelnih prevar, je to za starejše lahko zelo težko, tako v finančnem kot v čustvenem pogledu.

01

Finančna izguba

Če postanete žrtev dobrodelne prevare, lahko izgubite težko zaslužene prihranke in naložbe. Morda boste imeli precej manj denarja, kot ste pričakovali, kar bo vplivalo na vašo zmožnost kritja vsakodnevnih stroškov in uživanja v pokoju.

02

Čustvena stiska

Zaradi manipulacije v dobrodelni prevari se lahko počutite izdane, krive in v zadregi, ker ste postali žrtev te prevare.

03

Težave z zaupanjem

Prevare zmanjšajo tudi vaše nadaljnje zaupanje v zakonite, saj je težje razlikovati med resničnimi in lažnimi pozivi.

Navidezni altruizem: dobrodelna prevara

— NAČINE ZAŠČITE:



Alenka prejme e-poštno sporočilo, ki se sklicuje na dobrodelno organizacijo in prosi za donacije za pomoč otrokom v stiski. Elektronsko sporočilo vsebuje čustvene zgodbe in fotografije otrok, ki naj bi prejemale pomoč dobrodelne organizacije. Vendar se Alenka spomni prebranega nasveta o previdnosti pri elektronskih sporočilih, ki se nanašajo na donacije dobrodelnim organizacijam.



Alenkina zgodba žal ni edini primer, ki kaže na pomen zaščite starejših pred dobrodelnimi goljufijami. Starejši se morajo zavedati različnih oblik prevar, s katerimi se lahko srečajo, in poznati metode, kako se jim izogniti.

1. KORAK: Raziščite organizacijo

Alenka pred donacijo preveri status registracije dobrodelne organizacije in ocene na verodostojnih spletnih straneh.

2. KORAK: Bodite previdni pri nepričakovanih zahtevah

Alenka je podvomila o vsebini zapisani v nepričakovanem elektronskem sporočilu s prošnjo za donacijo.

3. KORAK: Ne delite osebnih podatkov

Alenka ni želela neznanim ali nepreverjenim dobrodelnim organizacijam posredovati občutljivih podatkov, kot so številke socialnega zavarovanja ali bančni podatki.

4. KORAK: Neposredna donacija

Če želi Alenka donirati, naj namesto klikanja na povezave v e-poštnih sporočilih ali odzivanja na telefonske klice raje donira neposredno prek uradne spletne strani dobrodelne organizacije.

Navidezni altruizem: dobrodelna prevara



NAČINI ZAŠČITE:

Zaščita pred dobrodelnimi prevarami in njihovimi posledicami je zelo pomembna. Tukaj je nekaj preprostih navodil, s pomočjo katerih lahko preprečite, da bi postali žrtev dobrodelne goljufije.

Raziščite dobrodelne organizacije tako, da preverite njihov status in ocene na verodostojnih spletnih straneh dobrodelnih organizacij.



Bodite previdni pri nepričakovanih prošnjah za donacije prek e-pošte, telefonskih klicev ali družbenih medijev, saj prave dobrodelne organizacije običajno ne uporabljajo taktike visokega pritiska.

Nikoli ne delite osebnih podatkov, kot so številke socialnega zavarovanja ali bančni podatki, z neznanimi dobrodelnimi organizacijami.

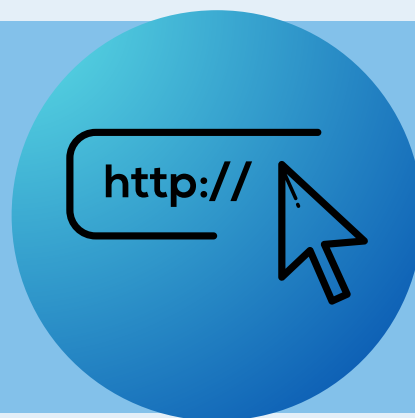


Navidezni altruizem: dobrodelna prevara



NAČINI ZAŠČITE:

Donirajte neposredno prek uradne spletne strani dobrodelne organizacije ali tako, da pošljete ček na njihov preverjeni naslov.



Informirajte se o pogostih dobrodelnih prevarah in se naučite prepoznati opozorilne znake.

Ne oklevajte in prosite družino, prijatelje ali finančne svetovalce za pomoč pri ocenjevanju prošelj za dobrodelne namene, če sumite, da gre za prevaro.



Mamljive iluzije: izmišljene nagrade, loterije in nagradne igre

— ZNAČILNOSTI NEVARNOSTI:

Prevare, ki temeljijo na lažnih nagradah in loterijah, so zavajajoče in namerno izkoriščajo željo ljudi po zmagi, tako da jih prepričajo, da so osvojili velike nagrade. Prevaranti prepričujejo žrtve, da jim bodo izplačali lažne dobitke, vendar na koncu ukradejo denar iz njihovih denarnic.

Vrste manipulacij pri fiktivnih nagradah in loterijah:

Prevaranti se pogosto lažno predstavljajo kot predstavniki priznanih podjetij ali loterij, ki jih upravljajo vlade (zlasti tuje), in uporabljajo manipulativne taktike, da izkoristijo zaupanje svojih žrtev v upanju, da bodo izkoristili njihovo željo po finančni varnosti.

Lažno predstavljanje

Prevaranti skušajo žrtve prepričati, da so bili izbrani kot edini ali redki srečneži z namenom, da bi pri žrtvi ustvarili občutek edinstvenosti in ekskluzivne priložnosti.

Ekskluzivnost

Prevaranti obljublajo nerealne denarne nagrade, luksuzne izdelke itd., ki so preveč dobri, da bi bili resnični, in uporabljajo taktiko pritiska, da bi žrtve prisilili k takojšnjemu odzivu in jih hkrati prepričujejo, da ostanejo diskretne.

Nerealne obljube

Mamljive iluzije: izmišljene nagrade, loterije in nagradne igre



POSLEDICE:

Posledice prevar »vabljive iluzije« so različne in pogosto dolgotrajne.

01 Finančne posledice

Ena najhujših posledic takšnih prevar je finančno opustošenje žrtev in večina žrtev pogosto utrpi veliko finančno škodo. Žrtve lahko izgubijo življenjske prihranke, postanejo prezadolžene ali celo bankrotirajo. Okrevanje po takšnih finančnih težavah lahko traja več let.

02 Čustvene posledice

Žrtve goljufij pogosto doživljajo globoko čustveno stisko in se borijo z občutki izdaje, nasilja, sramu in krivde. Čustveni pretres, ki ga povzročita prevara in goljufija, lahko povzroči tesnobo, depresijo in celo posttravmatsko stresno motnjo (PTSM) ter lahko vpliva tudi na fizično zdravje.

03 Pravne posledice

V primerih prevar, pri katerih so žrtve prepričane, da unovčijo lažne "nagradne čeke", se lahko poleg finančne izgube celo soočijo s pravnimi posledicami, vključno z obtožbami zaradi pranja denarja ali poneverbe.

Mamljive iluzije: izmišljene nagrade, loterije in nagradne igre

— NAČINI ZAŠČITE:



Greta je prejela nepričakovano SMS sporočilo, v katerem je bila obveščena, da je zadela glavni dobiček na tuji loteriji in da mora nemudoma plačati vnaprejšnjo "administrativno provizijo", da prevzame denarno nagrado.

V sporočilu je bilo tudi zapisano, da informacij o svojem dobitku na loteriji in postopkih za prejem nagrade ne sme deliti z nikomer.

Na žalost prevaranta ...

Greta se je nedavno udeležila tečaja o kibernetiski varnosti, ki je vključeval tudi predavanje o spletnih prevarah.



1. KORAK: Prepoznavanje opozorilnih znakov

Greta je takoj opazila znake prevare: nepričakovano sporočilo, dobiček na loteriji (za katerega ni kupila listka) in zahtevo po predplačilu.

3. KORAK: Izogibanje vpletenosti

Greta se na SMS sporočilo ni odzvala, s čimer je zaščitila svoje osebne podatke in se izognila finančni izgubi.

2. KORAK: Prepoznavanje drugih strategij

Greta je navodila, naj podrobnosti o loterijskem zadetku ne razkriva drugim, prepoznala kot taktiko, s katero so jo želeli osamiti in si olajšati, da bi nasedla prevari.

4. KORAK: Prijava

Greta je o poskusu prevare takoj obvestila svojo družino, prijatelje in pristojne organe ter informacijo delila na družbenih omrežjih.

Mamljive iluzije: izmišljene nagrade, loterije in nagradne igre



NAČINI ZAŠČITE:

Če naletite na poskus prevari tipa "Mamljiva iluzija", si najprej zapomnite, da brezplačnega denarja ni, in upoštevajte znani rek: "Če je nekaj videti predobro, da bi bilo res, verjetno je." Tukaj je nekaj dodatnih nasvetov za primer, če se znajdete v takšni situaciji.

Uporabite zdrav razum:

Uprite se želji po hitrem reagiranju ob nepričakovanih obvestilih o nagradah, ki ste jih prejeli po e-pošti, družbenih omrežjih ali SMS sporočilu!

Preden ukrepate, se vprašajte, ali ste sploh sodelovali v kakšni nagradni igri ali loteriji.



Preverite verodostojnost:

Preverite spletno stran ali pošiljatelja obvestila po drugih kanalih.

Pobrsajte po internetu, se posvetujte z družino ali prijatelji, da preverite verodostojnost!

Ne klikajte ali tapajte povezav v sporočilih, še posebej, če so videti sumljive!

Mamljive iluzije: izmišljene nagrade, loterije in nagradne igre

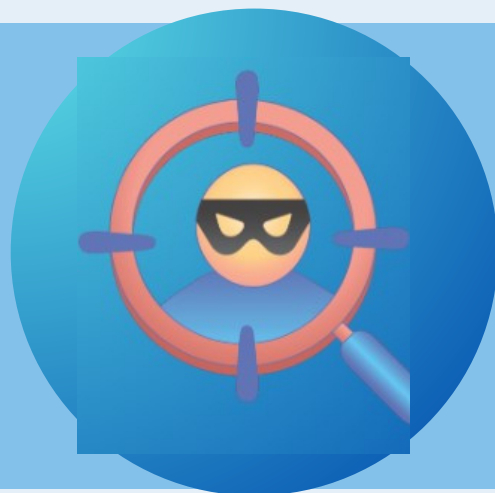


NAČINI ZAŠČITE:

Preglejte podrobnosti:

V obvestilu natančno preverite vse informacije, ki ste jih prejeli.

Bodite pozorni na morebitne nejasne ali nenavadne zahteve, kot so zahteve po osebnih podatkih, finančnih podatkih ali vnaprejšnjem plačilu!



Ne pozabite:

Nikoli ne pošiljajte denarja ali plačajte provizije za prevzem nagrade/denarja ob nepričakovanem obvestilu o nagradi!

Zakonite nagradne igre ne zahtevajo nobenega plačila za sodelovanje ali prevzem nagrade, sodelovanje v loterijah pa zahteva nakup vstopnice.



Mamljive iluzije: izmišljene nagrade, loterije in nagradne igre



NAČINI ZAŠČITE:

Če ste prevarantu razkrili svoje osebne ali finančne podatke, nemudoma **spremenite gesla svojega e-poštnega računa in vseh drugih računov. Spremenite tudi PIN-e na svojih bančnih računih**, če uporabljate spletno banko, pa **ne pozabite spremeniti tudi gesla za spletno banko.**

Uporabljajte močna gesla s kombinacijo velikih in malih črk, števil in posebnih znakov!



Če ste odprli sumljivo povezavo in delili svoje finančne ali osebne podatke ali utrpeli finančno izgubo, to nemudoma prijavite ustreznemu organu v vaši državi!

Prevare z digitalnimi valutami

— ZNAČILNOSTI NEVARNOSTI:

Prevare s kriptovalutami (kot je na primer Bitcoin) se nanašajo na vse goljufive dejavnosti, povezane z digitalnimi valutami. Imajo lahko več oblik, vključno z lažnimi začetnimi ponudbami kovancev (ICO), Ponzijevimi shemami in lažnimi naložbenimi priložnostmi. Te prevare običajno obljublajo visoke donose, da bi zvale žrtve, ki nato izgubijo svoje naložbe, ko prevaranti izginejo z njihovim denarjem. Starejši so zaradi nepoznavanja digitalnih tehnologij in interneta še posebej ranljivi za tovrstne prevare. Prevaranti pogosto izkoriščajo zaupanje starejših in njihovo potrebo po finančni varnosti, zato je pomembno, da starejše ozaveščamo in jih izobražujemo, saj jih tako zaščitimo pred tovrstnimi prevarami.

Vrste prevar s kriptovalutami:

Ta vrsta prevare se odvija v fazi zbiranja sredstev za nove kriptovalute. Razvijalci predstavijo obetavno novo digitalno valuto, pogosto skupaj z obsežnim ti. "belim dokumentom", ki opisuje cilje projekta, tehnologijo in potencialne donose. Na žalost, ko zberejo dovolj sredstev od vlagateljev, ti razvijalci izginejo brez sledu, vlagatelji pa ostanejo z ničvrednimi žetoni.

Te sheme obljublajo visoke donose z nizkim tveganjem. Vendar se donosi izplačajo s sredstvi novih vlagateljev, ne iz dobička. Shema se sesuje, ko ni dovolj novih vlagateljev, kar povzroči znatne izgube predvsem za zadnje vlagatelje.

Ta vrsta prevare vključuje aplikacije ali programsko opremo, ki domnevno varno hranijo kriptovalute. Te denarnice imajo pogosto profesionalno oblikovane vmesnike in lahko celo posnemajo legitimne denarnice. Vendar pa so v resnici namenjene odtujitvi digitalnih valut. Ko uporabnik svoje kriptovalute naloži v te lažne denarnice, prevaranti pridobijo dostop, kar pogosto povzroči popolno izgubo uporabnikovega digitalnega premoženja.

**Prevara
Začetne
ponudbe
kovancev
(ICO)**

**Ponzijeve
sheme**

**Prevare s
ponarejeno
denarnico**

Prevare z digitalnimi valutami



POSLEDICE:

Finančne in naložbene manipulacije imajo lahko resne negativne posledice kot so:

01 Finančna izguba

Najbolj neposredna in očitna posledica goljufij s kriptovalutami je finančna izguba. Žrtve pogosto izgubijo celotno naložbo, kar je lahko uničujoče, zlasti če so vložile velik del svojih prihrankov.

02 Izguba zaupanja

Žrtve goljufij s kriptovalutami pogosto izgubijo zaupanje v digitalne valute in morda oklevajo glede naložb ali sodelovanja v digitalnem gospodarstvu v prihodnosti. To lahko ovira širjenje, uveljavljanje in sprejemanje kriptovalut.

03 Pravne posledice

V nekaterih primerih se lahko udeleženci v goljufivih shemah, tudi če se tega ne zavedajo, soočijo s pravnimi posledicami. To lahko vključuje preiskavo zakonodajnih organov in morebitne obtožbe, tudi če so nevede pripomogli pri omogočanju izvajanja prevare.

Prevare z digitalnimi valutami

— NAČINEI ZAŠČITE:



Nekega dne je Helena prejela elektronsko sporočilo, s povabilo k naložbi v novo kriptovaluto, ki je obljubljala velike donose. Navdušena in v želji, da bi povečala svoj digitalni portfelj, se je odločila, da ga razišče. Elektronsko sporočilo je poslalo podjetje z imenom "CryptoGold", njihova spletna stran pa je bila impresivna, polna pričevanj zadovoljnih vlagateljev in obljub o visokih donosih. Priložnost se ji je zdela preveč dobra, da bi jo zamudila, zato se je odločila vložiti majhen del svojih prihrankov. Dnevi so se spremenili v tedne, Helena pa je vsak dan nestrpno preverjala svojo spletno denarnico in upala, da bo njena naložba rasla. Toda namesto tega je opazila, da se njena naložba zmanjšuje. Zmedena in zaskrbljena je poskušala vzpostaviti stik s podjetjem "CryptoGold". Vendar so se vsa njena elektronska sporočila vrnila nazaj, nekoč impresivna spletna stran pa je bila nedostopna.

Helenina zgodba opozarja na potrebo po zaščiti starejših pred prevarami s kriptovalutami preko ozaveščanja in izobraževanja. Starejši so lahko ranljivi zaradi nepoznavanja digitalnih tehnologij, zato morajo razumeti tveganja, znake prevar in pomen skeptičnega stališča do obljub o visokem donosu. Za varno digitalno navigacijo so ključnega pomena tudi podpirne mreže.



1. KORAK: Raziščite podjetje

Helena bi morala pred naložbo temeljito raziskati "CryptoGold". Namesto da bi bila navdušena nad spletno stranjo in pričevanji, bi morala preveriti, ali je podjetje registrirano, in poiskati ocene ali opozorila drugih uporabnikov.

3. KORAK: Izogibajte se takojšnjim odločitvam

Helena se je hitro odločila za naložbo, ne da bi si vzela čas, da bi popolnoma razumela pogoje in povezana tveganja. Morala bi se izogibati prenapljenim naložbenim odločitvam in poiskati nasvet pri kompetentnih posameznikih ali finančnih svetovalcih.

2. KORAK: Preverite komunikacijo

Helena je prejela nezaželeno e-pošto in ji zaupala brez preverjanja. Morala bi biti previdna in potrditi identiteto pošiljatelja s preverjanjem pri zaupanja vrednih virih, kot so uradni kontaktni podatki podjetja ali znani forumi o kriptovalutah.

4. KORAK: Redno spremljajte naložbe

Helena ni opazila takojšnjih znakov goljufije in je še naprej upala na pozitivne donose. Svoje naložbe bi morala redno spremljati in biti pozorna na morebitne nenavadne aktivnosti ali pomanjkanje preglednosti ter jih podrobneje raziskati.

Prevare z digitalnimi valutami



NAČINI ZAŠČITE:

Zaščita pred prevarami s kriptovalutami je ključnega pomena, zlasti pri starejših, saj so lahko zaradi nepoznavanja digitalnih tehnologij še posebej ranljivi. Goljufi pogosto targetirajo starejše z obljubami o visokih donosih ter izkoriščajo njihovo zaupanje in potrebo po finančni varnosti. Če postanejo žrtve teh prevar, lahko utrpijo veliko finančno izgubo, izgubijo zaupanje v digitalne inovacije in utrpijo morebitne pravne posledice. Izobraževanje, temeljito raziskovanje in zdrava mera kritičnosti do ponudb, ki so preveč dobre, da bi bile resnične, so bistveni koraki pri varovanju premoženja in zagotavljanju finančne blaginje.

Izobraževanje:

Prvi korak k preprečevanju goljufij je razumevanje delovanja kriptovalut. To vključuje razumevanje tehnologije, ki stoji za njimi, delovanja transakcij ter varnega in zanesljivega shranjevanja in zaščite digitalnega premoženja.



Raziskovanje:

Pred naložbo v katero koli kriptovaluto temeljito raziščite digitalno valuto, ekipo, ki stoji za njo, in preberite vse razpoložljive ti. bele knjige. Še posebej bodite previdni pri novih kriptovalutah, ki obljublajo visoke donose ob majhnem tveganju.

Prevare z digitalnimi valutami



NAČINI ZAŠČITE:

Zavarujte svojo digitalno denarnico:

Zaščitite svoja digitalna sredstva z uporabo varne digitalne denarnice. To je lahko strojna denarnica, ki shranjuje valuto brez internetne povezave, ali verodostojna spletna denarnica z močnimi varnostnimi ukrepi. Vedno omogočite dvofaktorsko avtentikacijo, če je le na voljo.



Bodite skeptični:

Bodite skeptični do vsake naložbe, ki obljublja visoke donose z malo ali nič tveganja. Te so pogosto predobre, da bi bile resnične. Ne pozabite, da zakonite naložbe običajno ne jamčijo za dobiček in vedno vključujejo določeno stopnjo tveganja.

Prijavite sumljivo dejavnost:

Če naletite na morebitno prevaro s kriptovalutami, to prijavite svojim lokalnim oblastem in vsem ustreznim spletnim platformam. S tem ne boste zaščitili le sebe, temveč boste pomagali, opozorili in zaščitili tudi druge.



Mednarodne finančne prevare

— ZNAČILNOSTI NEVARNOSTI:

Prevara 419, znana tudi kot nigerijska prevara, je zloglasna goljufija s predplačili, ki izvira iz Nigerije. Izvaja se že od prvih dni interneta in je postala ena najbolj razširjenih prevar na svetu.

Vrste manipulacije v prevari 419:

Z besedo "Pozdravljeni" v vrstici elektronskega sporočila "Zadeva" vas bo pozdravil bogat nigerijski princ (celo nigerijski astronaut), bogat odvetnik ali poslovnež in vam ponudil veliko vsoto denarja, v zameno za majhno predplačilo za kritje domnevnih stroškov transakcije, za pomoč pri prenosu njegovega denarja iz Nigerije (ali za vašo pomoč pri dostopu do računa).

Z besedo "Pozdravljeni" v vrstici elektronskega sporočila "Zadeva" vas bo pozdravila oseba, ki se je znašla v težki življenjski situaciji, kot je ugrabitev njenih otrok, ali oseba, ki je zaradi političnih razmer postala ubežnik ali nedolžni zapornik itd. Vsi pa imajo dolgo in žalostno zgodbo o tem, zakaj ne morejo dvigniti svojega denarja, zato vas prosijo za pomoč.

Lažno predstavlanje
(različica 1)

Lažno predstavlanje
(različica 2)

Mednarodne finančne prevare

Za nigerijskimi prevarami stojijo profesionalni prevaranti, ki s sistematičnim pristopom in preizkušenimi tehnikami manipulirajo s človeškimi čustvi in ranljivostmi. Uporabljajo vnaprej pripravljen priročnik, ki je v nigerijskih goljufijah znan kot "script" ali "format". Ta pogosto vključuje izdelane zgodbe, lažne identitete in ponarejene dokumente, ki so videti legitimni in jih prevaranti preprosto kopirajo ter uporabljajo v komunikaciji z žrtvami.

Pri nigerijski prevari komunikacija poteka izključno prek elektronske pošte, SMS sporočil ali družbenih omrežij. Pri tej vrsti prevare goljufi z žrtvami ne komunicirajo prek videa ali telefonskega pogovora. Prejeta sporočila vsebujejo slovnične napake in slabo ubeseditev besedila.

Ko žrtev ne posreduje več denarja ali osebnih podatkov ali ko ugotovi, da je bila prevarana, goljufi nemudoma prenehajo odgovarjati na korespondenco in preprosto izginejo.

**Igranje na
človeška
čustva**

**Izključna
uporaba pisne
digitalne
komunikacije**

Izginotje

Mednarodne finančne prevare



POSLEDICE:

Ta prevara lahko ogrozi ljudi vseh starosti, še posebej tiste, ki verjamejo v sheme za hiter zaslužek ali so finančno naivni. Vendar pa so starejši še bolj ranljivi, saj običajno bolj zaupajo drugim in manj vedo o spletni varnosti.

01 Finančne posledice

Žrtve lahko izgubijo velike vsote denarja, kar povzroči resne finančne težave. Ko se žrtve odzovejo pozitivno, se ujamejo v past, saj prevaranti od njih zahtevajo vedno več denarja in si izmišljujejo najrazličnejše lažne izgovore ali predloge za dodatna plačila. V tem primeru se lahko pojavi tudi ti. zmeta o nepovratnih/potopljenih stroških (Sunk Cost Fallacy), ko žrtve še naprej nadaljujejo z nečim, v kar so že veliko investirale (denar, čas, trud, čustveno energijo itd.), čeprav bi bilo veliko bolje, če bi odnehale.

02 Čustvene posledice

Če sram ali zadrega spodbujata skrivnostno in prikrito vedenje, se lahko zgodi, da so žrtve večkrat prevarane.

03 Socialne posledice

Po tem, ko je oseba prevarana, se lahko njeno zaupanje v druge ljudi močno zmanjša, kar vodi v izolacijo in težave pri pri ohranjanju in vzpostavljanju odnosov.

Mednarodna finančna prevara

— NAČINI ZAŠČITE:



Ema je brskala po spletu, ko je prejela e-pošto z zadevo "Pozdravljeni". Pošiljatelj e-pošte je bil nigerijski "princ", ki je potreboval njeno pomoč pri nakazilu velike vsote denarja iz Nigerije. V zameno za majhno provizijo za posredovanje pri transakciji naj bi prejela odstotek sredstev za svojo pomoč.

Kljub mamljivi ponudbi je Ema postala sumničava!

Na žalost prevaranta ...

Ema je nedavno prebrala spletni članek o 419 prevarah in se poučila o vseh različicah te prevare.



1. KORAK: Prepoznavanje opozorilnih znakov v komunikaciji

Ema je opazila, da je bila vsebina e-pošte napisana v zelo slabi angleščini in da sploh ni imela nobega smisla.

2. KORAK: Uporaba znanja

Ema je med branjem spletnega članka o 419 prevarah izvedela tudi, da v Nigeriji ni kraljevih družin.

3. KORAK: Odločno ukrepanje

Ema je e-pošto takoj označila kot neželeno in jo izbrisala. Enako je storila tudi z nadaljnjimi elektronskimi sporočili, ki so bila poslana od "domnevnega" nigerijskega princa.

4. KORAK: Spodbujanje skupnosti ozaveščenih in informiranih posameznikov

Ema je svojo izkušnjo delila z možem, družino in prijatelji ter informacije o poskusu prevare delila tudi v družabnih medijih.

Mednarodne finančne prevare



NAČINI ZAŠČITE:

Če naletite na poskus 419 vrste prevare, si morate najprej zapomniti, da še nihče na svetu ni prejel velike vsote denarja zaradi nepričakovanega sporočila v svojem e-poštnem nabiralniku!

Tukaj je nekaj dodatnih nasvetov, če se morda znajdete v takšni situaciji.

Če prejmete ponudbo s strani goljufa 419 in vas mika, da bi jo sprejeli, se ustavite in si zastavite dve preprosti zdravorazumski vprašanji:

Zakaj bi svoje osebne in finančne podatke delili s popolnim neznancem (ki prihaja iz države, s katero nimate nobene povezave) in zakaj bi ta neznanec izbral prav vas, da bi z njim delil bogastvo?



Tudi če vas je zgodba o »ugrabitvi otroka« ganila v dno srca, nikoli ne pošljite denarja (ali drugih finančnih podatkov), dokler ne preverite pristnosti osebe, ki vas prosi za finančno pomoč!

Upoštevajte tudi, da vas 419 goljufije nagovarjajo k plačilu prek storitev za prenos denarja (običajno Western Union).

Mednarodne finančne prevare



NAČINI ZAŠČITE:

Preverite pristnost vsebine:

Ker prevaranti 419 vedno znova uporabljajo skripte, lahko pristnost vsebine e-pošte preverite tako, da preprosto vstavite kratek del vsebine v iskalnik (Google, Bing itd.). Če je vsebina del znanih ali odkritih prevarantskih sporočil, boste našli spletna mesta, ki opozarjajo na to prevaro, in o kateri so že poročale druge žrtve.



Ne odgovarjajte na lažna e-poštna sporočila (niti za šalo)!

Nemudoma jih izbrišite!

Ne pozabite, če odgovorite – se boste najverjetneje ujeli v finančno past!

Mednarodne finančne prevare



NAČINI ZAŠČITE:

Če ste prevarantu razkrili svoje finančne podatke, **spremenite kodo PIN in geslo za prijavo** (če uporabljate spletno bančništvo).

Sprejmite dodatne varnostne ukrepe za finančne transakcije, kot sta **dvofaktorica avtentikacija** (2FA) in **funkcija opozorila o transakcijah**, ter **redno spremljajte stanje na svojem računu**.



REPORT

Če ste utrpeli finančno izgubo, jo nemudoma prijavite svoji banki in drugim pristojnim organom v vaši državi!

Dodatno branje



FINANČNE IN NALOŽBENE MANIPULACIJE

- <https://faircanada.ca/investing-basics/protecting-vulnerable-investors-from-financial-abuse/>
- <https://economictimes.indiatimes.com/wealth/legal/will/how-can-senior-citizens-protect-themselves-from-financial-exploitations-by-their-own-families/articleshow/103877992.cms?from=mdr>
- <https://www.morganstanley.com/articles/elder-financial-abuse-protecting-loved-ones>
- <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6044329/>
- <https://www.psychiatrist.com/pcc/financial-abuse-older-adults-screening-prevention-interventions-primary-care-providers/>
- <https://www.youtube.com/watch?v=7G8lil8Yupg>
- <https://www.c-span.org/video/?324176-1/financial-exploitation-senior-citizens>



NAVIDEZNI ALTRUIZEM: DOBRODELNA PREVARA

- <https://www.bbc.com/news/uk-34530586>
- <https://www.youtube.com/watch?app=desktop&v=MTm-fq0OUQQ>
- https://www.americansenioralliance.com/episode_5
- <https://www.youtube.com/watch?v=vR53sRLVgpc>
- <https://www.theguardian.com/society/2015/sep/01/charities-face-scrutiny-over-trading-of-elderly-mans-data>

Dodatno branje



MAMLJIVE ILUZIJE: IZMIŠLJENE NAGRADE, LOTERIJE IN NAGRADNE IGRE

- <https://www.identityguard.com/news/lottery-scams>
- <https://www.pcrisk.com/> <https://www.naperville.il.us/services/naperville-police-department/community-education-and-crime-prevention/frauds-and-scams/>
- <https://www.scamwatch.gov.au/system/files/Little%20Black%20Book%20of%20Scams%20-%20Final.pdf>
- <https://www.gamblingcommission.gov.uk/public-and-players/guide/lottery-scams-and-fraud>
- <https://www.identityguard.com/news/online-safety-tips-for-seniors>
- <https://www.liveabout.com/warning-signs-of-sweepstakes-scams-886996>
- <https://surfshark.com/research/data-breach-impact/crime-lottery-inheritance-scam> <https://www.aura.com/learn/sweepstakes-scams>



PREVARE Z DIGITALNO VALUTO

- <https://www.consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams> <https://www.coindesk.com/learn/crypto-scams-types-of-crypto-schemes-and-kako-se-izogniti-prevaram>
- <https://www.fastex.com/en/learn/crypto-scams-explained>
- <https://cointelegraph.com/explained/impersonation-scams-in-crypto-explained> <https://www.ftc.gov/news-events/news/press-releases/2022/06/new-analysis-finds-consumers-reported-losing-more-1-billion-cryptocurrency-scams-2021>
- <https://www.mdpi.com/2227-9091/11/3/51>
- <https://www.cybertrace.com.au/cryptocurrency-fraud-explained>
- <https://www.arkoselabs.com/guide-to-cryptocurrency-security>
- <https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-new-analysis-reveals-consumers-lost-nearly-500-million-cryptocurrency-scams>
- <https://www.kaspersky.com/resource-center/threats/top-seven-tips-for-preventing-cryptocurrency-scams>

Nadaljnja branja



MEDNARODNE FINANČNE GOLJUFIJE

- <https://www.altospam.com/en/glossary/scam-nigerian419/>
- <https://www.comparitech.com/identity-theft-protection/nigerian-scam/>
- <https://www.comparitech.com/identity-theft-protection/nigerian-scam/>
- <https://www.britannica.com/topic/cybercrime/Identity-theft-and-invasion-of-privacy#ref829190>
- <https://www.wallstreetmojo.com/nigerian-scam/#nigerian-letter-scam-explained>
- <https://whatismyipaddress.com/nigerian-fraud-combines-scams>
- <https://hackernoon.com/the-nigerian-prince-email-and-the-history-of-social-engineering-techniques>
- <https://www.cnbc.com/2019/04/18/nigerian-prince-scams-still-rake-in-over-700000-dollars-a-year.html>

3. POGLAVJE

SOCIALNA MANIPULACIJA IN ČUSTVENA PREVARA

Sodobne prevare so vse pogostejše v obliki socialne in čustvene manipulacije, zato so starejši še posebej ranljivi za te grožnje. Kriminalci izkoriščajo čustva, zaupanje in naivnost, da bi dosegli svoje cilje, pri čemer pogosto uničijo njihovo finančno in čustveno blaginjo. Namen tega poglavja je obravnavati najpogostejše prevare, ki temeljijo na čustveni in socialni manipulaciji, ter pomagati starejšim, da prepoznajo te nevarnosti in se pred njimi zaščitijo.

Med najnevarnejšimi so romantične prevare, pri katerih kriminalci vzpostavljajo razmerja, da bi izsilili denar. Resno nevarnost predstavljajo tudi ribarjenje in telefonske prevare, saj se prevaranti izdajajo za zaupanja vredne posameznike ali institucije, da bi pridobili osebne podatke ali denarna sredstva.

Prevare starih staršev, pri katerih se goljufi izdajajo za družinske člane, in prevare, ki vključujejo medicinske izdelke, so dodatne metode manipulacije.

Razumevanje teh nevarnosti je ključnega pomena za zaščito finančnega in čustvenega blagostanja starejših.

Prevare v odnosih – romantične prevare

— ZNAČILNOSTI NEVARNOSTI:

Prevara na spletnih zmenkih, znana tudi kot romantična prevara, se zgodi, ko je žrtev zavedena, da verjame, da je v romantičnem razmerju z nekom, ki ga je spoznala na spletu. Vendar je njen domnevni partner goljuf.

Vrste manipulacije v spletni romanci:

Prevaranti ustvarjajo lažne spletne profile in se predstavljajo, da so daleč stran od žrtve, največkrat v tujini, na misiji (zdravnik, vojak, filantrop), delajo na naftni ploščadi itd.

Prevarantovi interesi in hobiji so skoraj povsem enaki interesom in hobijem žrtve ... fotografije pa so preprosto ... WOW! Čeprav razen nekaj "popolnih" fotografij ni veliko (ali sploh nobenih) drugih fotografij, na katerih bi bil/-a prikazan/-a v različnih realnih in življenjskih situacijah.

Ko je vse videti rožnato (ljubezenska izjava, snubitev itd.), goljuf žrtve povabi k zasebni komunikaciji (tako pridobi njihovo telefonsko številko, e-poštni naslov in druge podatke) ter jim obljubi, da se bodo kmalu srečali osebno.

In ravno ko je vse videti še bolj rožnato, se pojavi zahteva po denarju, ki jo spremlja empatija vzbujajoča zgodba in zahteva po točno določenih načinih plačila (bančno nakazilo, na novo odprt bančni račun na ime žrtve ipd.).

**Lažna
identiteta**

Popolnost

**Hiter
napredek**

**Zahteva za...
DENAR**

Prevare v odnosih – romantične prevare



POSLEDICE:

Romantične prevare lahko povzročijo hude finančne izgube in veliko čustveno stisko za žrtve.

01 Finančne posledice

Ker žrtve pogosto verjamejo, da pomagajo ljubljeni osebi v stiski, so pripravljene uporabiti svoj denar in ga vložiti v razmerje. Zavaljo »ljubezni« nekateri žrtve celo žrtvujejo vse svoje prihranke, najamejo dodatna posojila ali celo prodajo svoje premoženje. Podatki, ki jih prevaranti pridobijo od žrtev (bančni račun, podatki o kreditni kartici), se lahko uporabijo za nepooblaščne transakcije ali dvige, kar povzroči znatne finančne izgube.

02 Čustvene posledice

Goljufije pri spletnih razmerjih so še posebej krute, saj igrajo na čustva ljudi. Razkritje, da je spletno razmerje prevara, žrtvi povzroči podobno čustveno škodo kot nenadna prekinitev razmerja, ki temelji na fizični interakciji. Zaradi tega žrtve pogosto težko prekinejo naklonjenost, ki jo čutijo do goljufa, tudi ko ugotovijo, da so bile prevarane.

03 Psihološke posledice

Žrtve romantičnih prevar so nagnjene k psihološkim bolečinam, kot so sram, zadrega, stres, tesnoba, depresija in strah. Žrtve lahko doživijo simptome, ki spominjajo na hujše depresivne motnje, žalovanje ali posttravmatsko stresno motnjo (PTSM).

Prevare v odnosih – romantične prevare

— NAČINI ZAŠČITE:



Dve leti po moževi smrti so vnuki prepričali Marto, naj se prijavi na spletno stran za zmenkarije. Kmalu je začela klepetati z moškim po imenu Tom, zdravnikom na humanitarni misiji v Afriki.

Po nekaj tednih prisrčnih pogovorov je Tom zatrdil, da ima "težave z denarnim prilivom" in da potrebuje denar za kritje stroškov. Marta je postala sumničava in se o nenavadni prošnji pogovorila z vnuki. Skupaj so raziskali njegov profil in ugotovili, da je Tom prevarant.

Na žalost prevaranta ...

Marta se je pravilno odločila, ko je svojim najbližjim odkrito povedala, da sumi, da gre za prevaro.



1. KORAK: Sledite intuiciji

Marta je začutila, da je nekaj narobe. Zaupala je svoji intuiciji in ni hitela s pomočjo Tomu, ampak je najprej razmislila o nenavadnosti njegove prošnje.

2. KORAK: Iskanje nasvetov zaupanja vrednih ljudi

Namesto da bi se odločila sama, se je Marta posvetovala z vnuki. Predstavila jim je vse podrobnosti Tomove prošnje in jih prosila za nasvet.

3. KORAK: Raziskujte

Marta je skupaj z vnuki raziskala Tomov profil in ugotovila, da gre za prevaranta. To spoznanje je Marti pomagalo, da mu ni poslala denarja in postala žrtev njegove prevare.

4. KORAK: Prijava

Marta je obvestila stran za zmenke, tako, da je stopila v stik z administratorjem strani in prijavila Toma zaradi suma goljufije.

Prevare v odnosih – romantične prevare



NAČINI ZAŠČITE:

Romantični prevaranti izkoriščajo osamljenost starejših, zlasti nedavno ovdovelih ali ločenih, ter izrabljajo njihovo ranljivost in finančna sredstva za vzpostavljanje lažnih spletnih romantičnih razmerij na platformah družabnih medijev, spletnih straneh za zmenke itd.

Tukaj je nekaj dodatnih nasvetov, če se morda znajdete v takšni situaciji.

Bodite previdni, kaj delite na spletu:

Informacije, ki jih delite javno (vaši interesi, hobiji, življenjski slog itd.), lahko prevaranti uporabijo za ustvarjanje lažne identitete, da bi pritegnili vaše romantično zanimanje.



V katerem koli spletnem razmerju zadržite svoje osebne/finančne podatke zase:

Ne delite preveč osebnih podatkov s potencialnim spletnim romantičnim partnerjem in vsekakor ne razkrivajte svojih finančnih podatkov.

Predvsem pa – **ne pošiljajte denarja ali kupujte dragocenosti nikomur, ki ga še niste srečali!**

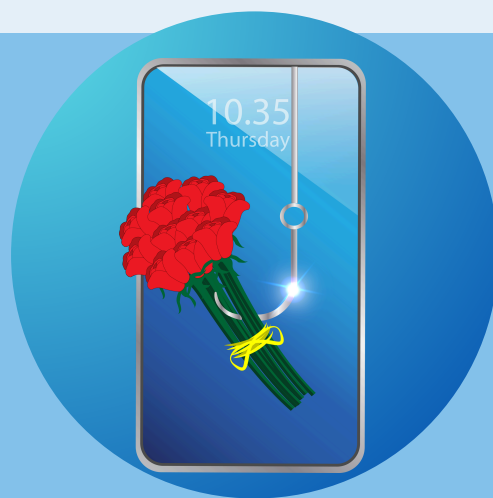
Prevare v odnosih – romantične prevare



NAČINI ZAŠČITE:

Preverite:

Čeprav ne morete preveriti vsega, kar vam romantični spletni partner pove, lahko nekatere konkretne podatke preverite tako, da **prek spleta preverite ime, priimek, kraj bivanja, profile v družabnih omrežjih, pristnost objavljenih in poslanih fotografij** ter preverite, **ali v komunikaciji uporablja reciklirane zgodbe ali izraze**, saj prevaranti pogosto večkrat uporabijo iste zgodbe in stavke.



Ne pozabite!

Če se vaš romantični spletni partner **noče srečati v živo, si izmišljuje izgovore, zakaj se ne more srečati, ali se nikoli ne udeleži video klica ali drugih oblik „interakcije“** v živo, se lahko zgodi, da ste se zapletli z goljufom.

Prevare v odnosih – romantična prevara



NAČINI ZAŠČITE:

Če ste delili gesla za svoje račune in ste zaznali sumljivo aktivnost, **nemudoma preverite, ali so bile nastavitve spremenjene, ter preverite zadnje prijave in aktivnosti v svojih računih.** Če opazite kakršne koli neznane ali sumljive prijave v računih, **obvestite svojega ponudnika storitev** in vaše **stike** ter jih opozorite, naj bodo pozorni na sumljiva sporočila, za katera se zdi, da prihajajo od vas.

Najboljši nasvet je, da spremenite vsa gesla, do katerih ste omogočili dostop!



REPORT

Če sumite, da je vaše spletno razmerje prevara, **nemudoma prenehajte komunicirati in blokirajte goljufa** v družabnih medijih, e-pošti, aplikacijah za sporočanje, spletnih mestih za zmenke itd.

Če so bili uporabljeni vaši bančni ali računi kreditnih kartic, takoj kontaktirajte banko ali policijo!

Razširite besedo!

SMS prevare – Smishing



ZNAČILNOSTI NEVARNOSTI:

Smishing je sestavljanka iz besed “SMS” (storitev kratkih sporočil) in “phishinga” (ribarjenje). V teh napadih kibernetски kriminalci pošiljajo lažna besedilna sporočila in poskušajo žrtve pretentati ali z njimi manipulirati, da razkrijejo osebne ali finančne podatke, tapajo na zlonamerne povezave ali prenesejo zlonamerno programsko opremo oz. zlonamerne aplikacije.

Vrste manipulacije pri smishingu:

Prevaranti zavajajo žrtve tako, da se v besedilnih sporočilih izdajajo za pravne ustanove, podjetja ali druge organizacije. V teh sporočilih žrtve pozivajo k takojšnjemu ukrepanju, na primer k tapanju na povezavo v sporočilu, odgovoru in posredovanju osebnih podatkov ali klicu določene številke.

Z uporabo situacije, ki bi lahko bila pomembna in relevantna za žrtve (npr. sporočilo banke, storitve kreditnih kartic, podpora strankam itd.), lahko goljufi ustvarijo učinkovito krinko in odpravijo kakršen koli sum, da gre morda za neželeno pošto.

Z intenziviranjem čustev žrtve je sporočilo prilagojeno posamezniku in sproži poseben čustveni odziv, kot je nujnost, strah ali radovednost. S temi taktikami prevaranti oblikujejo sporočila, s katerimi želijo žrtve spodbuditi k takojšnjemu ukrepanju.

**Lažno
predstavljanje**

**Možen in
verjeten
kontekst**

**Igranje
na čustva**

SMS prevare – Smishing



POSLEDICE:

Starejši zaradi pomanjkanja izkušenj s sodobnimi tehnologijami in znanja o kibernetiki varnosti pogosto težko prepoznajo znake nevarnosti v smishing sporočilih, kot so na primer lažni pozivi k akciji ali sumljive povezave. Starejši so običajno tudi manj sumničavi in pogosteje verjamejo zavajajočim SMS sporočilom.

01 Finančne posledice

Če žrtve razkrijejo svoje osebne ali finančne podatke, kot so številke kreditnih kartic ali številke bančnih računov, lahko utrpijo večjo finančno škodo, saj prevaranti te podatke uporabijo za izvedbo nepooblaščenih transakcij ali dvig denarja z žrtvinega računa. Te posledice lahko povzročijo resne finančne težave in dolgoročno škodo.

02 Kraja identitete

V primeru kraja identitete so vaši osebni podatki zlorabljeni, kar vpliva na vašo osebno varnost in zasebnost. Če podatki postanejo povezani še z nezakonitimi dejavnostmi, se lahko soočite tudi s pravnimi posledicami. Pridobitev vaše identitete nazaj je lahko zelo zamudna, saj vključuje številne administrativne (in tudi pravne) postopke.

03 Psihološke posledice

Smishing sporočila pogosto izkoriščajo čustva, kot so strah, panika ali zmedenost, kar lahko vpliva na psihično počutje žrtev.

SMS prevare – Smishing



NAČINI ZAŠČITE:



Peter je na pametni telefon prejel SMS-sporočilo od svoje banke, v katerem ga je banka obvestila, da je bil njegov račun začasno blokiran. Sporočilo je vsebovalo nenavadno zahtevo, da naj TAKOJ tapne na povezavo v sporočilu in tako aktivira svoj račun. Čeprav je Petra za trenutek zgrabila panika, se je odločil, da ne bo tapnil na povezavo, kajti sporočilo se mu je zdelo zelo sumljivo.

Na žalost prevaranta ...

Peter si je pred kratkim ogledal spletni izobraževalni video o smishingu in se naučil prepoznati značilnosti te vrste prevare.



1. KORAK: Prepoznavanje opozorilnih znakov

Peter je v sporočilu opazil tudi pravopisne napake in nerodno oblikovane stavke, kar je kazalo na to, da sporočilo ni bilo avtorizirano.

2. KORAK: Pomanjkanje osebnega stika

Peter je tudi opazil, da je bilo sporočilo anonimno in ni vsebovalo podatkov o banki ali kontaktni osebi, na katero bi se stranka lahko obrnila za dodatne informacije.

3. KORAK: Preverjanje informacij

Namesto da bi tapnil na povezavo je Peter poklical banko na telefonsko številko iz svojega imenika in pri banki preveril, ali je sporočilo resnično.

4. KORAK: Informiranje/prijava

Potem ko je Peter obvestil banko, ki je potrdila poskus prevare, je banka obvestila vse svoje komitente in poskus prevare prijavila pristojnemu organu.

SMS prevare – Smishing



NAČINI ZAŠČITE:

Pred morebitnimi posledicami smishing napadov se je zelo enostavno zaščititi – preprosto jih ignorirajte. Seveda ne smete prezreti vseh sporočil, saj so SMS sporočila legitimno orodje, da vas lahko dosežejo številni trgovci in druge ustanove.

Tukaj je nekaj dodatnih nasvetov, če se boste morda znašli v takšni situaciji.

Ne odgovarjajte:

Če prejmete nepričakovano ali sumljivo sporočilo, celo z zahtevo, da se odzovete, na primer s sporočilom "STOP", da se odjavite, je to lahko taktika, ki se uporablja za prepoznavanje aktivnih telefonskih števil in lahko vodi v prevaro.



Brez panike:

Tudi če se zdi sporočilo nujno, si vzemite čas in ne hitite.

NUJNE posodobitve računa ali NUJNE časovno omejene ponudbe obravnavajte kot potencialne znake smihinga!

Ostanite previdni!



SMS prevare – Smishing



NAČINI ZAŠČITE:

Ne uporabljajte povezav ali kontaktnih podatkov v sporočilu!

Preverite in vzpostavite stik neposredno prek uradnih komunikacijskih kanalov in ne prek podatkov ali informacij, ki so navedeni v sporočilu.

Ne pozabite! **Legitimne institucije (npr. banke, vladne službe itd.) nikoli ne zahtevajo občutljivih podatkov prek SMS sporočil ali prek necertificiranih povezav.**



Če sumite, da je prišlo do poskusa napada, **nemudoma spremenite vsa gesla in PIN kode.**

Poleg tega **spremljajte svoje finance in spletne račune** za neobičajne prijave ali kakršne koli druge sumljive aktivnosti.

Če ste žrtev smishinga, se obrnite na pristojne institucije, ki vam lahko nemudoma pomagajo. V primeru finančnega napada se obrnite na svojo banko, da zamrzne vaš račun ali prekliče vaše kreditne kartice.



Telefonske prevare starejših – Vishing



ZNAČILNOSTI NEVARNOSTI:

Telefonske prevare, znane tudi kot vishing, so še posebej učinkovite pri starejših. Tipične taktike vključujejo nepričakovane klice z neznanih ali tujih števil, lažnih števil ali platform, kot sta Viber in WhatsApp. Vishing klice lahko pošlje resnična oseba ali predhodno posnet robotski klic. Prevaranti uporabljajo govorne taktike za krajo zaupnih osebnih podatkov, kot so identifikacijski podatki, številke bančnih računov, prijavitni podatki in gesla.

Vrste manipulacij pri vishingu:

Prevaranti se pogosto izdajajo za uslužbence bank, državnih ustanov, zavarovalnic ali drugih znanih podjetij, da bi bili videti verodostojni ter na ta način prišli do finančnih in osebnih podatkov svojih žrtev.. Uporabljajo psihološke taktike za ustvarjanje občutka nujnosti in prepričujejo žrtve, da so v težavah. Žrtvam lahko celo grozijo in jih skušajo ustrahovati.

Prevaranti lahko uporabijo tudi prepričljiv jezik in ton, da žrtev prepričajo, da so na njeni strani. Zato pogosto vodijo pogovor na prijazen, dostopen, sočuten način in se zdijo ustrezljivi, med pogovorom pa pogosto uporabljajo dvoumen jezik ali spremenijo temo, da bi odvrnili pozornost žrtve.

Za prevarante je značilna vztrajnost, vključno s ponavljajočimi se klici z iste številke (žrtev lahko kontaktirajo tudi večkrat na dan itd.). Na ta način počasi in vztrajno pridobivajo žrtvino zaupanje. S to taktiko si pridobijo zaupanje žrtve in jo prepričajo, da razkrije občutljive podatke.

**Lažno
predstavljanje**

Prepričljivost

Vztrajnost

Telefonske prevare starejših – Vishing



POSLEDICE:

Starejši pogosto menijo, da so telefonski klici pomemben način komuniciranja, in cenijo osebno komunikacijo, ki jo omogoča telefonski klic. Prav zaradi visoke stopnje zaupanja v telefonsko (osebno) komunikacijo so bolj ranljivi za različne vrste telefonskih prevar in lažje verjamejo zavajajočim zahtevam goljufov po informacijah ali ukrepih.

01 Finančne posledice

Žrtve telefonskih prevar pogosto utrpijo neposredno finančno škodo. Prevaranti lahko žrtve zavedejo, da izvedejo plačila ali posredujejo bančne podatke, kar vodi do nepooblaščenih transakcij ali izpraznitve bančnih računov. To lahko znatno vpliva na njihove prihranke in finančno varnost.

02 Kraja identitete

Telefonske prevare pogosto vključujejo krajo osebnih podatkov, kot so številke socialnega zavarovanja, datumi rojstva in naslovi. Žrtve se lahko pri reševanju teh težav in povrnitvi svoje identitete soočijo z velikimi izzivi.

03 Oškodovanje finančnega ugleda

Če je posledica prevare nepooblaščen finančna dejavnost ali transakcija, lahko žrtev utрпи tudi škodo na svojem finančnem ugledu. Ponovna vzpostavitev ugleda je lahko zapletena in zahteva obsežno dokumentacijo ter komunikacijo s finančnimi institucijami.

Telefonske prevare starejših – Vishing



NAČINI ZAŠČITE:



Andreja je po telefonu poklicala oseba, ki se je predstavila kot predstavnik zdravstvene zavarovalnice, z zahtevo po dodatnih informacijah za posodobitev Andrejeve zdravstvene dokumentacije. Klicatelj je bil zelo prijazen, vendar se ni predstavil z imenom in priimkom. Dejal je le, da kliče v imenu zavarovalnice, in pojasnil, da gre za rutinsko preverbo. Ko je začel spraševati po osebnih podatkih, kot sta številka zavarovanja in datum rojstva, je Andrej postal sumničav.

Na žalost prevaranta ...

Andrej aktivno sodeluje v spletnih forumih in skupnostih, kjer se razpravlja o varnostnih vprašanjih in se izmenjuje izkušnje s spletnimi prevarami.



1. KORAK: Preverjanje identitete klicatelja

Andrej na uradni spletni strani zavarovalnice ni mogel preveriti identitete klicatelja, saj domnevni uslužbenec zavarovalnice ni navedel svojega polnega imena, zato je postal sumničav.

3. KORAK: Uporaba prejšnjega znanja

Andrej je prepoznal znake prevare zaradi aktivnega sodelovanja na spletnih forumih, kjer se razpravlja o varnostnih vprašanjih in spletnih prevarah, kar mu je pomagalo, da je hitro opazil sumljive elemente klica.

2. KORAK: Bodite pozorni na sumljive zahteve

Ko je klicatelj začel spraševati po osebnih podatkih, kot sta številka zavarovanja in datum rojstva, je Andrej podvomil o pristnosti klica in klic takoj prekinil.

4. KORAK: Informiranje/prijava

Andrej je neposredno poklical svojo zdravstveno zavarovalnico, da bi preveril, ali je bil klic poskus prevare, in o tem razširil besedo na forumih in skupnostih, kjer je aktiven.

Telefonske prevare starejših – Vishing



NAČINI ZAŠČITE:

Zaradi pospešenega napredka telekomunikacijske tehnologije so prevaranti izkoristili anonimnost in enostaven dostop do telefonskih klicev za izvajanje goljufivih dejavnosti. Zato je ključnega pomena, da starejši ohranijo visoko stopnjo pozornosti in se zavedajo tveganj, povezanih s komunikacijo po telefonu.

Tukaj je nekaj dodatnih nasvetov, če se morda znajdete v takšni situaciji.

Ignorirajte nepričakovane klice z neznanih števil ali jih preprosto pustite v glasovni pošti in se na podlagi posredovanih informacij odločite, ali boste klic vrnili.

Ne uporabljajte številke za povratni klic, ki jo navedejo, saj je lahko del prevare. Namesto tega **poiščite uradno telefonsko številko in neposredno pokličite ter potrdite upravičenost zahteve.**



Nikoli ne delite finančnih ali osebnih podatkov po telefonu!

Če poskušajo pridobiti od vas tovrstne podatke, takoj odložite slušalko!

Telefonske prevare starejših – Vishing



NAČINI ZAŠČITE:

Preverite linijo:

Zavedajte se, da lahko goljufi ohranijo odprto telefonsko linijo tudi po tem, ko ste odložili slušalko.

Uporabite drug telefon in preverite, če je linija prosta, ali pa **počakajte vsaj 10 do 15 minut**, da se prepričate, da so morebitni prevaranti odložili slušalko.



Poskusite blokirati klice:

Aktivirajte funkcije blokiranja klicev v telefonu, da filtrirate morebitne vishing prevare. Večina pametnih telefonov ponuja te funkcije.

Če nimate pametnega telefona, se obrnite na ponudnika telefonskih storitev in preverite, katere storitve ponuja za blokiranje neželenih klicev.

Če ste žrtev vishinga, se takoj obrnite na ustrezne institucije, ki vam lahko pomagajo.



Prevare, ki izkoriščajo čustvene družinske vezi

— ZNAČILNOSTI NEVARNOSTI:

Prevara starih staršev (ti. "Grandparent scam") je vrsta goljufije, pri kateri goljufi izkoriščajo čustvene vezi med starimi starši in njihovimi vnuki. Prevarant se običajno pretvarja, da je vnuk v stiski in potrebuje takojšnjo finančno pomoč.

Vrste manipulacije v prevari starih staršev:

Prevarant ustvari občutek nujnosti, z namenom da prepreči starim staršem, da bi preveč premišljevali ali stopili v stik z drugimi družinskimi člani.

Prevaranti lahko stare starše pozovejo, naj situacijo ohranijo v tajnosti, češ da jim je nerodno ali da se bojijo, da bi se znašli v še večjih težavah.

Prevaranti izkoriščajo ljubezen in skrb starih staršev za vnuke, da bi dosegli takojšen odziv.

Nujnost

Tajnost

**Čustveno
manipulacija**

Prevare, ki izkoriščajo čustvene družinske vezi



POSLEDICE:

Če postanete žrtev prevare starih staršev, ima to lahko hude posledice.

01 Finančna izguba

Iz finančnega vidika lahko izgubite težko prislužen denar, saj goljufi pogosto zahtevajo visoke zneske, ki lahko izčrpajo vaše prihranke. Če jim posredujete svoje bančne podatke, lahko ukradejo še več.

02 Čustvena stiska

Iz čustvenega vidika lahko lažne nujne pomoči povzročijo velik stres in tesnobo, ob odkritju, da je šlo za prevaro, pa se lahko počutite globoko izdane in prizadete.

03 Izguba zaupanja

Ta izkušnja lahko privede do izgube zaupanja, zaradi česar dvomite v resnične primere za nujno pomoč in postanete nezaupljivi do vseh kontaktov in interakcij, tudi tistih, ki prihajajo iz verodostojnih virov.

04 Izolacija

Poleg tega se lahko počutite v zadregi ali se sramujete, zaradi česar ne želite komunicirati o finančnih zadevah z družino ali prijatelji; Goljufi pa vas lahko ponovno izberejo za tarčo, saj vas obravnavajo kot lahek plen.

Prevare, ki izkoriščajo čustvene družinske vezi

— NAČINI ZAŠČITE:



Marica živi sicer sama, vendar ima z družino, zlasti z vnuki zelo tesen odnos. Nekega večera jo je poklical neznanec, ki se je predstavljal za njenega vnuka Jana in urgentno zahteval veliko vsoto denarja. Ta klic je za Marico pomenil neprijetno izkušnjo. Vendar se Marica spominja nasveta, ki ji ga je dal njen vnuk, da je potrebno biti previden pri telefonskih klicih z osebami, ki prosijo za denar.

Maricina izkušnja opozarja, kako pomembno je biti obveščen o prevarah in preverjati vse urgentne in čustvene prošnje za denar. Z razumevanjem taktik, ki jih uporabljajo prevaranti, kot so ustvarjanje nujnosti, zahteva po tajnosti in manipuliranje s čustvi, se lahko starejši bolje zaščitijo, da ne postanejo žrtve. Če ste v dvomih, vedno preverite informacije pri drugih družinskih članih in nikoli ne hitite s pošiljanjem denarja.



1. KORAK: Preverjanje

Mary je klicatelju zastavila vprašanja, katere odgovore bi poznal le Jan in nemudoma poklicala Jana, da bi se izognila prevari.

2. KORAK: Ozaveščanje

Z vnaprejšnjim informiranjem o takšnih prevarah je Marica lažje prepoznala opozorilne znake.

3. KORAK: Komunikacija

Marica se je z družino že pogovarjala o potencialnih prevarah. Dodatno zaščitol pa lahko za nujne primere zagotovi tudi vzpostavitev družinske šifre.

Prevare, ki izkoriščajo čustvene družinske vezi



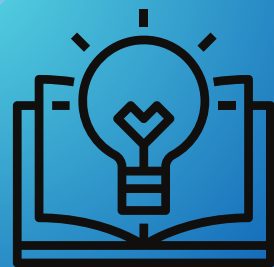
NAČINI ZAŠČITE:

Zaščita pred goljufijami, ki izkoriščajo čustvene družinske vezi, je ključnega pomena za zaščito vašega težko prisluženega denarja. Tukaj je nekaj enostavnih korakov, ki jih lahko naredite.

Bodite obveščeni:

Izobražujte sebe in svoje ljubljene o pogostih prevarah, ki ciljajo na starejše, vključno s prevaro starih staršev.

Spremljajte verodostojne vire informacij in bodite na tekočem z novimi taktikami, ki jih lahko uporabljajo prevaranti.



Preverite identiteto:

Vedno postavljajte vprašanja, ki jih lahko pozna le pravi družinski član, na primer ime hišnega ljubljence ali poseben družinski dogodek.

Če ste v dvomih, pokličite nazaj na znano številko, da preverite identiteto klicatelja.

Vzpostavite družinsko šifro:

V družini vzpostavite skrivno šifro, ki jo bodo poznali le zaupanja vredni posamezniki.

To šifro uporabite v nujnih primerih, da preverite identiteto klicateljev, ki se predstavljajo kot družinski člani.



Prevare, ki izkoriščajo čustvene družinske vezi



NAČINI ZAŠČITE:

Izogibajte se hitrim odločitvam:

Pri nepredvidenih ali nujnih prošnjah za denar si vzemite čas.

Prevaranti izkoriščajo urgentnost, z namenom, da bi vam preprečili dvomiti v njihovo zgodbo ali poiskati nasvet pri drugih.



Uporabite ID klicatelja in blokiranje klicev:

Uporabite ID klicatelja (funkcija, ki na vašem telefonu prikaže številko in ime osebe ali organizacije, ki vas kliče) za pregledovanje dohodnih klicev in funkcijo blokiranje neznanih ali sumljivih števil.

Prijavite prevarantske klice svojemu ponudniku telefonskih storitev ali ustreznim organom.

Varujte osebne podatke:

Bodite previdni pri posredovanju osebnih in finančnih podatkov po telefonu ali spletu. Izogibajte se posredovanju občutljivih podatkov, če niste prepričani o identiteti prejemnika.



Prevare, ki vključujejo medicinske izdelke

— ZNAČILNOSTI NEVARNOSTI:

V zadnjih letih so prevaranti vse pogostejše ciljali na ranljive posameznike, vključno s starejšimi, z goljufijami, povezanimi z medicinskimi izdelki. Te prevare pogosto izkoriščajo čustva in strahove, povezane z zdravstvenimi težavami, ter obljublajo čudežna zdravila, tretmaje ali rešitve, ki so preprosto preveč dobri, da bi bili resnični.

Vrste manipulacij pri prevarah z medicinskimi izdelki:

Prevaranti o svojih izdelkih navajajo drzne trditve in obljublajo čudežne rezultate z malo ali brez znanstvenih dokazov.

Pogosto uporabljajo prodajne taktike visokega pritiska in vas pozivajo k hitremu nakupu, preden poteče "časovno omejena ponudba".

Te prevare igrajo na vaša čustva, izkoriščajo vaše strahove pred zdravstvenimi težavami in ponujajo lažno upanje za hitro in enostavno rešitev.

**Lažne
obljube**

**Taktike
visokega
pritiska**

**Čustvena
manipulacija**

Prevare, ki vključujejo medicinske izdelke



POSLEDICE:

Manipulacija z medicinskimi izdelki ima lahko resne negativne učinke, kot so:

01 Finančna izguba

Če postanete žrtev prevare z medicinskimi izdelki, lahko za neučinkovite ali celo nevarne izdelke porabite velike vsote denarja in s tem izčrpate svoje prihranke.

02 Zdravstvena tveganja

V nekaterih primerih goljufi uporabljajo nenadzorovane ali ponarejene medicinske izdelke, ki lahko v povezavi z uporabo obstoječih (regularnih) zdravil povzročijo resne zdravstvene zaplete.

03 Čustvena stiska

Prevara lahko povzroči občutke sramu, krivde in zadrege. Lahko se počutite izdano in anksiozno, kar lahko negativno vpliva na vaše splošno duševno zdravje in dobro počutje.

04 Poslabšanje kakovosti življenja

Skupni učinki finančne izgube, zdravstvenih tveganj in čustvenih stisk lahko znatno poslabšajo kakovost življenja žrtev. Žrtve imajo lahko težave z obvladovanjem vsakodnevnih aktivnosti in ohranjanjem samostojnosti.

Prevare, ki vključujejo medicinske izdelke

— NAČINI ZAŠČITE:



Tomaž prejme e-pošto o novem "čudežnem dodatku", ki naj bi čez noč pozdravil artritis, diabetes in visok krvni tlak. V sporočilu ponujajo časovno omejen popust in ga spodbujajo, naj kupi takoj, da ne zamudi priložnosti za boljše zdravje. Vendar se Tomaž spomni nasveta, ki ga je prebral o previdnosti pri čudežnih zdravilih.

Tomaževa zgodba žal ni edini primer. Prevare z medicinskimi izdelki izkoriščajo ranljivost in čustva starejših ter obljubljajo hitre rešitve za zapletene zdravstvene težave. Če ostanete informirani, skeptični in se posvetujete z zdravstvenimi delavci, se lahko zaščitite pred tem, da bi postali žrtve teh goljufivih shem. Ne pozabite, da je vaše zdravje neprecenljivo in da do dobrega počutja ni bližnjic.



1. KORAK: Bodite skeptični

Tomaž se je spomnil, da so legitimni medicinski dosežki strogo testirani in potrjeni s strani strokovnjakov.

2. KORAK: Posvetujte se s strokovnjaki

Tomaž je poklical svojega osebnega zdravnika in se pogovoril o morebitnih novih zdravljenjih ali dodatkih.

3. KORAK: Raziskovanje

Tomaž je pred odločitvijo o nakupu poiskal nepristranska mnenja in znanstvene dokaze, ki potrjujejo trditve o izdelku.

Prevare, ki vključujejo medicinske izdelke

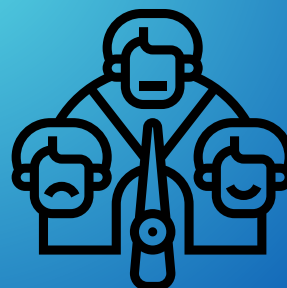


NAČINI ZAŠČITE:

Ne pozabite, da je zaščita pred prevarami z medicinskimi izdelki ključnega pomena za zaščito vašega težko prisluženega denarja in vašega zdravja. Eden najpomembnejših korakov je tudi iskanje čustvene podpore. Tukaj je nekaj enostavnih korakov, ki jih lahko naredite.

Poiščite čustveno podporo:

Socialna podpora družine, prijateljev in članov skupnosti lahko starejšim nudi čustveno moč in zagotovilo, ki ga potrebujejo, da se uprejo manipulaciji. Ko se starejši počutijo podprte in cenjene, je manj verjetno, da bodo postali žrtev prevarantov, ki izkoriščajo čustveno ranljivost.



Bodite obveščeni:

Družabna omrežja so lahko pomemben vir informacij. Družinski člani in prijatelji lahko delijo opozorila o aktualnih prevarah, svetujejo, kako prepoznati prevare, in predlagajo preverjene vire za nakup medicinskih izdelkov ali zdravljenja. Če ostanete obveščeni prek socialne podpore, lahko znatno zmanjšate tveganje, da bi se ujeli v goljufijo.

Prevare, ki vključujejo medicinske izdelke



NAČINI ZAŠČITE:

Posvetujte se z zdravstvenimi delavci:

Preden preizkusite kakršen koli nov medicinski izdelek ali zdravljenje, se posvetujte s svojim zdravnikom, da se prepričate o njegovi varnosti in učinkovitosti.



Bodite skeptični do trditev o čudežih:

Če za izdelek navajajo, da zdravi več nepovezanih zdravstvenih stanj ali da ponuja hitre in enostavne rezultate, je verjetno preveč dober, da bi bil resničen.

Temeljito raziskujte:

Vzemite si čas za raziskovanje izdelka in podjetje, ki ga proizvaja. Poiščite ocene iz verodostojnih virov in preverite, ali so izdelek odobrile regulativne in druge pristojne agencije.



Dodatno branje



PREVARE V ODNOSIH – ROMANTIČNA PREVARA

- <https://www.sciencedirect.com/science/article/pii/S2949791423000441>
- <https://hu.usembassy.gov/be-wary-of-online-romance-scams/>
- <https://consumer.ftc.gov/articles/what-know-about-romance-scams#whatis> <https://us.norton.com/blog/online-scams/romance-scams>
- <https://www.unit21.ai/fraud-aml-dictionary/romance-fraud>
- <https://www.hsbc.co.uk/help/security-centre/romance-scams-case-study/>
- <https://www.equifax.co.uk/resources/identity-protection/how-to-spot-and-avoid-romance-scams.html>
- <https://dfpi.ca.gov/2024/03/05/romance-scams-what-consumers-need-to-know/>
- <https://complyadvantage.com/insights/what-is-a-romance-scam/>



SMS PREVARE – SMISHING

- <https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it>
- <https://www.proofpoint.com/us/threat-reference/smishing>
- <https://www.sinch.com/blog/what-is-smishing/>
- <https://business.bofa.com/en-us/content/what-is-smishing-how-to-prevent-it.html>
- https://www.forbes.com/advisor/business/what-is-smishing/#how_to_protect_against_smishing_section
- <https://www.techtarget.com/searchmobilecomputing/definition/SMiShing>
- <https://cybeready.com/category/the-complete-guide-to-smishing>
- <https://www.rd.com/article/what-is-smishing/>

Dodatno branje



TELEFONSKE PREVARE STAREJŠIH – VISHING

- <https://www.ageuk.org.uk/information-advice/money-legal/scams-fraud/phone-scams/>
- https://www.ageuk.org.uk/globalassets/age-uk/documents/information-guides/ageukig05_avoiding_scams_inf.pdf
- <https://www.helpguide.org/articles/abuse/elder-scams-and-senior-fraud-abuse.htm>
- <https://www.seniorliving.org/research/common-elderly-scams/>
- <https://www.ooma.com/blog/home-phone/protect-seniors-from-elderly-phone-scams>
- https://taking.care/blogs/resources-advice/scams-targeting-the-elderly#How_to_avoid
- <https://www.terranovasecurity.com/solutions/security-awareness-training/what-is-vishing>
- <https://www.kaspersky.com/resource-center/definitions/vishing>
- <https://www.proofpoint.com/us/threat-reference/vishing>



PREVARE, KI IZKORIŠČAJO ČUSTVENE DRUŽINSKE VEZI

- <https://www.homeinstead.com/location/347/news-and-media/the-grandparent-scam/>
- <https://www.europol.europa.eu/media-press/newsroom/news/crime-against-elderly-four-arrests-in-germany-and-poland>
- <https://www.identityguard.com/news/grandparent-scam#:~:text=%20najpogostejša%20prevara%20starih%20staršev,za%20katere%20se%20pogosto%20trdi,da%20so%20%20v%20tujini.>
- <https://www.cbsnews.com/news/what-being-targeted-by-grandparent-scam-sounds-like-60-minutes/>
- <https://www.youtube.com/watch?v=v2VFy2igHPE>
- <https://globalnews.ca/video/9901367/calgary-senior-falls-victim-to-grandparents-scam-costing-her-thousands>

Dodatno branje



PREVARE, KI VKLJUČUJEJO MEDICINSKE IZDELKE

- <https://www.forres-gazette.co.uk/news/older-people-targeted-by-medical-scam-116453/>
- <https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products>
- <https://www.ema.europa.eu/en/human-regulatory-overview/public-health-threats/falsified-medicines-overview>
- <https://www.bbc.com/news/business-58029113>
- <https://www.europol.europa.eu/media-press/newsroom/news/544-arrests-and-%E2%82%AC63-million-of-fake-pharmaceuticals-and-illegal-doping-substances-seized>

4. POGLAVJE

PREVARE PRI SPLETNIH TRANSKCIJAH

V dobi spletnih plačil in transakcij je vedno več poročil o spletnih prevarah. Prevaranti izkoriščajo dejstvo, da imajo mnogi starejši manj izkušenj z novimi tehnologijami, kar jih dela dovzetnejše za prevare. V tem poglavju bomo razpravljali o najpogostejših prevarah pri spletnih transakcijah, da bi starejšim pomagali pri njihovem prepoznavanju in preprečevanju.

Prevare na področju potovanj in nakupov vozovnic vključujejo ponujanje fiktivnih ponudb, ki se nikoli ne uresničijo. Pri naročniških goljufijah so starejši prevarani, da sprejmejo storitve, ki samodejno zaračunavajo stroške. Pri prevarah s naročninami so starejši prevarani v sprejemanje storitev, za katere se samodejno zaračunavajo pristojbine. Lažne spletne trgovine izsiljujejo plačila za nedostavljene izdelke. Prevare pri nakupu in prodaji vključujejo lažne nakupe, pri katerih izdelki niso navedeni na seznamu ali niso na voljoter situacije, ko starejši prodajajo svoje stvari na spletnih oglasnikih.

Razumevanje teh groženj je ključno, da lahko starejši varno izkoristijo priložnosti, ki jih ponuja internet, in zaščitijo svoje finance pred prevarami.

Prevare pri potovanjih in nakupu vozovnic

— ZNAČILNOSTI NEVARNOSTI:

Prevare pri potovanjih in prodaji vozovnic so goljufive sheme, ki vključujejo prodajo lažnih potovalnih paketov, izletov in vozovnic. Ta vrsta prevar se pogosto pojavlja na spletu, kjer goljufi vzpostavijo profesionalno oblikovane spletne strani ali pošiljajo e-poštna sporočila, ki ponujajo zelo ugodne ponudbe. Starejši, ki slabše poznajo sodobne spletne taktike goljufanja, so še posebej izpostavljeni tem prevaram. Nevedni kupci, še posebej starejši, ki jih pritegnejo te ponudbe, plačajo za neobstoječe storitve in ostanejo brez možnosti povračila, ko se zavedo, da so bili ogoljufani. Izobraževanje starejših o teh goljufivih shemah je ključnega pomena, da bi se jim tako izognili znatni finančni izgubi in čustveni stiski. Ključnega pomena je, da starejše poučimo o teh goljufivih shemah in jim tako pomagamo preprečiti veliko finančno izgubo in čustveno stisko.

Vrste prevar pri potovanjih in nakupu vozovnic:

Gre za prevare v katerih goljufi prodajajo neobstoječe letalske vozovnice. Goljufi lahko vzpostavijo lažne spletne strani, ki so videti kot spletne strani pravih letalskih prevoznikov, privabijo stranke z ugodnimi cenami vozovnic, nato pa po prejemu plačila izginejo.

Prevaranti ponujajo bogate počitniške pakete po zelo ugodnih cenah. Ko kupec plača, ugotovi, da paket ne obstaja ali da ne vključuje obljubljenega.

Prevaranti se lahko predstavljajo kot prodajalci ali posredniki in obljublajo ugodne ponudbe nepremičnin za določen časovni zakup. Zahtevajo vnaprejšnje plačilo in po prejetju plačila pa preprosto izginejo.

**Ponarejene
letalske
karte**

**Lažni
počitniški
paketi**

**Prevare s
časovnim
zakupom**

Prevare pri potovanjih in nakupu vozovnic



POSLEDICE:

Prevare pri potovanjih in nakupu vozovnic imajo lahko resne negativne učinke, kot so:

01 Finančna izguba

Najbolj neposredna posledica prevar na področju potovanj in prodaje vozovnic je finančna škoda. Goljufi poberejo denar za neobstoječe storitve, žrtve pa nimajo nobene možnosti, da bi izterjale svoj denar.

02 Kraja identitete

Te vrste prevare pogosto pod pretvezo rezervacije potovanja zahtevajo, da žrtev posreduje občutljive osebne in finančne podatke. Ti podatki se lahko nato uporabijo za krajo identitete.

03 Čustvena stiska

Če postanete žrtev takšne goljufije, vam to lahko povzroči veliko čustveno stisko. Navdušenje ob načrtovanem potovanju se spremeni v razočaranje in frustracijo, poleg tega pa se pojavljajo tudi občutki ogroženosti in ranljivosti po tem, ko ste bili ogoljufani.

Prevare pri potovanjih in nakupu vozovnic

— NAČINI ZAŠČITE:



Nekega dne je Jure prejel e-poštno sporočilo spletne potovalne agencije, ki je ponujala izjemno ugodno ponudbo za paket počitnic v Evropi. Ponudba je vključevala lete, nastanitev in ogled znamenitosti v Rimu, Parizu in Londonu. Paket je bil zelo ugoden in Jure, navdušen nad možnostjo sanjskega potovanja, se je odločil, da ga bo podrobneje raziskal. Kliknil je na spletno stran potovalne agencije, ki je bila videti zelo profesionalno in je vključevala visokokakovostne slike destinacij ter navdušujoča pričevanja zadovoljnih strank. Prepričan, se je odločil rezervirati počitniški paket. Vnesel je podatke o svoji kreditni kartici in prejel elektronsko sporočilo s potrditvijo rezervacije. Dnevi so se spremenili v tedne, Jure pa ni prejel nobenega nadaljnjega sporočila o svojem potovanju. Postal je zaskrbljen in je poskušal stopiti v stik s potovalno agencijo, vendar je ugotovil, da je telefonska številka izključena, njegova elektronska sporočila pa so ostala brez odgovora.

Juretova zgodba kaže na potrebo po izobraževanju starejših o spletnih prevarah. Ker starejši postajajo vse bolj tehnično spretni, so izpostavljeni večjemu tveganju. Z obveščanjem o znakih prevar, kot so pretirano ugodne ponudbe, in o pomenu preverjanja pristnosti podjetja pred nakupom jim lahko pomagamo, da ostanejo varni. Z izmenjavo takšnih izkušenj lahko starejše učinkovito opozorimo na spletne goljufije.



1. KORAK: Preverjanje verodostojnosti proti zaupanju

Jure je potovalni agenciji zaupal na osnovi profesionalno oblikovane spletne strani in navedenih mnenj strank, brez dodatnega preverjanja. Jure bi moral preveriti verodostojnost potovalne agencije tako, da bi preveril mnenja strank, registracijo potovalne agencije in njen fizični naslov ter ocenil njeno odzivnost tako, da bi jo neposredno kontaktiral.

2. KORAK: Uporaba varnega načina plačila proti neposrednemu vnosu podatkov o kreditni kartici

Jure je podatke o svoji kreditni kartici vnesel neposredno na spletno stran potovalne agencije, ne da bi preveril varnost plačilnega postopka. Jure bi moral uporabiti varne načine plačila, ki zagotavljajo zaščito kupca, kot je npr. uporaba kreditne kartice prek zaupanja vredne plačilne platforme, in se izogibati neposrednemu posredovanju podatkov o kreditni kartici na neznani spletni strani.

3. KORAK: Nadaljnja komunikacija proti čakanju brez ukrepanja

Jure je več tednov čakal, ne da bi prejel kakršno koli nadaljnjo komunikacijo o svojem potovanju, in je poskušal stopiti v stik z agencijo šele, ko ga je začelo skrbeti. Jure bi moral že kmalu po opravljeni rezervaciji nadaljevati stik s potovalno agencijo, da bi potrdil podrobnosti in zagotovil neprekinjeno komunikacijo.

4. KORAK: Prijava sumljive dejavnosti proti zapoznelemu odzivu

Jure je odlašal s kontaktiranjem izdajatelja kreditne kartice, dokler ni ugotovil, da je nekaj narobe. Jure bi moral vsako sumljivo dejavnost ali pomanjkljivo komunikacijo nemudoma prijaviti izdajatelju kreditne kartice, ki bi lahko ustavil transakcijo in raziskal zadevo.

Prevare pri potovanjih in nakupu vozovnic



NAČINI ZAŠČITE:

Starejši se morajo nujno zaščititi pred prevarami pri potovanjih in prodaji vozovnic, da bi se izognili veliki finančni izgubi, čustveni stiski in morebitni kraji identitete. Goljufi pogosto ciljajo na starejše, ki morda slabše poznajo taktike spletnih prevar, in izkoriščajo njihovo zaupanje TER navdušenje nad potovalnimi ponudbami. Če se starejši ustrezno zaščitijo, lahko preprečijo krajo težko prisluženega denarja, zagotovijo varnost svojih osebnih podatkov in preprečijo, da bi jim goljufive sheme pokvarile potovalne načrte.

Temeljito raziščite podjetje:

Pred nakupom vedno opravite temeljito raziskavo podjetja. Poiščite mnenja in ocene strank, da ugotovite verodostojnost podjetja in se prepričate o njegovi legitimnosti. Na ta način boste pridobili boljši vpogled v ugled podjetja ter izkušnje njegovih preteklih strank.



Uporabljajte samo varne načine plačila:

Pri spletnem nakupovanju je ključno, da uporabljate le varne načine plačila. Izogibajte se neposrednim bančnim nakazilom in ne delite podatkov o kreditni kartici na platformah, ki niso ustrezno zavarovane. Vedno je varneje izbrati plačilne načine, ki vključujejo zaščito kupca.

Prevare pri potovanjih in nakupu vozovnic



NAČINI ZAŠČITE:

Bodite previdni pri ponudbah, ki se zdijo preveč dobre, da bi bile resnične:

Če se ponudba ali popust zdi predober, da bi bil resničen, verjetno tudi je. Še posebej bodite previdni pri močno znižanih cenah za izdelke, kot so letalske vozovnice ali počitniški paketi. Preden se odločite za takšne ponudbe, je vedno bolje opraviti manjšo tržno raziskavo.



CONTACT US

Neposredno se obrnite na letalsko družbo ali hotel:

Če prejmete e-poštno sporočilo s ponudbo znižanega leta ali bivanja v hotelu, je dobro, da kontaktirate neposredno letalsko družbo ali hotel, da preverite ponudbo. Tako se boste prepričali, da je ponudba verodostojna in da ne gre za prevaro.

Zagotovite, da so vaši osebni podatki varni:

Pri deljenju osebnih podatkov bodite previdni. Pred vnosom občutljivih podatkov vedno preverite, ali je platforma varna. Nikoli ne delite pomembnih osebnih podatkov na platformah, ki nimajo ustreznih varnostnih ukrepov.



Prevare z naročninami

— ZNAČILNOSTI NEVARNOSTI:

Prevara z naročninami je vrsta goljufije, pri kateri so posamezniki zavedeni, da se brez njihovega vedenja prijavijo na draga članstva ali storitve. Te prevare pogosto povzročijo redne stroške, ki jih je težko prekiniti, kar prizadene ranljive posameznike, vključno s starejšimi.

Vrste manipulacij pri naročniških prevarah:

Prevaranti uporabljajo zavajajoče oglase ali pojavna okna, da vas zvabijo k prijavi na nekaj, kar se zdi kot brezplačna preizkusna različica ali cenovno ugodna storitev.

Pogoji naročnine, vključno s stroški in trajanjem, so pogosto skriti v drobnem tisku ali sploh niso jasno pojasnjeni.

Po registraciji se naročnina samodejno podaljša, kar povzroči nepričakovane obremenitve kreditne kartice ali bančnega računa.

Preklic naročnine je namerno otežen z zapletenimi postopki, neodzivno službo za pomoč uporabnikom ali nejasnimi pravili za preklic in prekinitev naročnine.

**Zavajajoči
oglasi in
povezave**

Skriti pogoji

**Samodejna
podaljšanja**

**Težava pri
preklicu**

Prevare z naročninami

— POSLEDICE:

Prevare pri naročninah imajo lahko resne negativne učinke, kot so:

01 Finančna izguba

Če postanete žrtev naročniške prevare, lahko izgubite težko zaslužene prihranke. Zaradi ponavljajočih se bremenitev, ki jih niste predvideli ali se z njimi strinjali, lahko izgubite precej denarja.

02 Kraja identitete

Posredovanje osebnih in podatkov za plačevanje na prevarantskih spletnih straneh lahko privede do kraje identitete in nadaljnje finančne škode.

03 Čustveni stres

Razočaranje in stres zaradi neavtoriziranih obremenitev in poskusa preklica naročnine lahko vplivata na vaše čustveno počutje.

Prevare z naročninami

— NAČINI ZAŠČITE :



David je na spletu videl oglas za brezplačen preizkus novega vitaminskega dodatka. Oglas je trdil, da mora za naročnino plačati le nekaj denarja za dostavo, nato pa bo do konca leta neomejeno prejemal vitamine. Navdušen nad možnostjo, da bi preizkusil vitaminski dodatek, se je odločil, da bo vnesel podatke o svoji kreditni kartici in tako poravnal stroške pošiljanja. Medtem ko je to počel, se je David spomnil, kar je prebral o nekaterih spletnih straneh, ki ljudem nevede jemljejo denar. Kaj je torej David naredil?



Prevara z naročninami je lahko draga in frustrirajuča izkušnja, še posebej za starejše osebe. Z budnostjo, skrbnim branjem drobnega tiska in aktivnim zaščitnim ukrepanjem svojih osebnih ter finančnih podatkov se lahko izognete temu, da postanete žrtev teh prevar. Vedno pristopite previdno k brezplačnim preizkusom in ponudbam s popustom ter se prepričajte, da temeljito razumete vse pogoje, preden posredujete svoje plačilne informacije. Bodite obveščeni, bodite previdni in se zaščitite pred naročniškimi prevarami.

1. korak: Preberite drobni tisk

Preden se je prijavil, je David iskal morebitne omembe tekočih naročnin ali dodatnih stroškov.

2. korak: Raziskovanje

Poiskal je podjetje in prebral ocene, da bi ugotovil, ali so tudi drugi imeli podobne izize.

3. korak: Spremljajte bančne izpiske

Redno je preverjal bančne izpiske, da bi pravočasno odkril nepooblašcene stroške.

Prevare z naročninami

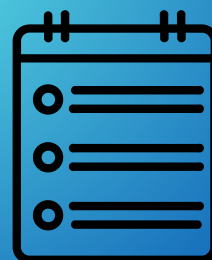


NAČINI ZAŠČITE:

Zaščita pred naročniškimi prevarami je ključnega pomena za zaščito vašega težko prisluženega denarja. Tukaj je nekaj enostavnih korakov, ki jih lahko naredite.

Preberite drobni tisk:

Vedno preberite določila in pogoje, preden se prijavite za katero koli storitev, še posebej, če vključuje brezplačno preskusno ali znižano ponudbo.

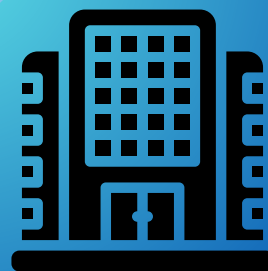


Bodite previdni pri brezplačnih preizkusih:

Bodite previdni pri brezplačnih preizkusih, ki zahtevajo vaše podatke o kreditni kartici. Preverite, ali se preizkus samodejno pretvori v plačljivo naročnino in kakšni bodo stroški.

Raziščite podjetje:

Poiščite mnenja in ocene podjetja, ki ponuja naročnino. Prepričajte se, da uživajo dober ugled in imajo zanesljivo službo za pomoč strankam.



Prevare z naročninami



NAČINI ZAŠČITE:

Spremljajte bančne izpiske:

Redno preverjajte svoje bančne izpiske in izpiske kreditnih kartic za morebitne nepooblaščne ali sumljive bremenitve.



Nastavite opozorila:

Uporabite opozorila o računu, da vas obvestijo o morebitnih novih bremenitvah ali transakcijah. Na ta način lahko hitro prepoznate in izpodbijate nepooblaščne bremenitve vašega računa.

Poiščite pomoč:

Če se postanete žrtev naročniške prevare, se takoj obrnite na svojo banko ali izdajatelja kreditne kartice in prijavite nepooblaščne bremenitve. Pomagali vam bodo ustaviti nadaljnje stroške in povrniti denar.



Prevare pri ustvarjanju lažnih spletnih trgovin

— ZNAČILNOSTI NEVARNOSTI:

Lažne spletne trgovine so prevarantska spletna mesta, zasnovana tako, da izgledajo kot legitimne spletne trgovine. Goljufi uporabljajo zavajajoče prodajne taktike, da ljudi prepričajo v nakupe. Namesto da bi prejeli naročene izdelke, žrtve pogosto prejmejo ponarejeno blago, izdelke slabe kakovosti ali pa sploh ničesar. Ta vrsta prevare lahko močno prizadene ranljive posameznike, vključno s starejšimi.

Vrste manipulacij v lažnih spletnih trgovinah:

Goljufi privabljajo kupce z neverjetno nizkimi cenami ali velikimi popusti na priljubljene artikle.

Medtem ko so nekatera ponarejena spletna mesta zelo prefinjena, imajo mnoga slabo grafično podobo, nedelujoče povezave ali fotografije nizke kakovosti.

Legitimna podjetja zagotavljajo jasne kontaktne podatke, vključno s pravimi naslovi in telefonskimi številkami za pomoč strankam.

Pomanjkanje resničnih mnenj strank ali samo pretirano pozitivna, splošna in generična mnenja so lahko znak za nevarnost.

Legitimna nakupovalna spletna mesta uporabljajo varne povezave za zaščito vaših podatkov. V naslovni vrstici brskalnika poiščite "https" in ikono ključavnice.

Preveč ugodne cene, da bi bile resnične cene

Slab dizajn spletne strani

Omejeni kontaktni podatki

Brez ocen ali lažne ocene

Brez varne povezave

Prevare pri ustvarjanju lažnih spletnih trgovin

— POSLEDICE:

Prevare v zvezi z lažnimi spletnimi trgovinami lahko povzročijo resne negativne učinke, kot so:

01 Finančna izguba

Če postanete žrtev prevare z lažnimi spletnimi trgovinami, lahko to vodi v izgubo prihrankov. Morda boste ugotovili, da imate precej manj denarja, kot ste pričakovali, kar lahko vpliva na vašo sposobnost pokrivanja vsakodnevnih stroškov in uživanja v pokoju.

02 Čustveni stres

Ko starejši ugotovijo, da so bili prevarani, lahko to povzroči veliko čustveno stisko. Morda se počutijo osramočene, ponižane ali krive, ker so nasedli prevari. Takšen čustveni vpliv lahko vodi v tesnobo, depresijo in zmanjšano zaupanje v spletno nakupovanje ter finančne institucije.

03 Kraja osebnih informacij

Lažne spletne trgovine pogosto zbirajo osebne in finančne podatke med postopkom plačila. Te informacije lahko uporabijo za krajo identitete, kar vodi do nepooblaščenih transakcij, odpiranja novih kreditnih računov na ime žrtve in drugih oblik prevare.

Prevare pri ustvarjanju lažnih spletnih trgovin

— NAČIN ZAŠČITE:



Eva je na družabnih omrežjih videla oglas za vrhunski mešalnik s 75-odstotnim popustom. Navdušena nad ugodno ponudbo je kliknila povezavo in bila preusmerjena na spletno stran, ki je bila videti profesionalno, vendar je ponujala le omejene kontaktne podatke. Za uveljavljanje ugodne cene je spletna stran zahtevala plačilo z bančnim nakazilom. Po plačilu Eva ni nikoli prejela mešalnika, poskusi vzpostavitve stika s službo za pomoč strankam pa niso bili uspešni.

Kaj bi morala Eva storiti, da bi se izognila prevari?



Lažne spletne trgovine so lahko zavajajoče ter lahko povzročijo veliko finančno in čustveno škodo, zlasti starejšim. Z obveščanjem in upoštevanjem spodaj opisanih zaščitnih ukrepov lahko zmanjšate tveganje, da postanete žrtev teh prevar. Pred nakupom si vedno vzemite čas za raziskavo in preverjanje spletnih trgovin, saj si boste le tako zagotovili varno in zanesljivo nakupovalno izkušnjo.

1. KORAK: Raziščite spletno stran

Preverite ocene in poiščite kontaktne podatke trgovine.

2. KORAK: Preverite povezavo

Preverite, ali ima spletno mesto oznako https in ikono ključavnice.

3. KORAK: Bodite skeptični do ponudb

Postavite pod vprašaj popust, ki je preveč dober, da bi bil resničen.

4. KORAK: Uporabite varne načine plačila

Izogibajte se bančnim nakazilom namesto tega uporabite kreditno kartico.

Prevare pri ustvarjanju lažnih spletnih trgovin



NAČINI ZAŠČITE:

Ne pozabite, dragi starejši, da je zaščita pred lažnimi spletnimi trgovinami ključnega pomena za zaščito vašega denarja in čustev. Tukaj je nekaj enostavnih korakov, ki jih lahko naredite.

Raziščite spletno mesto:

Preverite, ali so na spletni strani objavljena mnenja in ocene drugih strank. Za preverjanje legitimnosti trgovine se poslužujte tudi zaupanja vrednih drugih spletnih strani z recenzijami. Poiščite kontaktne podatke trgovine in jo še pred nakupom poskusite kontaktirati.



Preverite povezavo:

Prepričajte se, da spletno mesto uporablja varno povezavo (https in ikona ključavnice). Na spletnih mestih brez varne povezave se izogibajte vnosu osebnih podatkov ali podatkov za plačilo.

Bodite skeptični do ponudb, ki so preveč dobre, da bi bili resnične:

Če se cene zdijo neverjetno nizke ali so ponudbe predobre, da bi bile resnične, verjetno so. Primerjajte cene z drugimi priznanimi trgovci.



Prevare pri ustvarjanju lažnih spletnih trgovin



NAČINI ZAŠČITE:

Uporabite varne načine plačila:

Za spletne nakupe uporabljajte kreditne kartice, saj ponujajo boljšo zaščito pred goljufijami. Izogibajte se uporabi bančnih nakazil, predplačniških kartic ali kriptovalut.



Preverite podrobnosti na spletnem mestu:

Poiščite jasne, podrobne opise izdelkov in profesionalne fotografije. Preverite kontaktne podatke spletnega mesta, vključno s telefonskimi številkami in fizičnimi naslovi.

Seznajte se s pravilnikom o vračilu denarja:

Legitimne trgovine imajo jasna pravila o vračilu denarja. Bodite previdni, če teh informacij ni ali so nejasne.



Prevarantski nakupi prek spletnih oglasov (nakup)



ZNAČILNOSTI NEVARNOSTI:

Spletno prevarantsko oglaševanje je velika grožnja, saj prevaranti izkoriščajo platforme družabnih medijev, priljubljena spletna mesta in celo iskalnike, kot je Google. Lažni oglasi se lahko pojavijo v različnih oblikah, vključno s pojavnimi okni, pasicami, oglasi v družabnih omrežjih in celo v obliki sponzoriranih vsebin. Goljufivi spletni oglasi so zasnovani tako, da nič hudega sluteče uporabnike zavedejo, da kliknejo nanje, kar lahko privede do goljufivih nakupov.

Vrste manipulacij pri nakupih preko spletnih oglasov

Prevaranti običajno uporabljajo promocijski material (logotipe, napise, slogane itd.) znanih blagovnih znamk. Nato začnejo objavljati ciljno usmerjene oglase za prevaro žrtev. Pri tem lahko uporabijo tudi taktike socialnega inženiringa, kot so npr. mamljive ponudbe, s katerimi uporabnike privabijo, da kliknejo na oglase.

Ker so lažni oglasi lahko videti zelo profesionalno in prepričljivo, jih je težko ločiti od legitimnih oglasov. Ko žrtev klikne na oglas, običajno konča v lažni trgovini – kjer lahko pride do phishinga – ali v trgovini, ki prodaja ponaredke. V teh primerih (poleg phishinga) obstaja tudi tveganje, da žrtev izdelka ne bo prejela ali bo prejela izdelek slabše kakovosti od plačanega.

Prevaranti pogosto uporabljajo lažne oglase z vdelano zlonamerno kodo, ki lahko ob kliku okuži naprave uporabnikov. Ta metoda, znana kot "malvertising", je postala razširjena taktika kibernetских kriminalcev za širjenje zlonamerne programske opreme prek lažnih oglasov.

Posnemanje

**Brez
"pravega"
blaga**

**Zlonamerno
oglaševanje**

Prevarantski nakupi prek spletnih oglasov (nakup)



POSLEDICE:

Ne glede na izbrano metodo prevarante, ki se skrivajo za lažnimi oglasi vedno vodi finančni korist.

01 Finančne posledice – neposredna finančna tatvina

Za lažnimi oglasi, ki ponujajo zelo znižane izdelke znanih blagovnih znamk, se pogosto skrivajo trgovine, katerih namen je v fazi oddaje naročila pridobiti plačilne podatke in občutljive informacije. Te informacije se lahko uporabijo za krajo denarja z računov, za izvajanje nadaljnjih kibernetских napadov ali za prodajo drugim kibernetским kriminalcem. V številnih primerih žrtve prejmejo ponarejeno blago ali pa ne prejmejo ničesar.

02 Finančne posledice – stroški izsiljevalske programske opreme

Zaradi ogrožanja sistema in vdora v podatke s pomočjo zlonamerne oglaševanja lahko pride tudi do finančnih posledic. Po kliku na oglas se začne prenašati in nameščati izsiljevalska programska oprema – vrsta zlonamerne programske opreme, ki šifrira vaše datoteke – goljufi pa za njeno odstranitev zahtevajo plačilo. Stroški, povezani s plačilom odkupnine, popravilom sistema in odstranjevanjem zlonamerne programske opreme, so lahko zelo visoki.

03 Kraja identitete

S pomočjo metode lažnega predstavljanja (phishing) se prevaranti izdajo za legitimne blagovne znamke, da bi žrtve pretentali v deljenje osebnih podatkov ali v namestitev vohunske programske opreme (prek metode zlonamerne oglaševanja – malvertising), ki skrivaj zbira občutljive informacije z naprave, kot so prijavni podatki in finančni podatki. To lahko privede do resne kraje identitete, pri kateri se zlorabijo občutljivi podatki žrtev.

Prevarantski nakupi prek spletnih oglasov (nakup)

— NAČINI ZAŠČITE:



Liza, redna uporabnica različnih platform družabnih medijev, je brskala po Facebooku, ko je naletela na spletni oglas, ki je ponujal zelo lep hladilnik.

Oglas je prikazoval sliko vrhunskega hladilnika po izjemno nizki ceni in obljubo hitre dostave. Oglas se ji je zdel predober, da bi bil resničen, vendar je po pomoti kliknila nanj in bila preusmerjena v spletno trgovino, ki se je sprva zdela legitimna ... Vendar je Liza prepoznala opozorilne znake!

Na žalost prevaranta ...

Liza se je udeležila napredne delavnice o prevarah na družabnih omrežjih.



1. KORAK: Preverjanje kakovosti

Po preusmeritvi je Liza takoj opazila, da je spletna stran slabo oblikovana, da ima veliko slovničnih napak in da so fotografije v primerjavi z oglasom slabe kakovosti.

2. KORAK: Tehnični pregled

Liza je opazila, da se URL spletnega mesta ne ujema z imenom blagovne znamke. Namesto tega je bil naslov sestavljen iz naključnih črk in števil.

3. KORAK: Preverjanje verodostojnosti

Ko je Liza pregledala spletno stran, je ugotovila, da na njej ni ključnih kontaktnih podatkov, kot so naslov podjetja, telefonska številka in e-pošta službe za pomoč strankam.

4. KORAK: Preverjanje povratnih informacij

Liza je tudi opazila, da na spletnem mestu ni nobenih ocen strank ali povratnih informacij. Verodostojni spletni trgovci običajno objavljajo ocene in mnenja prejšnjih strank.

Prevarantski nakupi prek spletnih oglasov (nakup)



NAČINI ZAŠČITE:

Pri prevarah z lažnimi oglasi kriminalci ponujajo lažne ali neobstoječe izdelke po ugodnih cenah in izkoriščajo zanimanje starejših za popuste. Prevaranti lahko prevaro podaljšajo z izmišljenimi izgovori za zamude pri dostavi (dodatno plačila), kar še poveča finančno škodo za žrtve.

Tukaj je nekaj dodatnih nasvetov, če se morda znajdete v takšni situaciji.

Da bi se zaščitili pred morebitnimi prevarami, je **najbolj varno, da ignorirate oglase**, še posebej tiste, ki se vam zdijo sumljivi!

Pazite tudi, kje kliknete ali tapnete! Če ste pozorni na to, kje na zaslonu so vaša miška ali prsti, in če upoštevate, po katerem delu strani se pomikate, se lahko izognete nenamernim klikom ali tapom!



Bodite previdni pri klikanju ali tapanju na povezave, tudi na tiste, ki se pojavijo na vrhu rezultatov iskalnika.

Bodite pozorni, da ločite med oglasi in resničnimi rezultati iskanja. Oglasi se običajno prikažejo prvi in so označeni z "Ad" ali "Advertisement".

Zavedajte se tudi, da prevaranti namenoma plačujejo za objave svojih lažnivih oglasov v iskalnikih!



Prevarantski nakupi prek spletnih oglasov (nakup)



NAČINI ZAŠČITE:

Vedno vnesite URL spletne strani neposredno v svoj brskalnik:

Poiščite ikono ključavnice in "https" v brskalniku, da preverite, ali je stran varna, ter preverite URL (z miško se pomaknite nad URL).



Zaščitite svoj računalnik:

Pomembno je, da v računalnik namestite in redno posodabljate protivirusno in varnostno programsko opremo. Tako bo vaš računalnik zaščiten pred različnimi vrstami groženj, kot so virusi, hekerski napadi in zlonamerna programska oprema.

V spletnih brskalnikih omogočite funkcijo blokiranja pojavnih oken!

Prevarantski nakupi preko spletnih oglasnikov (prodaja)



NAČINI ZAŠČITE:

Lažni spletni prodajalci/prevaranti običajno zahtevajo plačilo z nezanesljivimi metodami, kot so bančna nakazila (saj v primerjavi z drugimi plačilnimi metodami, kot so kreditne kartice, nudijo manj zaščite v primeru prevare) ali prek neznanih plačilnih platform.

Nikoli ne opravite plačila na tak način! Prav tako nikoli ne razkrivate svojih finančnih ali drugih občutljivih podatkov!

Če se ujamete v prevaro, poskusite zbrati čim več dokazov in jo nemudoma prijavite ustreznemu organu!



REPORT

Prijavite! Večina platform ima vzpostavljene mehanizme za prijavo takšnih težav.

Uporabite funkcijo za prijavo v platformi, ki je običajno dostopna prek gumba "Prijavi" v oglasu ali uporabniškem profilu.

Počakajte na navodila podporne ekipe platforme in po prijavi prekinite vse interakcije z osumljenim posameznikom.

Prevarantski nakupi preko spletnih oglasnikov (prodaja)



ZNAČILNOSTI NEVARNOSTI:

Spletne tržnice so lahko odličen način za dodaten zaslužek starejših, saj lahko prodajajo svoje ročno izdelane umetnine, starine, nepotrebne gospodinjske predmete itd. Tako lahko zaslužijo dodaten denar, ki ga lahko uporabijo za izboljšanje življenjskega standarda ali za posebne priložnosti. Starejši morajo biti pri prodaji še posebej previdni, saj se na teh tržnicah pojavljajo tudi prevaranti, ki se izdajajo za potencialne kupce.

Vrste manipulacije pri prevarah preko spletnih oglasnikov (prodaja):

Prevaranti so pripravljeni "kupiti" predmet, ne da bi ga videli, in pogosto uporabljajo različne izgovore, kot so bolezen, medeni tedni, potovanje v tujino itd. Z žrtvami stopijo v stik samo prek SMS sporočil ali elektronske pošte in se izogibajo telefonskim ali video klicem. Pogosto zahtevajo, da se predmet pošlje njihovemu "posredniku", ali pa se za prevzem dogovorijo s kurirjem. Vsi ti načini komunikacije goljufom omogočajo, da prikrijejo svojo identiteto.

Prevaranti zahtevajo, da bodo plačali izključno s čekom, denarnim nakazilom, bančnim nakazilom, mednarodnim prenosom sredstev, aplikacijami za mobilno plačevanje itd., pošiljajo lažne potrditve plačila in upajo, da bodo žrtve poslale izdelek, preden bodo ugotovile, da gre za prevaro. Pri tem lahko uporabijo "izgovore", na primer, da je prišlo do težav s poslanim plačilom, od žrtev lahko zahtevajo vnaprejšnje plačilo stroškov transporta ali pošiljanja in jim obljubijo povračilo stroškov itd.

Prevaranti žrtvam običajno ponudijo več denarja od izklicne cene. Razlogi so različni - lahko zahtevajo nadomestilo za "težave" žrtve, kritje domnevnih stroškov pošiljanja ali pa se pretvarjajo, da so se zmotili pri znesku plačila. Ko pa žrtve prejmejo preplačilo, bodo prevaranti zahtevali presežna sredstva nazaj.

**Brez
osebne
stika**

Brez gotovine

Preplačilo

Prevarantski nakupi preko spletnih oglasnikov (prodaja)

— POSLEDICE:

Žrtve prevar s “kupci” na spletnih oglasnikih lahko doživijo naslednje negativne posledice:

01 Finančne posledice

Žrtve se lahko soočijo s finančnimi posledicami, kot je denarna izguba vrednosti artiklov, če so jih poslali, ne da bi prejeli plačilo. Če je prišlo do preplačila in so žrtve vrnile denar, bodo verjetno ugotovile, da je bilo prvotno plačilo lažno – ček ali pa kupčevo spletno plačilo bosta namreč zavrnjena – v tem primeru so žrtve izgubile „vrnjeni“ denar in denarno vrednost artiklov.

02 Čustvene posledice

Pri žrtvi se lahko pojavijo številni simptomi, vključno z negativnimi mislimi o sebi. Žrtve lahko mislijo, da niso dovolj inteligentne ali da je z njihovo sposobnostjo presojanja drugih nekaj narobe. Pogosto krivijo sebe, saj menijo, da so bile preveč zaupljive, in se počutijo jezne, žalostne, izdane, nemočne in v zadregi.

03 Pravne posledice

Če se je žrtev strinjala s plačilom s čekom in ga sprejela, vendar je bil ček ponarejen, bo nič hudega sluteča žrtev pravno odgovorna za poskus unovčenja nezakonitega čeka, ko bo banka odkrila ponaredek. Poleg tega se lahko žrtev sooči s težavami pri nadaljnjem finančnem poslovanju.

Prevarantski nakupi preko spletnih oglasnikov (prodaja)



NAČINI ZAŠČITE:



Leon je na Facebookovi tržnici objavil oglas za rabljeno kolo za 200 evrov in takoj prejel sporočilo "Tima", ki ga je želel kupiti brez pogajanj o ceni in ponudil celo 30 evrov več za poštnino. Leonu se je zdelo nenavadno, da si Tim izdelka ni želel osebno ogledati, čeprav živi v istem mestu. Tim je želel izdelek plačati tudi prek sistema PayPal ter zahteval Leonovo številko socialnega zavarovanja in domači naslov. Takrat se je Leon v naglici umaknil!

Na žalost prevaranta ...

Leon je spremljal kampanjo ozaveščanja v skupnosti uporabnikov in se poučil o pogostih poskusih tovrstnih prevar ter preventivnih ukrepih.



1. KORAK: Prepoznavanje sumljivega vedenja

Leonu se je zdelo čudno, da si Tim ni želel osebno ogledati kolesa, čeprav živi v istem mestu. To je bil prvi opozorilni znak, saj si pravi kupci običajno ogledajo artikle pred nakupom.

2. KORAK: Raziskovanje

Leon je raziskal Timov profil in našel sumljive kontaktne podatke in nedosledno komunikacijo. Leon je blokiral Tima in takoj prekinil vso komunikacijo ter tako preprečil nadaljnja tveganja.

3. KORAK: Zaščita

Tim je želel plačati prek PayPal, kar samo po sebi ni sumljivo, zahteval pa je tudi Leonovo številko socialnega zavarovanja in domači naslov, kar je zelo nenavadno in nepotrebno. Leon se je zavestno odločil, da teh informacij ne bo delil.

4. KORAK: Informiranje/prijava

Leon je svojo izkušnjo delil s skupnostjo in na platformi prijavil Timov profil. S tem je pripomogel k ozaveščanju in zaščiti tudi drugih uporabnikov.

Prevarantski nakupi preko spletnih oglasnikov (prodaja)



NAČINI ZAŠČITE:

Če oglašujete svoje artikle za prodajo prek spletnih portalov za male oglase, je tukaj nekaj preprostih korakov, s katerimi se lahko opolnomočite in zaščitite pred goljufi, ki se pretvarjajo, da so potencialni kupci.

Bodite previdni, če vam nekdo ponudi več, kot je vaša izklicna cena (razen če prodajate predmet z več konkurenčnimi ponudbami). Ne sodelujte z nikomer, ki vam ponudi plačilo v višjem znesku in pričakuje, da boste presežek poslali nazaj.

Takšno plačilo takoj zavrnite in vztrajajte pri prejemu pravilnega zneska v novi transakciji.



Zahtevajte plačilo v gotovini:

Če to ni mogoče, **ne pošiljajte artikla, preden prejmete plačilo, in se prepričajte, da je plačilo legalno in zakonito.**

Če pošljete artikel, preden vam zanj plačajo, nimate nobene možnosti, da ga boste dobili nazaj!

Prevaranski nakupi preko spletnih oglasnikov (prodaja)



NAČINI ZAŠČITE:

Ne zaupajte potrditvam plačil po e-pošti – lahko so lažne! Neposredno preverite svoj bančni račun in preverite, ali je bilo plačilo prejeto.

Da bi se izognili morebitnim prevaram, je najbolje, da **poslujete z lokalnimi kupci**, s katerimi se lahko osebno srečate, in da sprejemate le gotovino. **Ne plačujte nobenih navideznih stroškov pošiljanja ali pristojbin.** Posebno previdnost svetujemo pri prodaji kupcem v tujini.



Ignorirajte vse zahteve po posredovanju nepotrebnih informacij. Navedite le podatke, ki so nujno potrebni za dokončanje transakcije.

Če prodajate artikel, **ne klikajte na nobeno povezavo, ki vam jo pošlje kupec in kupcu ne posredujte nobenih podatkov, ki bi mu lahko omogočili dostop do katerega koli vašega bančnega računa.**

Prijavite! Večina platform ima vzpostavljene mehanizme prijavo za reševanje takšnih težav.

Uporabite funkcijo poročanja na platformi, ki je običajno dostopna prek gumba **“Prijavi”** v oglasu ali uporabniškem profilu.

Počakajte na navodila skupine za podporo platforme in po prijavi prekinite vse interakcije z osumljeno osebo.



Dodatno branje



PREVARE PRI POTOVANJIH IN NAKUPU VOZOVNIC

- <https://www.comparitech.com/blog/information-security/avoid-common-ticket-and-travel-scams-online/> <https://www.aura.com/learn/airline-scams>
- <https://www.interpol.int/en/Crimes/Financial-crime/Airline-ticket-fraud>
- <https://www.nyccriminallawyer.com/ticket-scams/>
- <https://www.chargebackgurus.com/blog/travel-agency-chargebacks>
- <https://chargebacks911.com/otas-lose-billions-every-year-to-travel-fraud/>
- <https://www.traveldailynews.com/post/how-fraudsters-exploit-travel-agencies>
- <https://www.consumerreports.org/travel/avoiding-travel-scams/>
- <https://www.bbb.org/all/travel-scams>
- <https://www.consumer.ftc.gov/articles/travel-scams>



PREVARE Z NAROČNINAMI

- <https://balkaninsight.com/2023/08/22/subscription-scams-the-mobile-users-paying-for-unwanted-services/>
- https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/coordinated-actions/consumer-frequent-traps-and-scams_en
- <https://www.evz.de/en/shopping-internet/internet-fraud/subscription-traps.html>
- <https://www.europe-consommateurs.eu/en/shopping-internet/internet-fraud-and-scams/subscription-traps.html>
- <https://www.flagright.com/post/understanding-subscription-fraud>
- <https://www.which.co.uk/news/article/5-subscription-scams-and-traps-to-watch-out-for-aYwJA0u8EFZ9>

Dodatno branje



PREVARE PRI USTVARJANJU LAŽNIH SPLETNIH TRGOVIN

- <https://www.statista.com/statistics/1182221/online-shopping-fraud-incidents-uk/>
- <https://www.northyorkshire.police.uk/news/north-yorkshire/news/news/2024/04-april/online-shopping-fraud/>
- <https://us.norton.com/blog/online-scams/fake-e-shops>
- <https://www.youtube.com/watch?v=ItI7DXrNQCA>
- https://www.youtube.com/watch?v=CQYmfcLW_oc



PREVARANTSKI NAKUPI PREKO SPLETNIH OGLASOV (NAKUP)

- <https://www.rd.com/list/fake-ads-on-social-media/>
- <https://www.seniorlifestyle.com/resources/blog/protect-your-parents-from-common-digital-traps/>
- <https://www.takefive-stopfraud.org.uk/advice/general-advice/purchase-fraud/> primeri <https://bolster.ai/glossary/fake-ads>
- <https://www.investigatetv.com/2023/11/14/how-determine-if-social-media-ads-are-real-or-fake/>
- https://thegratifiedblog.com/social-media-marketing/how-to-spot-fake-ads-on-facebook/#What_Are_Fake_Ads
- <https://trafficwatchdog.pl/en/articles/85/ad-frauds-in-social-media>
- https://www.tracit.org/uploads/1/0/2/2/102238034/tracit_fraudulentadvertising_online_execsummary_july2020_final.pdf
- https://commission.europa.eu/system/files/2020-01/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf

Dodatno branje



PREVARANTSKI NAKUPI PREKO SPLETNIH OGLASNIKOV (PRODAJA)

- <https://www.westpac.com.au/security/types-of-scams/online-shopping-scams/>
- <https://www.ccpc.ie/consumers/money/scams/social-media-scams/>
- <https://www.desjardins.com/qc/en/tips/spot-avoid-scams-online-classifieds.html> <https://www.obvy-app.com/en/magazine/individuals/avoid-scams/scam-sites-small-ads/2341>
- <https://www.interbank.com/fraud-protection/beware-of-online-scams-how-to-spot-fake-listings-on-social-media-sale-groups/>
- <https://www.dropzone.com/help/classifieds/classifieds-buyer-scams-r23/>
- <https://www.nab.com.au/about-us/security/online-safety-tips/buying-selling-scams>
- <https://fastercapital.com/content/Classified-ads-site--Safety-Measures-When-Using-Classified-Ad-Websites.html>
- <https://consumer.ftc.gov/consumer-alerts/2022/07/selling-stuff-online-heres-how-avoid-scam>

5. POGLAVJE

MANIPULACIJA IDENTITETE IN IZKORIŠČANJE JAVNEGA ZAUPANJA

Novodobne prevare vse bolj temeljijo na manipulaciji z identiteto in izkoriščanju zaupanja v javne institucije, kar starejše postavlja v še posebej ranljiv položaj. Kriminalci se ne le izdajajo za zaupanja vredne institucije, temveč za doseg svojih ciljev uporabljajo tudi najsodobnejšo tehnologijo. V tem poglavju bomo obravnavali najpogostejše prevare, ki temeljijo na zlorabi identitete in zaupanja, da bi starejšim pomagali prepoznati in se izogniti tem grožnjam.

Resne grožnje za starejše vključujejo lažne obtožbe za kazniva dejanja, v katerih prevaranti lažno obtožijo starejše z namenom, da bi od njih izsiljevali denar ali informacije. Lažno izdajanje za vladne institucije je še ena nevarna metoda, pri kateri se kriminalci predstavljajo kot predstavniki oblasti, da bi pridobili osebne podatke ali denar. Tehnologija globokih ponaredkov (deepfake) omogoča ustvarjanje lažnih, a prepričljivih posnetkov, kar lahko vodi v resne posledice. Storitvene prevare, povezane z lažnim izdajanjem za vladne institucije, pogosto vključujejo lažne ponudbe namenjene izsiljevanju denarja. Lažni računi se uporabljajo za izsiljevanje starejših z grožnjo, da bodo razkrili neresnične informacije.

Razumevanje teh groženj in njihovih mehanizmov je ključno za učinkovito zaščito identitete, financ in zaupanja v javne institucije. V tem poglavju bomo podrobno razpravljali o teh vprašanjih, da bi vam pomagali prepoznati in se izogniti takšnim prevaram.

Obtožbe o vpletenosti v kazniva dejanja

— ZNAČILNOSTI NEVARNOSTI:

Gre za prevaro, pri kateri goljufi od uporabnika izsilijo denar, tako da se izdajajo za sodnika, policista ali tožilca, in trdijo, da je njegovo ime povezano s terorizmom. "Obtožbe o vpletenosti v kaznivo dejanje" se nanašajo na trditve ali obtožbe, da je posameznik, organizacija ali celo starejša oseba sodelovala v nezakonitih dejavnostih. Te obtožbe še niso dokazane in zahtevajo preiskavo, da bi se ugotovila njihova resničnost. Vrsta kaznivega dejanja, ki se žrtvam očita je lahko zelo različna, lahko gre za goljufijo, krajo ali različna druga nezakonita dejanja. Takšne obtožbe imajo lahko resne pravne in socialne posledice za obtožence, vključno s starejšimi. Starejši so še posebej ranljivi za takšne obtožbe zaradi morebitnega pomanjkanja poznavanja digitalne tehnologije in prevarantskih taktik.

Vrste obtožb o vpletenosti v kazniva dejanja:

Obtožbe, da je bančni račun žrtve povezan s transakcijami, ki financirajo teroristične dejavnosti, so vrsta prevare, katere cilj je prestrašiti žrtev in jo spraviti v paniko. V tem primeru goljuf poudarja resnost obtožbe in običajno zahteva takojšnje ukrepanje, kot je plačilo "globe" ali "pristojbine". Med interakcijo goljuf uporablja psihološke manipulacijske taktike, da bi žrtev spravil v paniko in jo z manipulacijo prisilil, da mu posreduje svoje osebne podatke in/ali denar. Prav tako lahko žrtev opozori, naj ne kontaktira nikogar in naj ohrani zadevo v tajnosti.

V tem prevarantskem scenariju goljuf stopi v stik z žrtvijo in se predstavi kot uradna oseba, ter trdi, da je predstavnik organa pregona ali pravosodnega sistema. Žrtev opozori, da je njeno ime na seznamu oseb, povezanih z znano teroristično organizacijo in navede izmišljene podrobnosti, da žrtev prestraši in spravi v paniko. Nato zahteva, da žrtev takoj ukrepa, pri čemer uporablja grožnje ali zastrašujoč govor, da bi ohranil nadzor nad situacijo.

V tem prevarantskem scenariju pa goljuf stopi v stik z žrtvijo in se predstavlja kot policist, sodnik ali tožilec. Žrtev obvesti, da je njihova zgodovina potovanja ali nekatere dejavnosti vzbudile sum. Goljuf lahko celo omeni določena mesta, ki jih je žrtev dejansko obiskala, da bi prevara delovala bolj verodostojno. Doda lahko tudi podrobnosti, kot so datumi potovanja ali imena domnevnih teroristov, s katerimi naj bi bila žrtev v stiku. Tako kot v drugih primerih goljufi pritiskajo na žrtev, da sprejme hitre odločitve ter uporabljajo manipulativne taktike, da pridobijo osebne podatke.

Vpletenost v mrežo za financiranje terorizma

Povezava z znanimi terorističnimi organizacijami

Sumljiva zgodovina potovanja ali aktivnosti

Obtožbe o vpletenosti v kazniva dejanja



POSLEDICE:

Lažne vpletenosti v kaznivo dejanje imajo lahko resne negativne posledice, kot so:

01 Oškodovanje ugleda

Povezovanje s kaznivim dejanjem, tudi če obtožbe niso dokazane, lahko resno prizadene ugled osebe in lahko vpliva na osebne odnose in poklicne priložnosti.

02 Pravne posledice

Če obtožbe vodijo do kazenske preiskave in je oseba spoznana za krivo, se lahko sooči s pravnimi posledicami. Te lahko vključujejo denarne kazni, pogojne ali celo zaporne kazni.

03 Čustvena stiska

Obtožba kaznivega dejanja lahko povzroči veliko čustveno stisko. Oseba lahko občuti strah, sram ali zadrego, ta čustva pa lahko dolgoročno vplivajo na njeno psihološko počutje.

Obtožbe o vpletenosti v kazniva dejanja



POSLEDICE:

04 Kraja identitete in njena uporaba za nadaljnja kazniva dejanja

Obtožbe, povezane s krajo identitete, lahko vodijo do nadaljnjih kaznivih dejanj, ki se izvajajo v imenu žrtve, kar še poslabša pravne in osebne posledice.

05 Izguba denarnih sredstev

Žrtve obtožb kaznivih dejanj, zlasti tistih, ki vključujejo finančne goljufije, lahko utrpijo znatne finančne izgube, bodisi neposredno zaradi kraje bodisi posredno zaradi pravnih stroškov in drugih stroškov, povezanih z obrambo.

06 Okužba naprav z virusi

V zadevah, ki vključujejo obtožbe o kibernetiski kriminaliteti, obstaja tveganje, da bodo naprave obdolženca tarča in okužene z virusi ali zlonamerno programsko opremo, kar bo povzročilo vdore v podatke in nadaljnje zaplete.

Obtožbe o vpletenosti v kazniva dejanja

— NAČINI ZAŠČITE:



Nekega dne je Rozi prejela elektronsko sporočilo, ki jo je obvestilo, da je njeno ime vključeno v odmevno kriminalistično preiskavo, povezano z goljufivimi spletnimi transakcijami. Elektronsko sporočilo je izgledalo, kot da prihaja z lokalne policijske postaje in je bilo zelo podrobno, kar je v Rozi povzročilo občutek nujnosti in strahu.

V sporočilu je bilo tudi zapisano, da naj Rozi klikne na povezavo in vnese svoje osebne podatke, vključno s številko socialne varnosti in podatki o bančnem računu, domnevno za potrditev svoje identitete in izločitev svojega imena iz preiskave. Prestrašena zaradi obtožb in obupana, da bi čim prej rešila težavo, je Rozi sledila navodilom.

Nekaj dni kasneje je prejela klic iz svoje banke, ki jo je obvestila o sumljivih aktivnostih na njenem računu. Takrat je Rozi spoznala, da jo je goljuf prevaral, s tem ko je uporabil obtožbe o vpletenosti v kaznivo dejanje kot zvijačo.

Ta zgodba poudarja, kako pomembno je starejše poučiti o tveganjih in taktikah spletnih prevar. Kot se je pokazalo v Rozinem primeru, lahko goljufi izkoriščajo nepoznavanje digitalnega sveta in s taktiko ustrahovanja izsilijo od starejših, da jim posredujejo občutljive osebne podatke. Z izobraževanjem starejših o teh grožnjah in učenjem, kako preveriti verodostojnost takšnih zahtev, jih lahko zaščitimo, da ne postanejo žrtve tovrstnih prevar.



1. KORAK: Preverite

Če Rozi prejme nepričakovano e-pošto, zlasti od domnevnega vladnega organa ali organov pregona, naj ne odgovarja direktno. Uradne kontaktne podatke mora poiskati sama in jih preveriti.

2. KORAK: Zaščitite osebne podatke

Rozi ne sme deliti občutljivih podatkov, kot je številka socialnega zavarovanja ali bančni podatki, prek e-pošte. Verodostojne organizacije posredovanja teh podatkov ne zahtevajo po elektronski pošti.

3. KORAK: Nadzorujte račune

Rozi bi morala redno preverjati svoje finančne in spletne račune glede sumljivih aktivnosti, da bi pravočasno in dovolj zgodaj odkrila prevaro in zavarovala svoje račune.

4. KORAK: Uporabite varnostno programsko opremo

Namestitev in posodabljanje varnostne programske opreme lahko Rozi zaščiti pred spletnimi grožnjami, kot so virusi, zlonamerna programska oprema in phishing. Programska oprema lahko zazna nevarnosti in blokira sumljiva spletna mesta.

Obtožbe o vpletenosti v kazniva dejanja



NAČINI ZAŠČITE:

Starejši se morajo zaščititi pred obtožbami o kaznivih dejanjih, ki lahko škodijo njihovem ugledu, povzročijo pravne težave in čustvene stiske. Starejši so pogosto tarča prevar zaradi nepoznavanja digitalne tehnologije, zaradi česar so še bolj ranljivi za morebitne prevare. S preventivnimi ukrepi lahko zaščitite njihove finance, osebne podatke in njihovo dobrobit.

Preverjanje nepričakovanih zahtev:

Vedno bodite pozorni, kadar prejmete nepričakovana e-poštna sporočila ali drugo korespondenco, zlasti od vira, ki se predstavlja kot vladni organ, organ pregona ali kot storitveno podjetje, katerega storitve uporabljate. Namesto da se neposredno odzovete na e-poštno sporočilo ali kliknete na kakršne koli povezave, neodvisno poiščite uradne kontaktne podatke organizacije in se obrnite nanjo za preverjanje. Tako boste lahko potrdili, ali je zahteva zakonita ali gre za morebitno prevaro.



Bodite previdni pri posredovanju osebnih podatkov:

Vaši osebni podatki so dragoceni in jih je treba za vsako ceno zaščititi. Nikoli ne posredujte občutljivih osebnih podatkov, kot so številka socialnega zavarovanja, podatki o bančnem računu ali drugi osebni podatki, na zahtevo po e-pošti ali od nepreverjenega vira. Verodostojne organizacije običajno ne zahtevajo tovrstnih podatkov prek e-pošte.



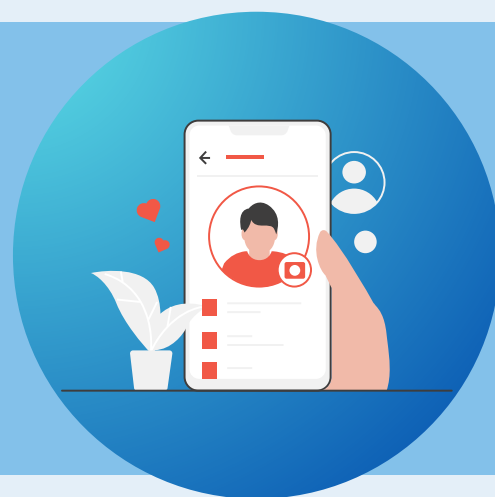
Obtožbe o vpletenosti v kazniva dejanja



NAČINI ZAŠČITE:

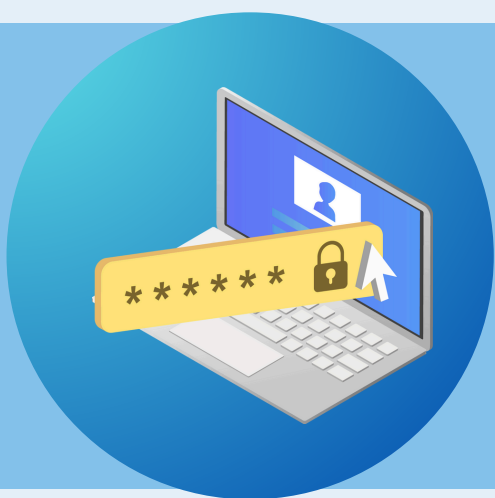
Redno spremljajte vaše račune:

Redno spremljanje finančnih in spletnih računov vam lahko pomaga pri zgodnjem odkrivanju morebitnih sumljivih aktivnosti. To je ključnega pomena za preprečitev nadaljnje škode, saj lahko aktivnost takoj prijavite ustreznim organom ali ponudniku storitev in sprejmete ukrepe za zavarovanje računa.



Uporabite varna in unikatna gesla:

Uporaba močnih in unikatnih gesel za vse spletne račune je ključen varnostni ukrep. Močno geslo vsebuje mešanico črk, števil in simbolov ter ga ni mogoče zlahka uganiti. Ne uporabljajte istega gesla za več računov. V primeru kompromitiranja enega računa ostanejo drugi računi varni.



Namestite varnostno programsko opremo:

Namestitev in redno posodabljanje varnostne programske opreme v računalnik sta prva obrambna linija pred številnimi spletnimi grožnjami. Mednje sodijo virusi, zlonamerna programska oprema, izsiljevalska programska oprema in poskusi phishinga. Programska oprema lahko pregleda vaš sistem za grožnje, blokira sumljive spletne strani in nudi zaščito v realnem času pred napadi zlonamerne programske opreme.



Manipulacije pri prevarah z lažnim predstavljanjem javnih institucij



ZNAČILNOSTI NEVARNOSTI:

Izdajanje za javne uslužbenke je vrsta prevare, pri kateri se goljufi izdajajo za uslužbenke različnih vladnih služb, kot so davčni organi, policija ali pokojninski skladi. Te prevare predstavljajo veliko grožnjo za varnost osebnih podatkov in finančno varnost posameznikov. Za prevaro svojih žrtev prevaranti uporabljajo različne taktike, vendar obstajajo nekateri skupni znaki, na katere je potrebno biti pozoren.

Vrste manipulacij pri prevarah z lažnim predstavljanjem javnih institucij:

Prevaranti žrtve običajno nepričakovano kontaktirajo po telefonu, elektronski pošti, SMS sporočilih ali celo prek spletnih oglasov. Njihov osnovni cilj je žrtve prepričati, da začnejo komunicirati z njimi. Običajno razpolagajo z osnovnimi osebnimi podatki o žrtvi, ki jo nameravajo ogoljufati, da se zdijo verodostojni. Ko je stik enkrat vzpostavljen, prevaranti od žrtve zahtevajo posredovanje občutljivih podatkov, plačilo "kazni" (prek neobičajnih plačilnih metod), ali da izvedejo druga dejanja.

V pogovorih z žrtvami goljufi podajajo veliko lažnih informacij o sebi, svojih nalogah in uporabljajo uradno zveneče izraze, s katerimi lažno nakazujejo povezavo z vladnimi organi. V komunikaciji po pošti ali prek spleta uporabljajo na videz uradne vladne žige, logotipe, imena dejanskih uradnikov na položajih, lažne spletne strani in e-poštne domene, z namenom, da žrtve preslepijo da jim zaupajo. Elektronska sporočila pogosto vsebujejo tudi priponko, (običajno datoteko PDF), in opozorilo, da je treba prebrati priložene dokumente.

Da bi izsilili takojšen odziv žrtev, se goljufi poslužujejo ustrahovanja in časovnih rokov ter grozijo s pravnimi ukrepi ali denarnimi kaznimi. V elektronskem sporočilu, ki naj bi bilo od policije, lahko na primer grozijo z uvedbo kazenskega postopka, če se žrtev ne bo odzvala v določenem roku. Te taktike lahko povzročijo paniko in poslabšajo presojo, zaradi česar se tudi običajno razumni posamezniki odzovejo iz strahu.

Neželena komunikacija

Pretvarjanje, da so zaupanja vredni

Grožnje in nujnost

Manipulacije pri prevarah z lažnim predstavljanjem javnih institucij



POSLEDICE:

Tovrstne prevare dobesedno temeljijo na dejstvu, da so starejši ljudje odlične potencialne žrtve, saj starejše generacije pogosto bolj zaupajo vladnim ustanovam in so bolj navajene spoštovati avtoritete in institucije. Poleg tega imajo prihranke in verjetno prejemajo katero od oblik državnih podpor ali ugodnosti.

01 Finančne posledice

Žrtve izgubijo denar, ki ga prevarantom nakažejo kot plačilo za reševanje fiktivnih davčnih, pravnih ali drugih obveznosti. Poleg izgubljenega denarja lahko žrtve utrpijo tudi dodatne stroške za razreševanje situacije. Če prevaranti pridobijo dostop do njihovega bančnega računa, lahko to povzroči nadaljnje finančne izgube zaradi nepooblaščenih nakupov. V najslabšem primeru lahko račun izprazniijo, kar povzroči nepopravljivo škodo, zlasti starejšim, ki so morda izgubili svoje težko prislužene prihranke.

Manipulacije pri prevarah z lažnim predstavljanjem javnih institucij

02 Kraja identitete

Če žrtev izgubi občutljive osebne podatke, lahko to povzroči nadaljnjo finančno izgubo, saj lahko prevaranti uporabijo podatke iz potnega lista ali osebne izkaznice za odprtje novih bančnih računov in najemanje posojil v imenu žrtve brez njihove vednosti. V primeru kraje zdravstvene identitete lahko žrtev izgubi zdravstvene ugodnosti, pri kraji davčne identitete pa lahko ostane brez vračila davka. Kraja identitete je travmatična izkušnja in ima številne druge posledice, na primer kriminalci uporabijo identiteto žrtve za kazniva dejanja (vključno s kibernetскими kaznivimi dejanji), zaradi česar se lahko žrtev sooči s pravnimi posledicami za dejanja, ki jih ni storila.

03 Izguba zaupanja v javne institucije

Tovrstne prevare lahko pomembno vplivajo na zaupanje posameznikov v javne institucije, saj lahko žrtve občutijo globok občutek izdaje in izgube zaupanja v te institucije. To lahko povzroči, da postanejo skeptični do pristne komunikacije in manj pripravljeni sodelovati, saj lahko začnejo dvomiti o legitimnih zahtevah in informacijah, kar vodi v pomanjkanje pripravljenosti za sodelovanje z vladnimi institucijami. Povečana zaskrbljenost glede možnosti goljufij lahko vpliva tudi na javno mnenje in zmanjša zaupanje v sposobnost državnih organov, da učinkovito ščitijo državljane in jim služijo.

Manipulacije pri prevarah z lažnim predstavljanjem javnih institucij

— NAČIN ZAŠČITE:



Simona je poklicala oseba, ki se je v uradnem tonu predstavila kot uslužbenka davčne uprave. Povedala mu je, da dolguje zaostale davke in da bo aretiran in odpeljan v zapor, če ne bo takoj poravnal dolga s plačilom v eni od kriptovalut. Kljub temu da je bila klicateljica vztrajna in zastrašujoča, je Simon odložil slušalko.

Kmalu po koncu klica je prejel še SMS sporočilo z enako vsebino kot v pogovoru, ki je vključevalo tudi sumljivo povezavo do spletnega mesta davčnega organa.

Na žalost prevaranta ...

Simon se je udeležil izobraževalnega predavanja o prevarah z lažnim predstavljanjem, ki ga je organizirala davčna uprava.



1. KORAK: Prepoznavanje opozorilnih znakov

Simon je bil sprva prestrašen, a je prepoznal znake prevare, ko je klicatelja omenila plačilo neporavnanih davčnih obveznosti s kriptovaluto, kar ni standardni način plačevanja davka.

2. KORAK: Prepoznavanje nenavadnega vedenja

Ker je klicatelj grozil z aretacijo in zaporom, je Simon podvomil v zakonitost takšnih groženj in takoj prekinil klic.

3. KORAK: Preverjanje

Simon je takoj preveril, ali je telefonska številka povezana z pristojnim davčnim organom, in ugotovil, da ni. Sumljiva domena v sporočilu je samo potrdila njegove sume, zato je številko blokiral.

4. KORAK: Prijava

Simon je prek njihove službene telefonske številke kontaktiral uradni davčni organ in jih obvestil o poskusu prevare.

Manipulacije pri prevarah z lažnim predstavljanjem javnih institucij



NAČINI ZAŠČITE:

Tukaj je nekaj dodatnih nasvetov, če se morda znajdete v takšni situaciji.

Odložite slušalko, izbrišite, ne odgovarjajte:

Ne upoštevajte klicev, e-poštnih sporočil, SMS sporočil in sporočil v družabnih medijih, ki trdijo, da prihajajo iz državnih institucij, in od vas zahtevajo plačilo, potrditev občutljivih podatkov ali posredovanje drugih informacij.

Prava vladna institucija vas nikoli ne bo poklicala, poslala e-pošte, sporočila ali sporočila na družabnih omrežjih in od vas zahtevala denar ali podatke.



Ne vzdržujte stikov z goljufi in jim ne posredujte svojih osebnih podatkov ali izvajajte kakršnih koli plačil!

Legitimne institucije se držijo določenih postopkov in pravil glede plačil, finančnih obveznosti ter drugih administrativnih zadev in od vas nikoli ne bodo zahtevale plačila s plačilnimi metodami, kot so kriptovalute, denarne nakaznice, plačilne platforme itd.

Manipulacije pri lažnem predstavljanju državnih institucij



NAČINI ZAŠČITE:

Ne zaupajte kontaktnim podatkom v e-poštnih sporočilih in sporočilih SMS!

Preden se odzovete na korespondenco, ki naj bi prihajala od vladne institucije, se prepričajte, da ste neodvisno potrdili identiteto pošiljatelja.

Za zagotovitev legitimnosti sporočila poiščite uradne kontaktne podatke ustrezne agencije in stopite v neposreden stik z njo!



Takoj prekinite stike z vsemi, ki vam grozijo ali vas ustrahujejo!

Grožnje in ustrahovanje lahko povzročijo čustveno stisko in psihološko trpljenje.

Ne pozabite!

Zakonite državne institucije ne uporabljajo groženj z aretacijo ali zaporom, da bi dosegle plačilo davčnih obveznosti ali drugih dolgov.

Če ste postali žrtev prevare in ste prenesli denar, šele pozneje pa ugotovili, da je šlo za goljufijo, se takoj obrnite na banko in vložite pritožbo. Skodo prijavite tudi policiji.

Če so bili med goljufijo razkriti tudi drugi osebni podatki, o tem nemudoma obvestite ustrezno institucijo, ki so jo prevaranti uporabili za svoje goljufive namene.



REPORT

Manipulacija s tehnologijo deepfake

— ZNAČILNOSTI NEVARNOSTI:

Deepfake prevara je vrsta goljufije, pri kateri se umetna inteligenca uporablja za ustvarjanje ali spreminjanje videoposnetkov, zvočnih posnetkov ali fotografij z namenom zavajanja. To pogosto vključuje ustvarjanje sintetične vsebine posameznika, posnemanje njegovega glasu, obrazne mimike in manir, da bi bilo videti, kot da počne ali govori nekaj, česar ni naredil ali rekel. Ti lažni videoposnetki, zvočni posnetki ali fotografije se pogosto uporabljajo za prevaro žrtev z namenom, da bi od njih izsilili denar, da bi žrtve razkrile občutljive informacije ali pa da bi preprosto škodovali njihovem ugledu. Zlasti starejši so pogosto tarča žrtev teh prevar zaradi njihove domnevne ranljivosti in nepoznavanja tako izpopolnjenih tehnoloških groženj. Te prevare se lahko uporabljajo tudi za izsiljevanje, širjenje lažnih informacij ali za vdor v varnostne sisteme. Zaradi velikega čustvenega in finančnega vpliva na starejše je ključnega pomena, da jih ozaveščamo in izobražujemo o tem, kako prepoznati in se zaščititi pred takšnimi prevarami.

Vrste deepfake prevare:j

Ta vrsta deepfake prevare vključuje ustvarjanje sintetičnega videoposnetka, ki posnema določeno osebo. S tem videoposnetkom lahko goljuf žrtve zavede, da so prepričane, da komunicirajo s pravo osebo, kar lahko privede do finančne izgube ali kraje osebnih podatkov.

Pri tej vrsti prevare se deepfake tehnologija uporabljajo za širjenje dezinformacij ali propagande. To lahko vključuje ustvarjanje videoposnetkov o javnih osebah, ki govorijo ali delajo stvari, ki jih niso nikoli storile, s čimer zavajajo javnost in vplivajo na mnenja ali dejanja.

Deepfake tehnologija se lahko uporabljajo tudi za vdor v varnostne sisteme, ki temeljijo na tehnologiji prepoznavanja obraza. Z ustvarjanjem sintetičnega videa pooblašene osebe lahko goljufi pretentajo te sisteme in pridobijo nepooblaščen dostop do občutljivih območij ali tajnih podatkov.

**Kraja
identitete**

**Razširjanje
lažnih
informacij**

**Vdori v
varnostne
sisteme**

Manipulacija s tehnologijo deepfake



POSLEDICE:

Goljufije Deepfake imajo lahko resne negativne učinke, kot so:

01 Finančna izguba

Žrtve prevar z uporabo deepfake tehnologije lahko utrpijo znatno finančno izgubo. To se zgodi, ko so prevarane v prenos denarja ali razkritje finančnih podatkov na podlagi zavajajoče vsebine, ustvarjene s pomočjo deepfake tehnologije.

02 Čustvena stiska

Biti žrtev globoke lažne prevare lahko povzroči hudo čustveno stisko. Zaradi posega v osebno identiteto in morebitne razkritosti osebnih podatkov se lahko žrtve počutijo ranljive in prizadete.

03 Oškodovanje ugleda

Prevara z uporabo deepfake tehnologije lahko povzroči resno škodo ugledu posameznikov in organizacij. Lažne informacije, ki se širijo prelahko spodkopljejo zaupanje javnosti in povzročijo izgubo posla, pravne težave in druge negativne posledice

Manipulacija s tehnologijo deepfake



POSLEDICE:

04 Dezinformacije

Deepfake se lahko uporabljajo za širjenje lažnih informacij ali propagande, zavajanje javnosti in vplivanje na mnenja ali dejanja. To ima lahko resne družbene in politične posledice, resne družbene in politične posledice, na primer zmanjšanje zaupanja v institucije ali manipuliranje z izidi volitev.

05 Kraja identitete

Tehnologijo Deepfake je mogoče uporabiti za ustvarjanje sintetičnih videoposnetkov ali zvočnih posnetkov posameznikov, kar vodi v krajo identitete. Prevaranti se lahko izdajajo za nekoga in tako pridobijo dostop do osebnih podatkov, finančnih sredstev ali varnostnih sistemov.

06 Pravne posledice

Uporaba tehnologije deepfake za izvajanje prevar ali razširjanje lažnih informacij lahko povzroči pravne posledice tako za storilce kot za žrtve. Žrtve se lahko soočijo s pravnimi izzivi pri dokazovanju svoje nedolžnosti ali povrnitvi svojega ugleda, medtem ko se lahko storilci soočijo s kazenskimi ovadbami.

07 Izguba družbenega zaupanja

Zaradi razširjenosti deepfakeov se lahko zmanjša družbeno zaupanje in ljudje postanejo skeptični glede pristnosti digitalnih vsebin. Slednje lahko vodi v splošno nezaupanje v medije in informacije, ki se izmenjujejo na spletu, kar otežuje komunikacijo in širjenje resničnih informacij.

Manipulacija s tehnologijo deepfake

— NAČINI ZAŠČITE:

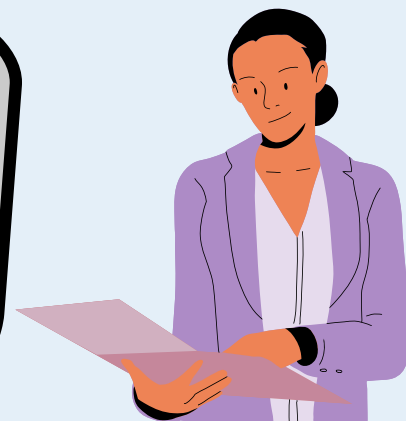


Nekega dne je Bill prejel elektronsko sporočilo svojega vnuka Jake. Elektronsko sporočilo je vsebovalo videoposnetek, v katerem je Jaka prosil za pomoč. Dejal je, da je na potovanju izgubil denarnico in da potrebuje denar za vrnitev domov. Videoposnetek je bil videti neverjetno pristen, saj je do potankosti odražal Jakin glas in njegovo obnašanje.

Bine je v skrbi za svojega vnuka takoj nakazal denar. Šele pozneje, ko je govoril s hčerko, je izvedel, da se Jaka sploh ni bil na potovanju.

Zmeden in šokiran je Bine ugotovil, da je bil žrtev prevare z deepfake tehnologijo. Videoposnetek z Jako ni bil resničen, ampak je bil deepfake – sintetični videoposnetek, ustvarjen z uporabo umetne inteligence.

Ta zgodba opozarja na ranljivost starejših za prevare z metodo deepfake ter poudarja potrebo po ozaveščanju in izobraževanju starejših. Starejši kot je Bine, se morda ne spoznajo na tako izpopolnjene prevare, zato so lahko lahka tarča. Zgodba poudarja, kako pomembno je starejše obveščati o tehnologiji deepfake, jih naučiti, kako preverjati prošnje za finančno pomoč, in spodbujati odprto komunikacijo v družinah, da bi potrdili pristnost takih prošenj.



1. KORAK: Preverjanje

Vedno preverite vse zahteve za finančno pomoč ali za občutljive podatke. Za Bilneta bi to pomenilo, da stopi v stik z vnukom neposredno prek znane in zaupanja vredne metode, kot je telefonski klic, da potrdi pristnost zahteve, preden ukrepa.

2. KORAK: Izobraževanje in ozaveščanje

Bine bi moral biti obveščen o najnovejših tehnoloških grožnjah, kot je npr. deepfake. Razumevanje, kako delujejo in kako jih je mogoče uporabiti pri prevarah, bi mu bo pomagalo prepoznati morebitne poskuse prevare in sprejeti ustrezne zaščitne ukrepe.

3. KORAK: Dodatni varnostni ukrepi

Bine bi moral uporabljati dodatne varnostne ukrepe, kot je npr. dvofaktorska avtentikacija za e-poštne račune in račune v družabnih omrežjih, ki omogoča dodatno raven zaščite pred nepooblaščenim dostopom in morebitnimi prevarami.

4. KORAK: Odprta komunikacija

Bine bi moral ohraniti odprto komunikacijo s svojo družino o kakršnih koli nenavadnih zahtevah ali sporočilih, ki jih prejme. Če se o tem pogovori z zaupanja vrednimi družinskimi člani, lahko hitro prepozna morebitne prevare in se jim izogne.

Manipulacija s tehnologijo deepfake



NAČINI ZAŠČITE:

Deepfake prevare lahko povzročijo veliko finančno izgubo, čustveno stisko in škodo ugledu. Poleg tega se lahko starejši pri okrevanju po takšnih prevarah soočajo s finančnimi in čustvenimi težavami. Če se starejši zavedajo teh groženj in sprejmejo zaščitne ukrepe, lahko zavarujejo svoje osebne podatke, ohranijo finančno varnost ter dostojanstvo in duševni mir.

Izobraževanje in ozaveščanje:

Bodite obveščeni o deepfakih, njihovih možnih uporabah in najnovejših orodjih, ki so na voljo za njihovo odkrivanje. Redno dopolnjujte svoje znanje o teh grožnjah in zaščitnih ukrepih pred njimi.



Preverjanje:

Vedno preverite vir videoposnetkov, zlasti tistih, ki vas pozivajo k finančni pomoči ali občutljivim informacijam. Stopite v stik z osebo, ki se pojavlja v videu, prek zaupanja vredne metode, da potrdite njeno verodostojnost in pristnost.



Manipulacija s tehnologijo deepfake



NAČINI ZAŠČITE:

Uporaba dodatnih varnostnih ukrepov:

Uporabite dodatne varnostne ukrepe, kot sta dvofaktorska avtentikacija in biometrično preverjanje, da zaščitite svoje osebne in finančne podatke.



Zaupajte zanesljivim virom:

Občutljive informacije delite le z zaupanja vrednimi viri in prek varnih platform. Bodite previdni pri nezaželenih sporočilih, ki zahtevajo osebne ali finančne podatke.

Prijavite sumljivo dejavnost:

Če naletite na morebitni deepfake, to prijavite ustreznim organom. To bo lahko preprečilo drugim, da bi postali žrtve, in pomagalo pri prijetju kriminalcev.



Storitvene prevare z lažnim predstavljanjem državnih institucij

— ZNAČILNOSTI NEVARNOSTI:

Storitvene prevare, ki se nanašajo za državne institucije, so povezane s prevaranti, ki se izdajajo za uslužbence uradnih vladnih organov ali služb. Ti prevaranti ponujajo pomoč pri urejanju uradnih dokumentov, kot so potni listi, vizumi ali socialna pomoč, vendar je njihov pravi cilj kraja vaših osebnih podatkov ali denarja.

Vrste manipulacij pri storitvenih prevarah:

Prevaranti ustvarjajo lažna spletna mesta ali pošiljajo e-poštna sporočila, ki so videti, kot da prihajajo od vladnih institucij. Lahko uporabljajo uradne logotipe in jezik, da so videti verodostojni.

Izdajanje za
uradne službe

Te prevare pogosto uporabljajo urgentni jezik in vas opozarjajo na posledice, če ne boste hitro ukrepali. To lahko vključuje grožnje z globami, pravnimi ukrepi ali zamujenimi roki.

Urgenten in
avtoritativen
jezik

Prevaranti od žrtev zahtevajo občutljive podatke, kot so številka socialnega zavarovanja, podatki o bančnem računu ali podatke o potnem listu.

Zahteve za
osebne
podatke

Prevaranti zahtevajo plačilo za svoje "storitve" vnaprej, pogosto z neizsledljivimi metodami, kot so bančna nakazila, predplačniške kartice ali kriptovalute.

Vnaprejšnja
plačila

Verodostojna in legitimna vladna spletišča vsebujejo jasne kontaktne informacije in možnosti za pomoč strankam. Na lažnih spletnih mestih so kontaktni podatki pogosto pomanjkljivi ali ponarejeni.

Pomanjkanje
neposrednih
kontaktnih
informacij

Storitvene prevare z lažnim predstavljanjem državnih institucij



POSLEDICE:

Storitvene prevare imajo lahko resne negativne učinke, kot so:

01 Pravne in administrativne posledice

Zaradi uporabe lažnih storitev lahko pride do pravnih težav, če žrtev nevede predloži lažne dokumente ali ne izpolnjuje zakonskih zahtev. To lahko povzroči globe, kazni ali dodatne pravne stroške.

02 Kraja identitete

Prevaranti pogosto zbirajo osebne podatke pod pretvezo, da jih potrebujejo za storitve, povezane z državo. Te podatke lahko uporabijo za krajo identitete žrtve, kar vodi do nepooblaščenih finančnih transakcij, odpiranja novih računov v njenem imenu in drugih goljufivih dejanj.

03 Izguba zaupanja v zakonite institucije

Če so bili prevarani s strani osebe, ki se je izdajala za predstavnika državne institucije, lahko starejši postanejo nezaupljivi do pravih državnih organov in uradnikov. To lahko zmanjša njihovo pripravljenost, da bi poiskali pomoč ali storitve, ki jih resnično potrebujejo.

04 Finančna izguba

Starejši lahko plačajo za lažne storitve, kot so stroški obdelave neobstoječih ugodnosti ali pomoč pri pripravi uradnih dokumentov. Posledica tega je neposredna finančna škoda, ki je lahko še posebej pereča za osebe s fiksnimi dohodki.

Storitvene prevare z lažnim predstavljanjem državnih institucij

— NAČINI ZAŠČITE:



Milka je od državne uprave prejela elektronsko sporočilo, v katerem je navedeno, da mora nujno obnoviti potni list, da bi se izognila kazni. Elektronsko sporočilo je vključevalo povezavo do spletnega mesta, ki je bilo videti uradno in je bilo opremljeno z logotipom ministrstva ter napisano v uradnem jeziku. Spletna stran je zahtevala posredovanje osebnih podatkov in plačilo pristojbine v višini 150 EUR za pospešitev postopka podaljšanja. Kaj naj stori Milka?

Storitvene prevare z lažnim predstavljanjem državnih institucij lahko povzročijo resno finančno in čustveno škodo, zlasti starejšim. Pred tovrstnimi prevarami se lahko zavarujete tako, da preverite vir informacij, ste skeptični do nujnih prošenj, zaščitite osebne podatke in uporabljate varne plačilne metode.

Vedno se prepričajte, da uporabljate prava in legitimna vladna spletišča in storitve, da ne postanete žrtev goljufivih shem.



1. KORAK: Preverite vir

Za potrditev postopka podaljšanja potnega lista neposredno preverite uradno spletno stran državnega oddelka ali pokličite njihovo službo za pomoč strankam.

2. KORAK: Bodite skeptični do nujnih zahtev

Upoštevajte dejstvo, da verodostojne vladne službe ne bodo pošiljale nujnih prošenj za podaljšanje po elektronski pošti.

3. KORAK: Ne delite osebnih podatkov

Na spletnem mestu ne vpisujte osebnih podatkov, dokler ne preverite njegove pristnosti.

4. KORAK: Uporabite varne načine plačila

Bodite previdni pri zahtevah za plačilo in preverite, ali urad določa takšne pristojbine in omogoča tovrstne storitve.

Storitvene prevare z lažnim predstavljanjem državnih institucij

— NAČINI ZAŠČITE:

Zaščita pred storitvenimi prevarami, ki se sklicujejo na državne institucije, je ključnega pomena za zaščito vaših osebnih podatkov, denarja in čustev. Tukaj je nekaj preprostih ukrepov, ki jih lahko storite, da se zaščitite.

Ne delite osebnih podatkov:

Izogibajte se posredovanju občutljivih podatkov, kot so vaša številka socialnega zavarovanja, bančni podatki ali podatki o potnem listu, razen če ste prepričani, da je spletno mesto legitimno.



Preverite vir:

Prepričajte se, da ste na uradni spletni strani državne institucije. V spletnem naslovu, ki ga uporabljajo vladne ustanove, poiščite "gov". Obrnite se neposredno na državno institucijo z uporabo informacij iz uradnega vira, ne s kontaktnimi podatki, navedenimi v sumljivem e-poštnem sporočilu ali na spletnem mestu.

Bodite skeptični do nujnih zahtev:

Bodite previdni, če prejmete nujna ali grozilna sporočila, ki zahtevajo takojšnje ukrepanje ali plačilo. Verodostojne državne ustanove ne delujejo na ta način.



Prevara z lažnimi računi

— ZNAČILNOSTI NEVARNOSTI:

Izsiljevanje z lažnimi računi je zavajajoča praksa, pri kateri prevaranti ustvarijo ponarejene profile v družabnih medijih in se pogosto izdajajo za nekoga, ki ga žrtev pozna ali mu zaupa. Ta prevara je usmerjena zlasti na starejše, ki morda slabše poznajo digitalne platforme. Prevaranti običajno vzpostavijo stik s pošiljanjem prošenj za prijateljstvo, nato pa začnejo deliti eksplicitno ali škodljivo vsebino. Prevaranti nato zahtevajo denar ali druge oblike plačila in grozijo, da bodo škodovali ugledu starejše osebe, saj jo bodo povezali z neprimerno vsebino.

Vrste izsiljevanja z lažnimi računi:

Prevarant ustvari lažni račun, pri čemer se predstavlja kot oseba, ki jo žrtev pozna, pridobi si njeno zaupanje in ga uporabi za začetek izsiljevanja.

Lažno predstavlanje za prijatelja ali znanca

Prevarant ustvari lažno identiteto, pogosto je to oseba, ki se romantično zanima za žrtev. Ko je žrtev čustveno vpletena, prevarant začne izsiljevanje.

"Catfishing" – lažno predstavlja nje na spletu

Prevarant ustvari lažni račun slavne ali javne osebe. Nato stopi v stik z oboževalci ali sledilci, z njimi deli eksplicitno vsebino in zahteva denar z grožnjo, da bo omadeževal ugled oboževalca.

Lažno predstavlanje za slavno ali javno osebo

Prevara z lažnimi računi



POSLEDICE:

Izsiljevanje z lažnimi računi ima lahko resne negativne posledice, kot so:

01 Čustvena in psihološka stiska

Med glavnimi posledicami, s katerimi se žrtev lahko sooča, so velike čustvene in psihološke stiske. To je pogosto neposredna posledica nenehnih groženj in nenehnega nadlegovanja, ki ga izvaja prevarant. Te stiske se lahko kažejo na številne načine, vključno s strahom, tesnobo, depresijo in motnjami spanja, kar bistveno vpliva na vsakdanje življenje žrtve.

02 Finančna izguba

Dodatno tveganje, ki so mu žrtve izpostavljene, je možnost velike finančne izgube. To se običajno zgodi, ko se žrtev, zaradi občutka pritiska in preobremenjenosti zaradi vztrajnih zahtev prevaranta, na koncu vdá. Posledično lahko doživi ne samo izgubo svojega težko prisluženega denarja, temveč tudi stres in tesnobo, ki spremljata takšno izgubo.

03 Oškodovanje ugleda

Poleg tega obstaja nevarnost, da bo žrtev resno oškodovana na svojem ugledu. To se lahko zgodi, če se prevarant odloči, da bo uresničil svoje grožnje, pri čemer lahko razkrije neželene ali občutljive informacije o žrtvi. To lahko povzroči znatno poslabšanje družbenega položaja žrtve in lahko vpliva na njene osebne in poklicne odnose ter njeno prihodnost nasploh.

Prevara z lažnimi računi

— NAČINE ZAŠČITE:



Nekega dne je Suzana prejela prošnjo za prijateljstvo z računa z imenom svojega starega prijatelja, s katerim že dolgo ni bila v stiku. Navdušena nad možnostjo ponovnega druženja je zahtevo sprejela. Kmalu zatem sta si začeli izmenjevati sporočila in se spominjati starih časov. Vendar so se stvari zapletle, ko je prijatelj začel deliti eksplicitno vsebino in zahteval denar ter grozil, da bo omadeževal njen ugled, ker bo njeno ime povezal z vsebino.

Suzano, ki jo je pretresla nenadna sprememba, se je odločila, da bo s svojim resničnim prijateljem stopila v stik prek drugega medija. Ko je izvedela, da njen prijatelj za ta račun ne ve, je ugotovila, da je komunicirala z lažnim računom, ki ga je ustvaril prevarant.

Ta zgodba poudarja, kako pomembno je starejše poučiti o morebitnih tveganjih, ki jih prinaša spletno komuniciranje z neznanimi osebami. Poudarja, kako so lahko starejši zaradi morebitnega nepoznavanja digitalnih platform tarča prevar, kot je izsiljevanje prek lažnih računov. Zgodba služi kot opomnik starejšim, naj preverijo identiteto posameznikov, preden z njimi sodelujejo na spletu, in o morebitnih sumljivih dejavnostih obvestijo platformo ali lokalne organe. Poudarja potrebo po ozaveščenosti in previdnosti v digitalnem svetu za zaščito dobrega počutja in finančne varnosti starejših.



1. KORAK: Preverite prošnje za prijateljstvo

Suzana je sprejela prošnjo za prijateljstvo z računa, za katerega je verjela, da je račun starega prijatelja, ne da bi preverila njegovo pristnost. Suzana bi morala stopiti v stik s svojim dejanskim prijateljem prek drugega medija, da preveri pristnost prošnje za prijateljstvo, preden jo sprejme.

2. KORAK: Bodite previdni z osebnimi podatki

Suzana je sodelovala v pogovorih in delila osebne spomine, ne da bi posumila v podlo igro. Suzana bi morala biti previdna in se izogibati razkrivanju osebnih podatkov ali vključevanju v občutljive pogovore, dokler ni prepričana o identiteti osebe druge strani.

3. KORAK: Prepoznajte sumljivo vedenje

Suzana je še naprej komunicirala s "prijateljem" tudi potem, ko je začel deliti eksplicitno vsebino in postavljati nenavadne zahteve. Ko je Suzana opazila sumljivo vedenje, bi morala takoj prenehati komunicirati in račun označiti kot sumljivega.

4. KORAK: Prijavite in se izobražujte

Ko je ugotovila, da je račun lažen, je Suzana prijavila incident in svojo izkušnjo delila s prijatelji in družino. Suzanina dejanja – prijava računa in izobraževanja drugih – sta bila primerna. Suzana bi morala še naprej spodbujati ozaveščenost in previdnost pred spletnimi prevarami.

Prevara z lažnimi računi



NAČINI ZAŠČITE:

Zaščita pred izsiljevanjem z uporabo lažnih računov je ključnega pomena, zlasti za starejše, saj pomaga preprečiti čustvene in psihološke stiske, finančno izgubo in oškodovanje ugleda. Starejši so lahko zaradi morebitnega nepoznavanja digitalnih platform bolj ranljivi za te prevare. Z pazljivostjo in previdnostjo na spletu lahko starejši zaščitijo svoje blagostanje in finančno varnost ter si tako zagotovijo varnejšo in prijetnejšo spletno izkušnjo.

Preverjanje prošelj za prijateljstvo:

Vedno preverite identiteto osebe, ki pošilja prošnjo za prijateljstvo, zlasti če z njo že nekaj časa niste bili v stiku. To lahko storite tako, da z njim vzpostavite stik prek d medija, ki ste ga pred tem uporabljali za komunikacijo.



Nastavitve zasebnosti:

Poskrbite, da bodo vaši računi v družabnih medijih nastavljeni na maksimalne nastavitve zasebnosti. Tako boste omejili količino informacij, ki jih lahko vidijo osebe, ki niso na seznamu vaših prijateljev.



Prevara z lažnimi računi



NAČINI ZAŠČITE:

Ne delite občutljivih informacij:

Izogibajte se deljenju osebnih ali občutljivih informacij na spletu. Če se oseba, s katero komunicirate, začne obnašati sumljivo ali zahtevati denar, takoj prekinite pogovor.



Prijavite sumljivo dejavnost:

Če naletite na sumljiv račun ali če nekdo začne deliti neprimerno vsebino ali groziti, prijavite račun platformi družabnih medijev in lokalnim oblastem.

Izobražujte sebe in druge:

Naučite se, kateri so najpogostejši znaki spletnih prevar, in o teh znakih poučite tudi druge. Tako se boste vi in vaši bližnji izognili temu, da bi postali žrtve takšnih prevar.



Dodatno branje



OBTOŽBE O VPLETENOSTI V KRIMINAL

- <https://www.legalmatch.com/law-library/article/allegations-of-criminal-involvement.html>
- <https://www.findlaw.com/criminal/criminal-charges/defending-against-criminal-charges.html>
- <https://www.nolo.com/legal-encyclopedia/criminal-defense-strategies>
- <https://www.lawinfo.com/resources/criminal-defense/>
- <https://www.justia.com/criminal/>
- <https://www.avvo.com/topics/criminal-charges>
- <https://www.legalzoom.com/articles/what-to-do-if-youre-accused-of-a-crime>
- <https://www.hg.org/criminal.html> <https://www.lawyers.com/legal-info/criminal/>
- https://www.americanbar.org/groups/criminal_justice/



MANIPULACIJE PRI PREVARAH Z LAŽNIM PREDSTAVLJANJEM JAVNIH INSTITUCIJ

- <https://www.ncoa.org/article/government-imposter-scams-what-they-are-and-how-to-spot-them>
- <https://www.nia.nih.gov/news/high-vulnerability-government-impersonation-scams-among-older-adults>
- <https://www.idnow.io/glossary/impostor-fraud/>
- <https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/senior-citizens-financial-scams/>
- <https://consumer.ftc.gov/articles/how-avoid-government-impersonation-scam#whattoknow>
- <https://regtechtimes.com/government-impersonation-scams-your-shield/>
- <https://www.europol.europa.eu/media-press/newsroom/news/beware-of-scams-involving-fake-correspondence-europol>

Dodatno branje



MANIPULACIJA S TEHNOLOGIJO DEEPPAKE

- <https://www.bitdefender.com/blog/labs/deepfakes-what-they-are-how-they-work-and-how-to-protect-against-malicious-usage-in-the-digital-age>
- <https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained>
- <https://www.media.mit.edu/posts/deepfakes-explained/>
- <https://www.sentinelone.com/blog/what-are-deepfakes-how-can-you-spot-them/>
- <https://www.datavisor.com/blog/how-deepfakes-are-made-and-how-fraudsters-use-them/>
- <https://www.iproov.com/blog/deepfake-fraud-identity-theft-explained>
- <https://techmonitor.ai/technology/ai-and-automation/audio-deepfake-scams-the-growing-threat-explored>
- <https://readwrite.com/are-deepfakes-illegal-ais-dark-side-explained/>



STORITVENE PREVARE Z LAŽNIM PREDSTAVLJANJEM DRŽAVNIH INSTITUCIJ

- <https://www.c-span.org/video/?468676-1/social-security-scams>
- <https://www.nia.nih.gov/news/high-vulnerability-government-impersonation-scams-among-older-adults>
- <https://www.bressler.com/news-1882>
- <https://consumer.ftc.gov/articles/how-avoid-government-impersonation-scam>
- https://www.facebook.com/europol/videos/%EF%B8%8F-beware-scammers-impersonating-europol-officers-europol-never-contacts-members-/1097501060976901/?_rdr

Dodatna branja



PREVARA Z LAŽNIMI RAČUNI

- <https://www.malwaretips.com/i-have-your-secrets-fake-blackmail-sextortion-scam-email>
- <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/sextortion-scams>
- https://www.scamnet.wa.gov.au/scamnet/Fight_back.htm
- <https://www.antivirus.com/blackmail-and-sextortion-emails>
- <https://www.malwaretips.com/hello-perv-blackmail-emails-are-fake>
- <https://www.womenslaw.org/about-abuse/abuse-using-technology/impersonation>
- <https://www.minclaw.com/how-to-deal-with-google-chat-blackmail>
- <https://www.digitalinvestigation.com/blog/blackmail-on-tiktok>
- <https://www.justice.gov/opa/pr/us-law-enforcement-joins-international-partners-disrupt-international-sextortion-ring>
- <https://www.cyber.gov.au/acsc/view-all-content/publications/sextortion-scams>



www.cybersafesenior.eu



Cyber-Safe-Senior



Funded by
the European Union

CYBER SAFE
SENIOR 



Instytut
Nowych Technologii



SIMBIOZA
MED GENERACIJAMI

"Financirano s strani Evropske unije. Izražena stališča in mnenja so zgolj stališča in mnenja avtorja(-ev) in ni nujno, da odražajo stališča in mnenja Evropske unije ali Erasmus+ nacionalne agencije. Zanje ne moreta biti odgovorna niti Evropska unija niti organ, ki dodeli sredstva".



To gradivo je na voljo pod odprto licenco CC.3.0 BY-NC-ND 3.0 PL (Priznanje avtorstva - nekomercialna dela - brez izpeljank 3.0 Poljska), ki vam omogoča distribucijo, predstavitev in izvajanje dela samo v nekomercialne namene in pod pogojem, da je ohranjeno v izvirni obliki (brez izpeljank). Več informacij: <https://creativecommons.org/licenses/by-nd/3.0/pl/legalcode>

