

Kibernetska varnost

Predavatelj: dr. Miha Dvojmoč

Naročnik: BUKEV d.o.o.

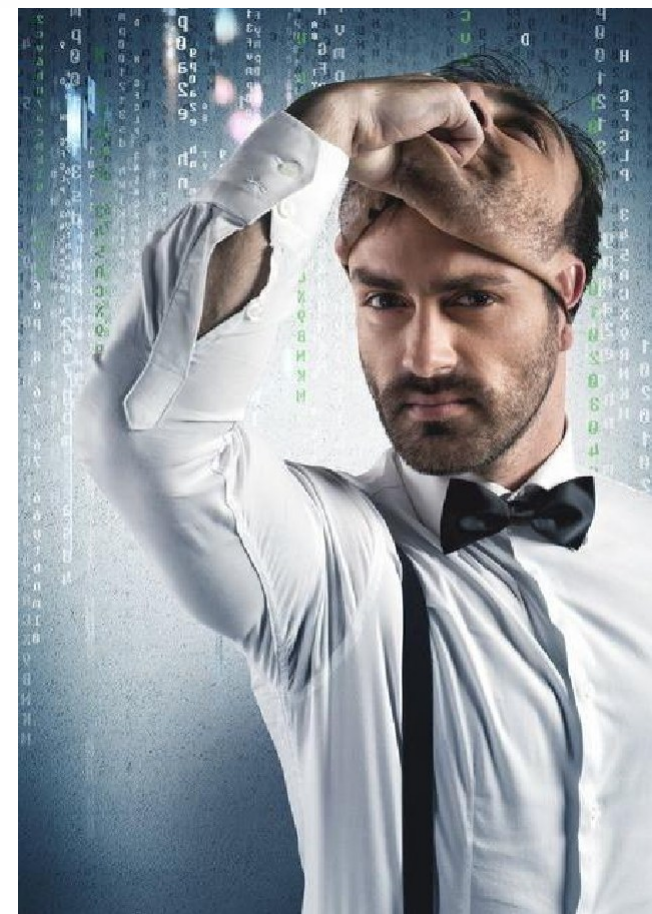
Izvajalec: MD svetovanje d.o.o.

Datum: 9. 12. 2024

Kaj je socialni inženiring?

Socialni inženiring je manipulacija s posamezniki, da ti razkrijejo zaupne informacije, običajno z namenom pridobitve nepooblaščenega dostopa do informacijskih sistemov.

Socialni inženiring predstavlja resno grožnjo za IT-varnost, saj se zanaša na človeški element, ki je pogosto najšibkejši člen v varnostnem sistemu. Izkorišča človeška čustva in lastnosti, kot so: zaupanje, strah, naivnost, radovednost, osamljenost in pohlep.

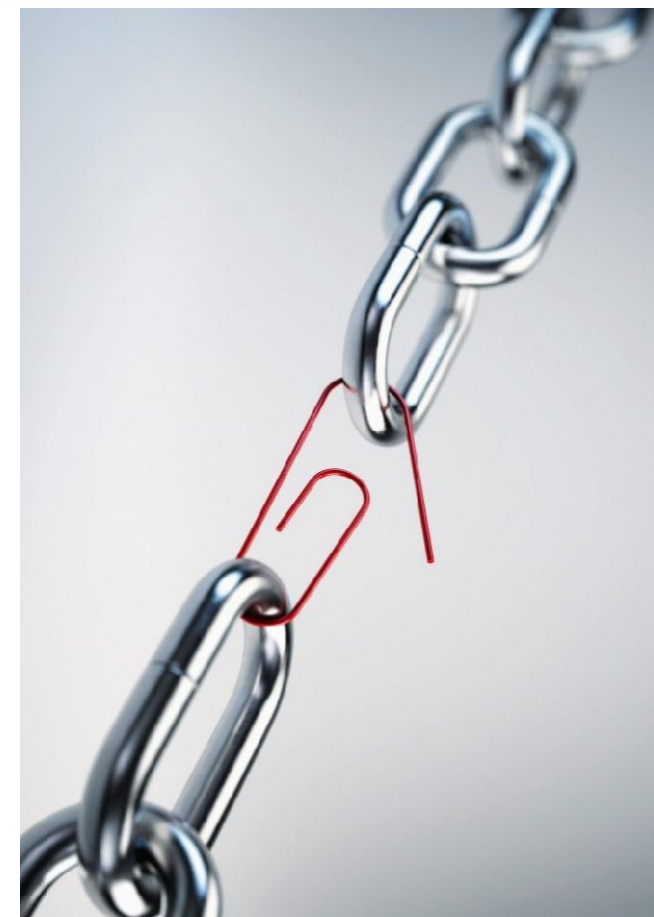


Iskanje najšibkejšega člena v organizaciji

Ko razmišljamo o kibernetiski varnosti, nas večina pomisli na obrambo pred virusi, črvi in hakerji, ki uporabljajo tehnološke pomanjkljivosti za napad na podatkovna omrežja.

Toda obstaja še en način vstopa v organizacije in omrežja, in to je izkoriščanje človeške šibkosti.

To je znano kot socialni inženiring, ki vključuje prevaro nekoga, da razkrije informacije ali omogoči dostop do podatkovnih omrežij.



Vrste napadov socialnega inženiringa

Zvabljanje: Prevaranti pošiljajo lažna e-poštna sporočila, da bi pridobili občutljive informacije, kot so gesla in številke kreditnih kartic.

Goljufije in prevare: Napadalci pogosto ustvarijo občutek nujnosti, da prisilijo žrtev v hitro in nepremišljeno delovanje.

Lažno predstavljanje: Napadalci se pogosto predstavljajo kot nekdo drugi, zaupanja vredne osebe ali avtoritete, da pridobijo dostop do informacij ali sistemov.



Zvabljanje – ribarjenje (phishing)

- Lažna e-pošta in priponke.
- Lažne spletne strani.
- SMS sporočila (smishing).
- Telefonski klici (vishing).
- Socialna omrežja.



Prevare preko E-pošte

PRIMER PREVARE – „MICROSOFT“

Danes lažna e-pošta že vsebuje pravilno slovenščino, smiselni e-naslov in domeno ter na videz zelo verodostojno spletno stran.



Microsoftov račun

Zazan je bil nov vpis

Nedavno ste se vpisali v svoj Microsoftov račun. Oglejte si nekaj podrobnosti za lastno varnost:

Država/regija: Slovenija
Datum: 08. 05. 2024 08:20 (CET)
Storitev: Link to Windows
Naslov IP: 176.76.227.94

Če ste to bili vi, lahko prezrete to e-poštno sporočilo.

Pregled dejavnosti računa

Prejemanje varnostnih obvestil lahko tudi [prekličete](#) ali spremenite naslov za prejemanje varnostnih obvestil.

Hvala,
Skupina za Microsoftov račun

[Izjava o zasebnosti](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Zaznana je bila nova zahteva za vpis za vaš Microsoftov račun

SZ

Skupina za Microsoftov račun <account-security-noreply@microsoft-support.eu>
Za mitja@virtual.si

Prevare preko E-pošte

PRIMER PREVARE – „NOVICE“

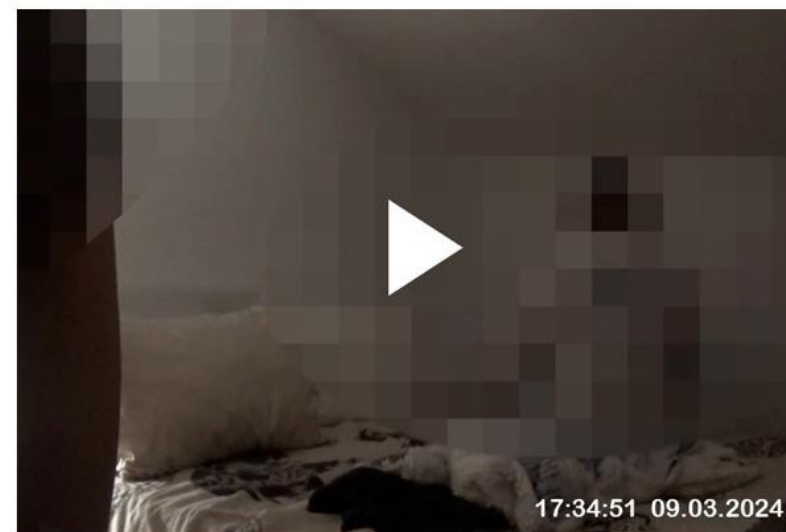
Po raziskavah največ ljudi klikne na povezave:

- **spolnost**
- **aktualni trači (znane osebe, dogodki ...)**
- **brezplačne stvari in nagradne igre**
- **ugodna ponudba**
- **zdravje in prehrana**

Šok! Znani Slovenec ujet med predajanjem spolnim užitkom ...

 novice@klik24.si
Za mitja@virtual.si

KLik24



Nadzorna kamera je ujela znanega Slovenca med predajanjem spolnim užitkom (samo za 18+) ...

Konec ugibanj, vsem poznani slovenec nas je vsa leta namerno zavajal ...

PRIMER PREVARE – „NOVICE“



8 navad, ki podaljšujejo življenje

Naš odnos do življenja ima neposreden vpliv na našo življenjsko dobo. Osebe z jasnimi cilji in načrti naj bi živeli do 13 let dlje ...

[Preberite več ...](#)



Potem pa šok, o moj bog ...

Znani štajerski slavček Damjan Murko o svojem skritem življenju. Murko: "Žena se je pač morala sprijazniti ..." Kdo je Damjanov "srečnež"?

[Preberite več ...](#)



Otok Pag, Novalja, Hotel ****

Pomlad je tu in s tem že topli dnevi, kar samo kliče po kratkem oddihu na morju ali po rezervaciji poletnih počitnic. Omejeni paketi noro ugodne ponudbe v hotelu s štirimi zvezdicami, lokacijo tik ob morju, lastnim bazenom, izvrstno kulinariko ...

[Preverite ponudbo!](#)

Ponudba meseca



OMEJENA PONUDBA

Zunanji disk 1TB za
samo 29,90 EUR

[Več informacij ...](#)



AKCIJA

Serum mladosti po
znižani ceni!

[Več informacij ...](#)



IZBERITE TERMIN

Pranje in voskanje
vozila za **9,90 EUR**

[Več informacij ...](#)

RE:RE: Naročilo M-HTECH



Ivana Predić <iveljkovk@falkenstein.rs>
Za undisclosed-recipients:



MATALJ Ponuda 30.05 2024 SMKTGTECH634667478874873845985309802Thayne.gz
5 KB

Dobro jutro,

Za vašo informacijo smo priložili osnutek tega Naročila in podrobnosti o ISF.
Obravnavajte kot nujno in oddajte ponudbo

Lep pozdrav,



Ivana Predić

Mobilni: +386 60 544 72 23

E-mail: office@mataljvinarija.si

Matalj Vinarija | Sneberska c. 22b, 1260
Ljubljana, Slovenia



www.mataljvinarija.si

LIVARNA TITAN / RFQ: FT-2024-S513 / APC9231913 (09.05.2024)



Anja Vodlan <anja.vodlan@livarna-titan.eu>
Za undisclosed-recipients:



LIVARNA TITAN RFQ FT-2024-S513 APC9231913.rar
7 KB

Dragi gospod,

Zahtevana ponudba je priložena

hvala

Prijazni pozdravi

Anja Vodlan

Purchase / Procurement

Phone: +386 1 830 93 54

Mobile: +386 30 703 833

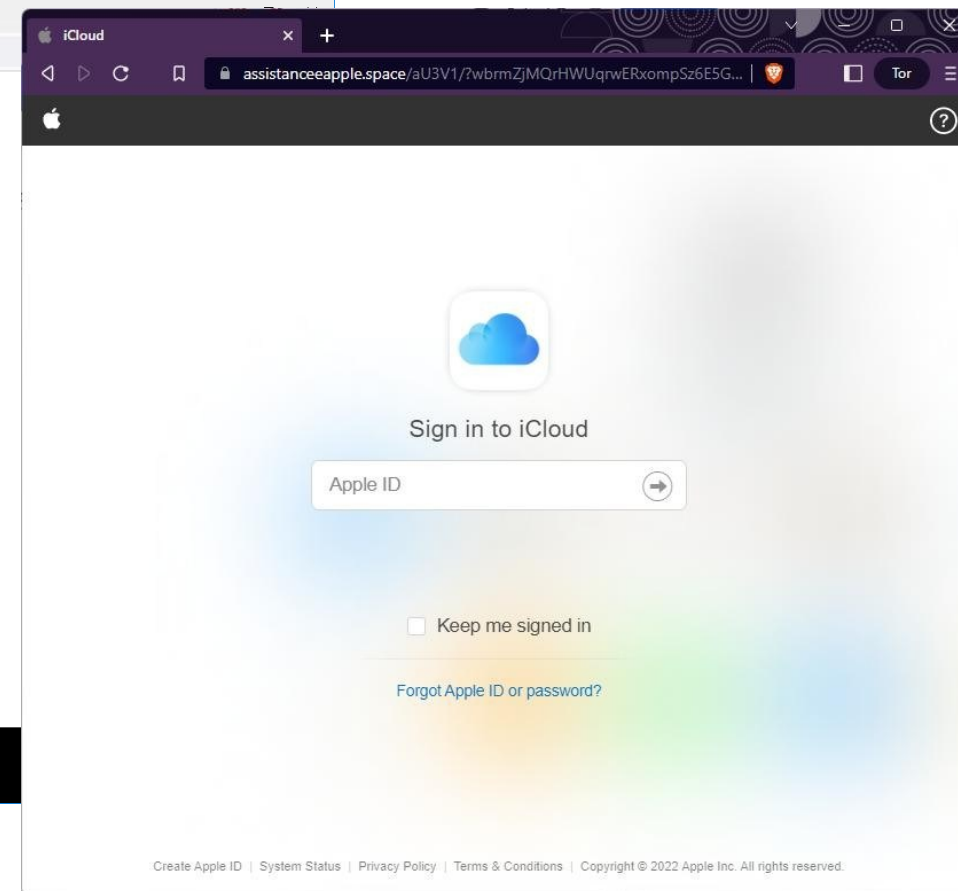
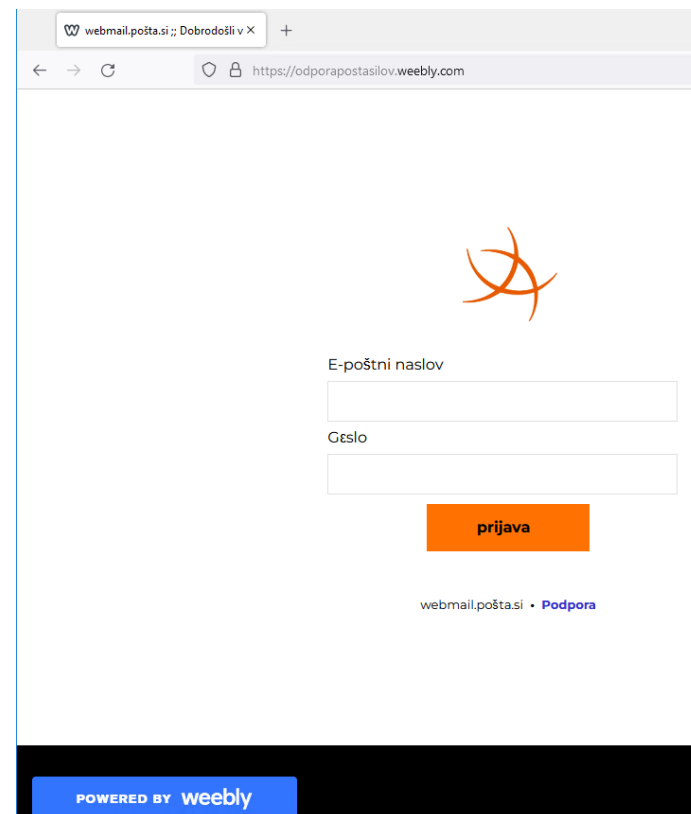
Email: anja.vodlan@livarna-titan.eu

Livarna Titan doo Kovinarska cesta 28, SI-1240 Kamnik, Slovenia, www.livarna-titan.eu

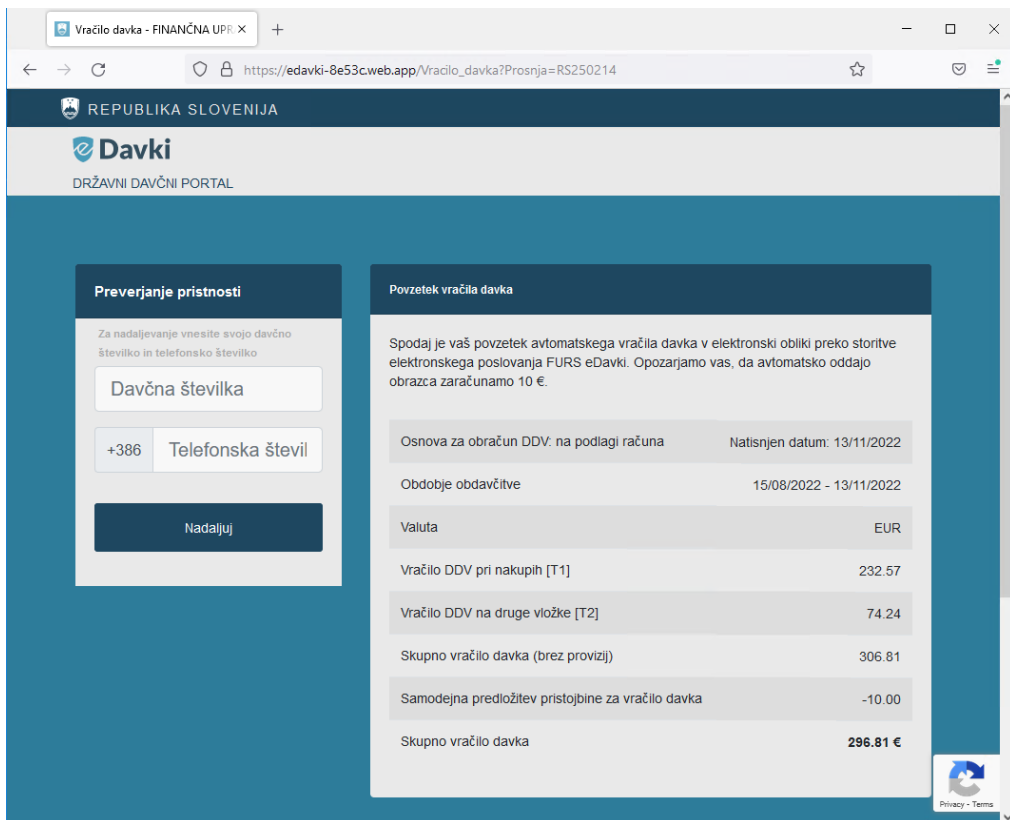


Lažne spletne strani

Zadnje obdobje se v Sloveniji pojavlja veliko lažnih spletni strani oziroma spletnih trgovin, ki želijo vplivati na miselnost ljudi ali jih finančno oškodovati.



PRIMERI LAŽNIH SPLETNI STRANI



Vračilo davka - FINANČNA UPRAVNA AGENCIJA

https://edavki-8e53c.web.app/Vracilo_davka?Prosnja=RS250214

REPUBLIKA SLOVENIJA

Davki

DRŽAVNI DAVČNI PORTAL

Preverjanje pristnosti

Za nadaljevanje vnesite svojo davčno številko in telefonsko številko

Davčna številka

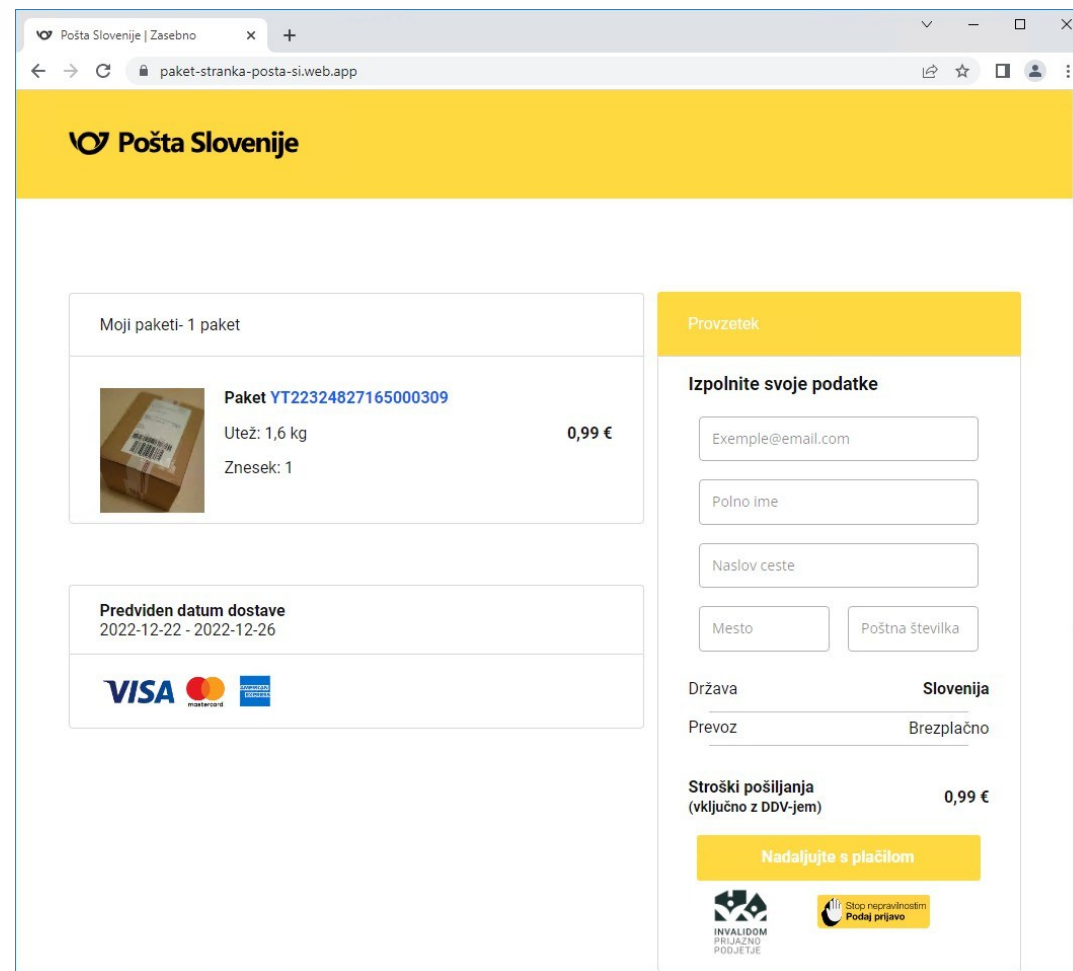
+386 Telefonska števil

Nadaljuj

Povzetek vračila davka

Spodaj je vaš povzetek avtomatskega vračila davka v elektronski obliki preko storitve elektronskega poslovanja FURS eDavki. Opozarjamo vas, da avtomatsko oddajo obrazca zaračunamo 10 €.

Osnova za obračun DDV: na podlagi računa	Natisnjen datum: 13/11/2022
Obdobje obdavčitve	15/08/2022 - 13/11/2022
Valuta	EUR
Vračilo DDV pri nakupih [T1]	232.57
Vračilo DDV na druge vložke [T2]	74.24
Skupno vračilo davka (brez provizij)	306.81
Samodejna predložitev pristojbine za vračilo davka	-10.00
Skupno vračilo davka	296.81 €



Pošta Slovenije | Zasebno

paket-stranka-posta-si.web.app

Pošta Slovenije

Moji paketi- 1 paket



Paket YT2324827165000309

Utež: 1,6 kg

Znasek: 1

0,99 €

Predviden datum dostave
2022-12-22 - 2022-12-26

VISA  

Provizetek

Izpolnite svoje podatke

Exemple@email.com

Polno ime

Naslov ceste

Mesto Poštna številka

Država **Slovenija**

Prevoz **Brezplačno**

Stroški pošiljanja (vključno z DDV-jem) **0,99 €**

Nadaljujte s plačilom

PRIMERI LAŽNIH SPLETNI TRGOVIN



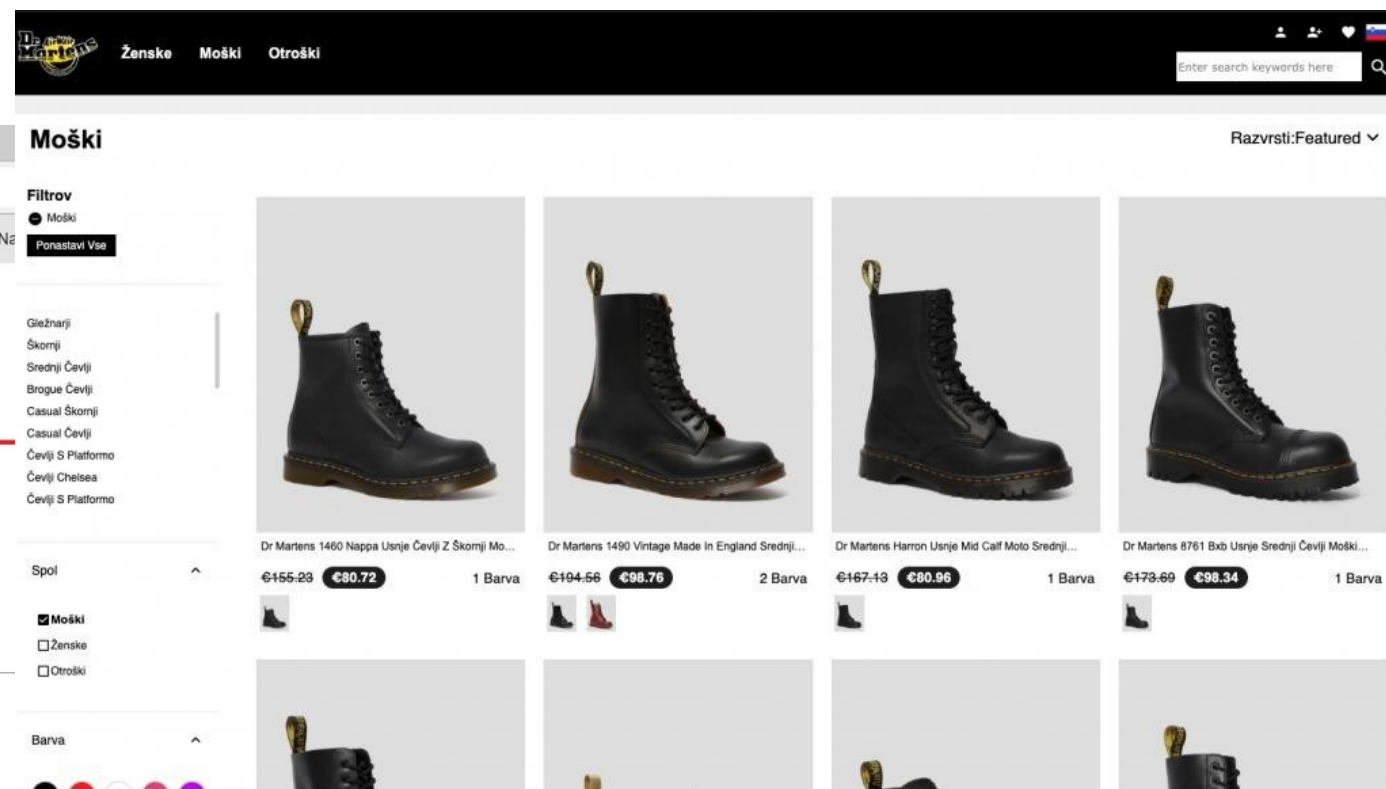
Full Name:

E-mail Naslov:

Preverjanje Računa 

Opiši Svojo Skrb Tukaj:

Pošlji

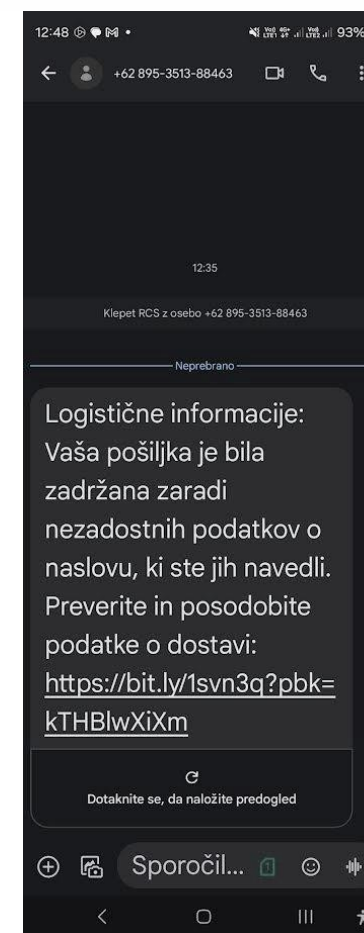
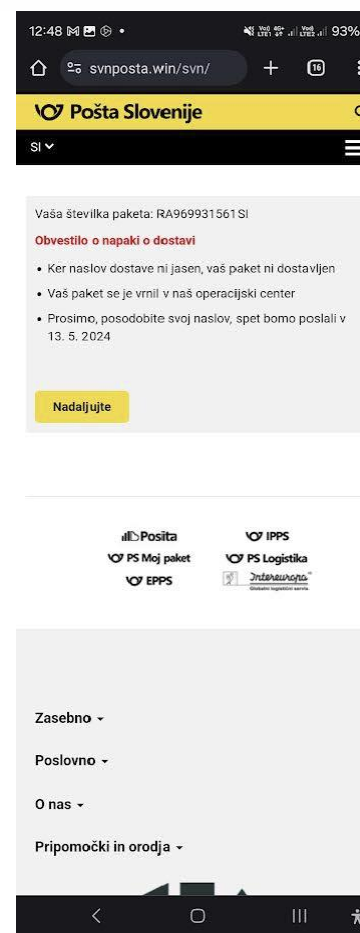


Prevare preko SMS sporočil

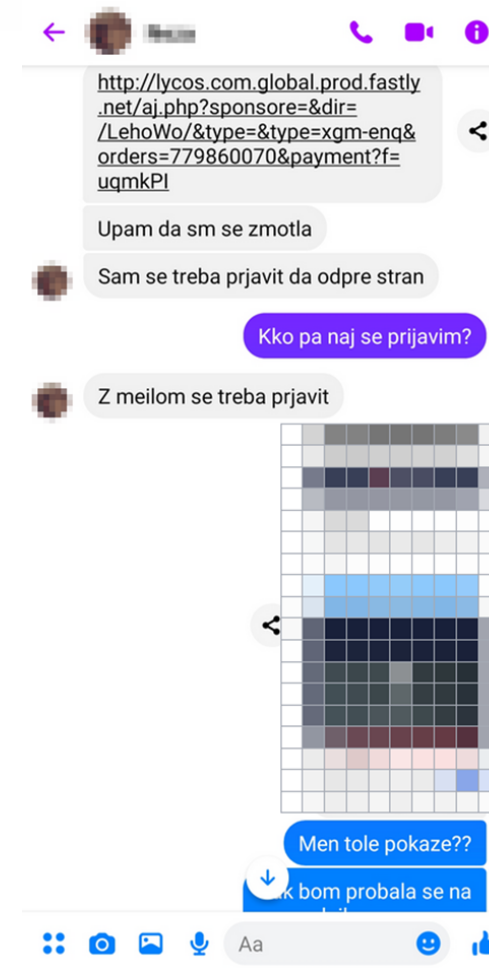
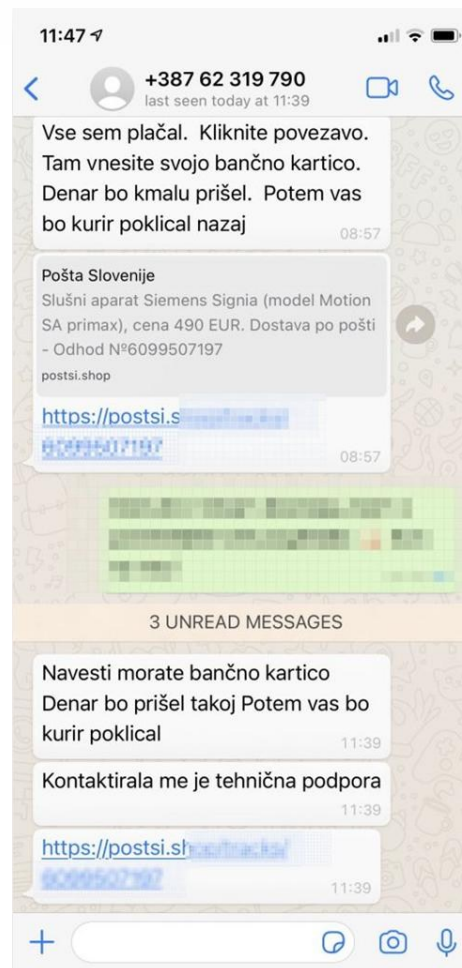
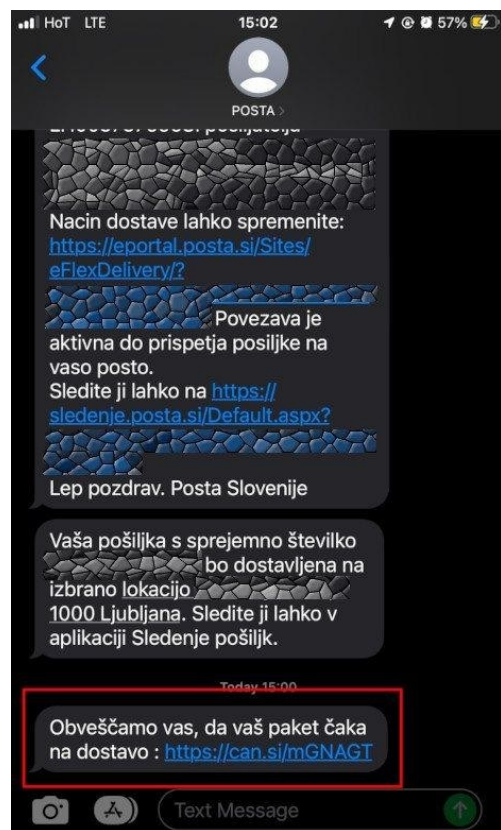
PRIMER PREVARE – „POŠTA SLOVENIJE“

Hekerji oziroma prevaranti se poslužujejo tudi komunikacije preko SMS sporočil z namenov:

- pridobiti podatke o plačilni kartici;
- namestiti zlonamerno programsko kodo za dostop do telefona (kraja podatkov in kasneje izsiljevanje).



PRIMERI LAŽNIH SMS SPOROČIL



Prevare preko socialnih omrežij

PRIMER PREVARE PREKO FACEBOOK

Prevaranti so prisotni tudi na socialnih omrežij, kjer želijo:

- pridobiti podatke o nas in naših plačilnih karticah;
- namestiti zlonamerno programsko kodo za dostop (kraja podatkov in kasneje izsiljevanje);
- ukrasti naš osebni profil na socialnem omrežju in ga zlorabiti;
- s prevaro od nas pridobiti finančna sredstva (kriptovalute ...).



Prevare preko telefona

Prevare preko telefona postajajo zadnje obdobje zelo popularne, predvideva se celo, da bodo v prihodnosti eno najmočnejših orodij pri prevarah zaradi umetne inteligence.

Najbolj pogosti primeri telefonskih prevar so:

- direktorske prevare (nadrejeni in računovodstvo);
- tehnična podpora (npr. Microsoft, IT-vzdrževalec ...);
- telefonske ankete, nagradne igre ...
- potencialna stranka oz. dobavitelj;
- javni uslužbenci (FURS, inšpektorati ...).



Lažno predstavljanje (impersonation)

- Napadalec doseže zaupanja žrtve tako, da se pretvarja, da ga pozna in/ali mu zaupa.
- Ponarejen profil na družbenih omrežjih.
- Direktorske prevare.



Prevare (scam, fraud ...)

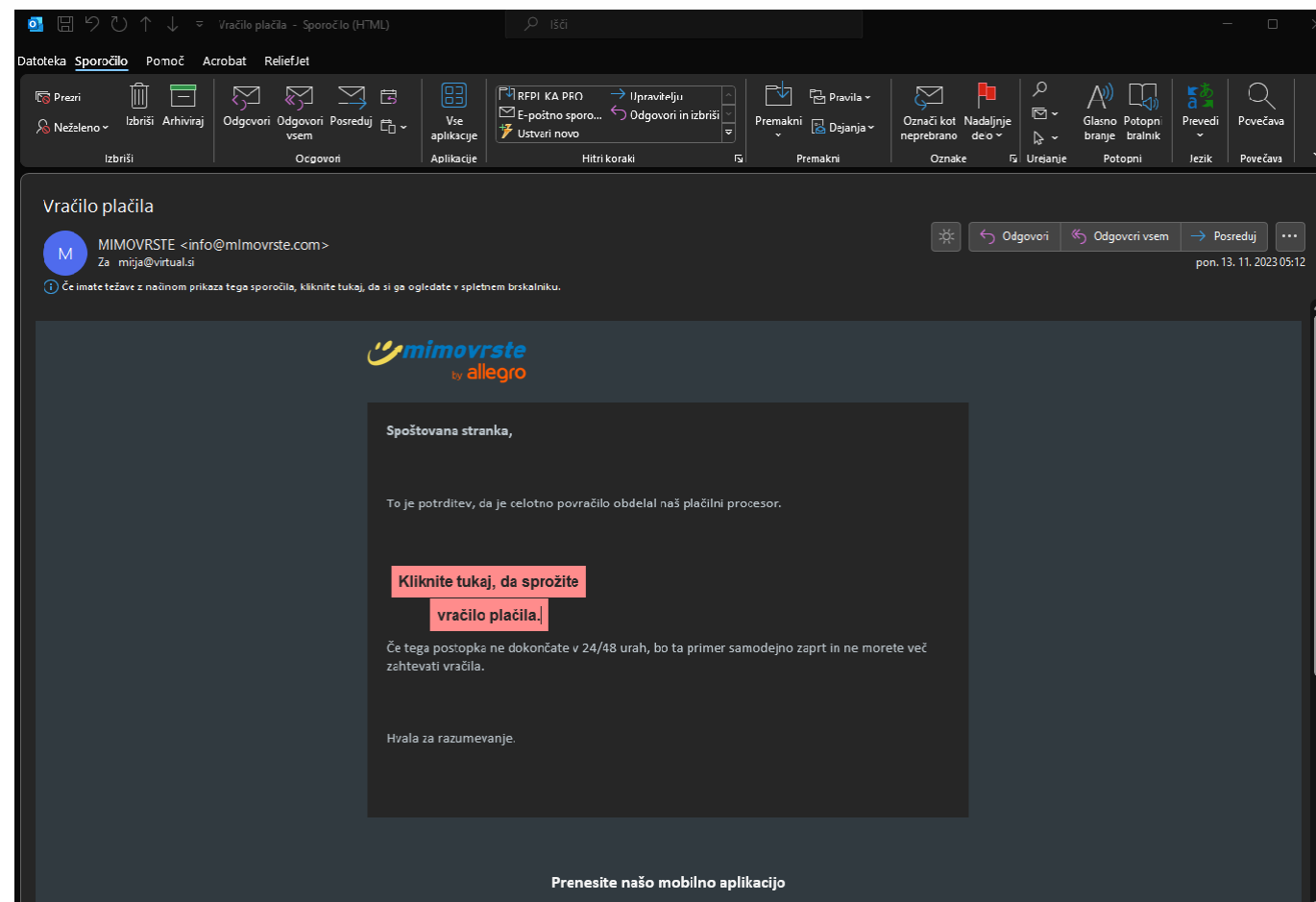
- Prevare s plačilnimi karticami
- Lažni krediti
- Telefonske prevare
- Ljubezenske prevare



Prevare s plačilnimi karticami

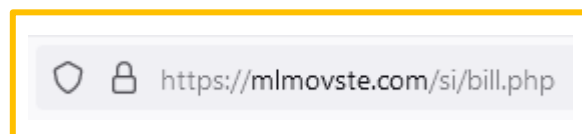
PRIMER PREVARE – „MIMOVRSTE“

Od: MIMOVRSTE <info@mlmovrste.com>
Poslano: ponedeljek, 13. november 2023 05:12
Za: mitja@virtual.si
Zadeva: Vračilo plačila



Prevare s plačilnimi karticami

PRIMER PREVARE – „MIMOVJRSTE“



Screenshot of the mimovrste.com/si/bill.php page. The page shows a checkout form with fields for Name, Surname, E-mail, Telephone, Address, City, and Postal Code. A red button labeled "NADALJUJ" (Continue) is visible at the bottom of the form.

Navigation links: Sledenje naročila, Osebni prevzem in dostava, Vračila in reklamacije, Kontakt, mimovrste=) partner

Search bar: Iskanje blaga...

Progress bar: 1 Prijavljeni > 2 Podatki za obračun > 3 Kartica

Form fields:

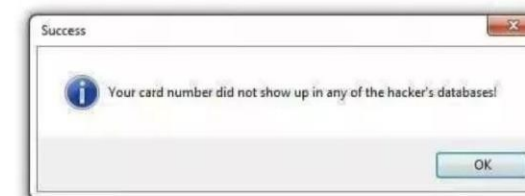
- Ime
- Preimek
- Vaš e-naslov
- Telefon
- Ulica in hišna št.
- Mesto
- Poštna številka

Red button: NADALJUJ

Footer text: pvina mimovrste=). Na mimovrste=) si zelo prizadevamo objavljati samo preverjene in pravilne podatke; če na naši strani odkrijete neresnične oziroma neustrezne informacije, nas kontaktirajte preko kontaktnega obrazca. Fotograf zagotovili ažurne in točne fotografije izdelkov, lahko zgodi, da je fotografija izdelka napačna ali stara. V tem primeru bo mimovrste=) kupcu omogočil odstop od nakupa.

Prevare s plačilnimi karticami

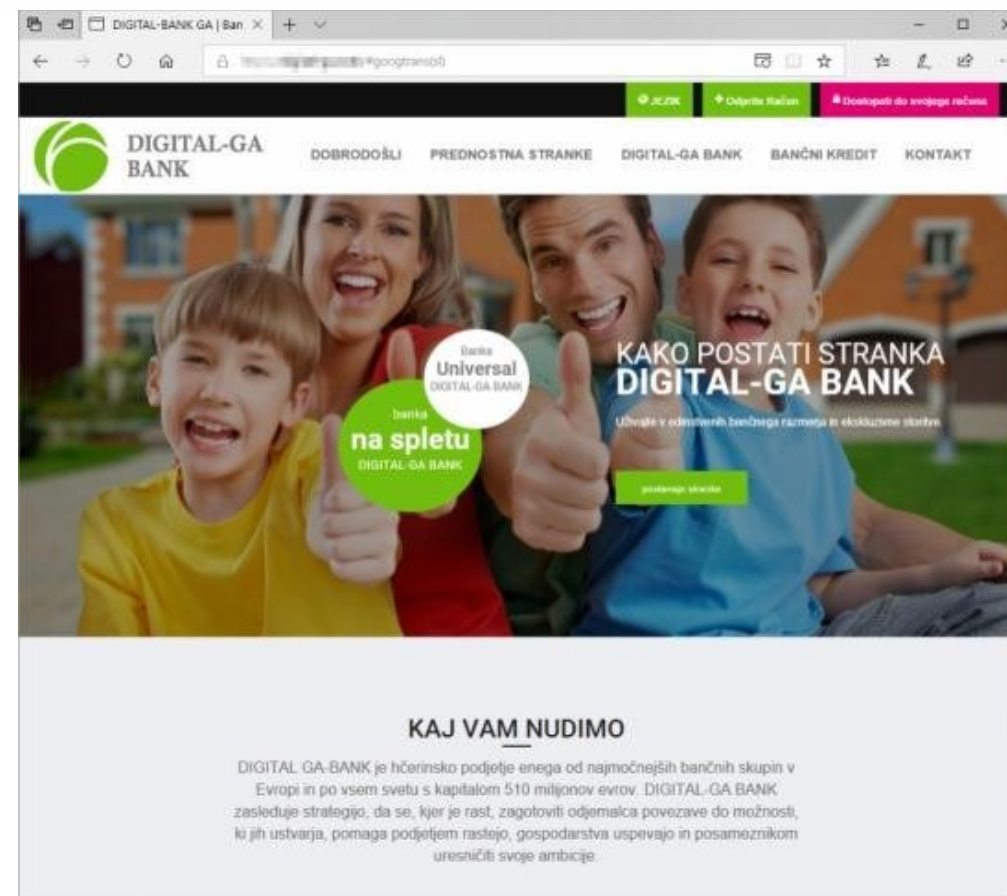
Prevaranti se poslužujejo različnih tehnik, da bi pridobili podatke o naših bančnih in kreditnih karticah. Primer prikazuje brezplačno in lažno aplikacijo s katero naj bi preverili ali je naša kartica v bazi hekerjev.



Lažni spletni krediti

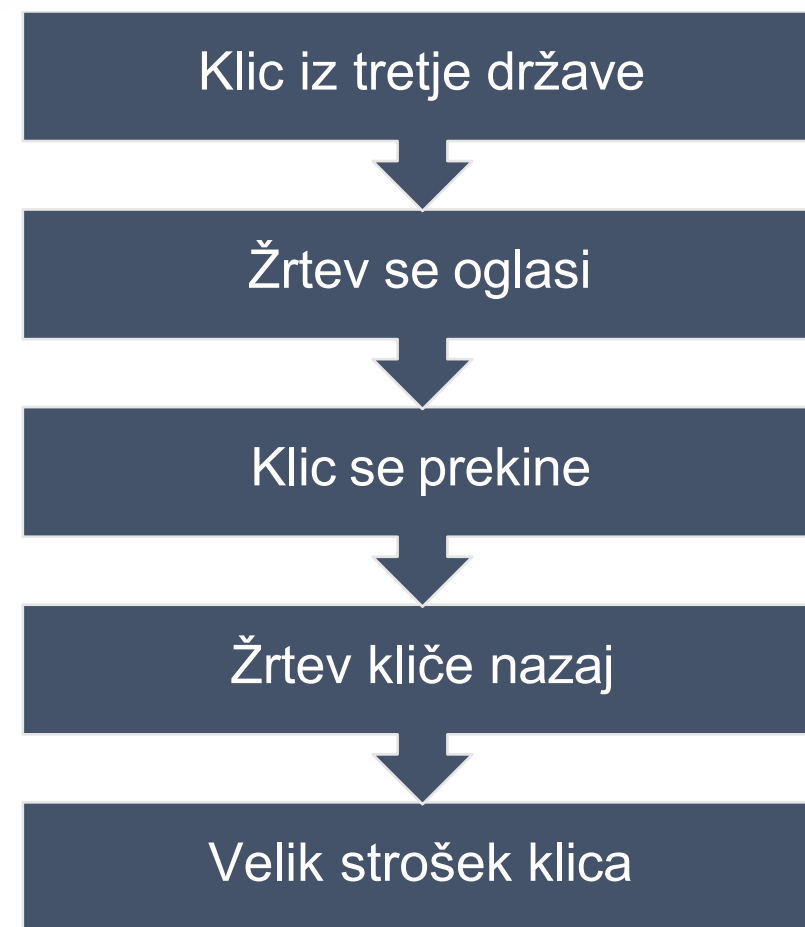
Na spletu so vse številčnejše ponudbe za ugodne kredite, ki pa posledično vodijo še v večjo stisko in finančno škodo.

Pri teh prevarah skoraj vedno pride do kraje osebnih podatkov, saj lažne banke od nas zahtevajo veliko osebnih podatkov, tudi kopijo osebnih dokumentov in morda še digitalni certifikat. Lahko pa pride tudi do finančne škode, ko od nas zahtevajo plačilo stroškov odobritve kredita, pristojbine ... še preden nam oni sploh nakažejo denar za že „odobren kredit“.



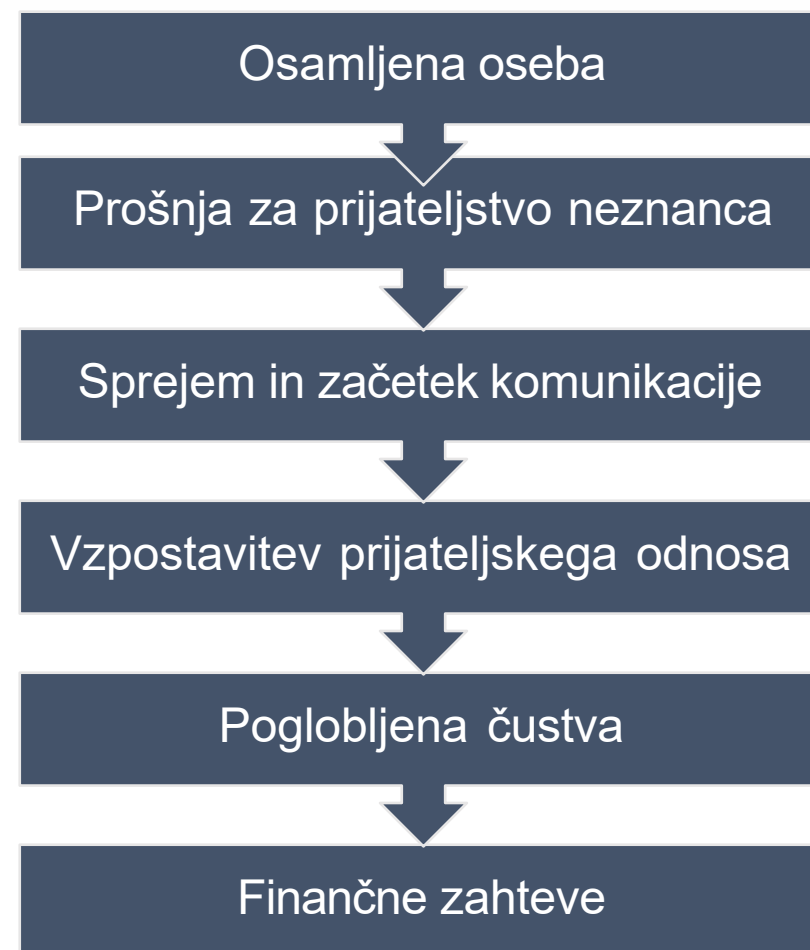
Robotizirane telefonske prevare

Poleg klasičnih telefonskih prevar, pri katerih sodelujejo fizične osebe ali napredna umetna inteligenca in so t.i. ciljan napad na organizacijo, kot del socialnega inženiringa, pa obstaja tudi robotiziran „ne ciljan“ napad, ki ga v celoti opravi stroj (bot). Ta po navadi iz predhodno določenih podatkov (država in omrežna skupina) naključno pokliče vse številke iz te baze, izključno z namenom, da prejemnik takšnega klica pokliče nazaj na njihovo plačljivo telefonsko številko, pri tem pa ima stroške.



Ljubezenske prevare na spletu

V Sloveniji vsako leto za t.i. spletne ljubezenske prevare zapravimo skoraj milijon evrov. To je uradno znan znesek, katerega vodijo organi in banke, ki so prijave prijeli od oškodovancev. Po neuradnih podatkih pa naj bi ta znesek bil nekajkrat večji, saj je oškodovance enostavno sram to prijaviti policiji in povedati svojcem.



Kaj je skupnega pri vseh teh prevarah?

Prelepo je, da bi bilo resnično.

Nasveti za zaščito

- Po telefonu ne izdajamo neznancem nobenih podatkov.
- Ne dajemo oddaljenega dostopa do računalnika neznancem.
- Uporabljamo močna gesla, ki jih vsaj na 3 mesece menjamo.
- Več faktorska avtentikacija (IT in fizično).
- Fizični dostop samo z dovolilnico in v spremstvu zaposlenega.
- Vključitev biometrije in umetne inteligence.
- Varnostni testi in redno izobraževanje zaposlenih.

Kaj je NIS2?

- NIS2 direktiva je nadgradnja prvotne direktive o varnosti omrežij in informacijskih sistemov iz leta 2016. Namenjena je izboljšanju kibernetске varnosti po vsej Evropski uniji z razširitvijo obsega in uvajanjem strožjih ukrepov za zaščito kritične infrastrukture.
- NIS2 širi obseg na več sektorjev, vključno z energetiko, transportom, zdravstvom, vodooskrbo in odpadnimi vodami, finančnimi storitvami, digitalno infrastrukturo, javno upravo in drugimi kritičnimi sektorji.

- NIS2 deli zavezance na **bistvene** in **pomembne subjekte**.
- NIS2 uvaja strožje zahteve glede upravljanja tveganj, vključno z obveznostjo sprejetja tehničnih in organizacijskih ukrepov za obvladovanje tveganj, povezanih s kibernetско varnostjo.
- Subjekti morajo poročati o večjih kibernetских incidentih v določenem časovnem okviru, kar omogoča hitrejšo odzivanje in boljše obvladovanje incidentov.

- NIS2 poudarja pomembnost sodelovanja med različnimi sektorji in državami članicami za izmenjavo informacij in ukrepanje ob kibernetiskih grožnjah.
- Direktiva NIS2 je začela veljati **16. januarja 2023**. Države članice imajo čas, da implementirajo nacionalne zakonodaje, ki bodo usklajene z zahtevami direktive, **do 17. oktobra 2024**. Do takrat morajo države članice poskrbeti, da bodo podjetja in organizacije, ki jih direktiva zadeva, izpolnjevale nove zahteve glede kibernetске varnosti.

Katere so glavne naloge za zavezance?

Ocena tveganja in upravljanje:

- Izvajanje rednih ocen tveganja za identifikacijo in analiziranje potencialnih kibernetских groženj.
- Razvijanje in vzdrževanje strategij za obvladovanje zaznanih tveganj.

Varnostni ukrepi:

- Uvedba tehničnih in organizacijskih ukrepov (npr. požarni zidovi, sistemi za odkrivanje vdorov, varnostna kopiranja, šifriranje podatkov) za zaščito omrežij ter informacijskih sistemov.
- Sprejetje ukrepov za preprečevanje motenj in ohranjanje kontinuitete poslovanja.

Poročanje o incidentih:

- Vzpostavitev postopkov za hitro odkrivanje, obvladovanje in poročanje o kibernetских incidentih.
- Poročanje o vseh pomembnih kibernetских incidentih ustreznim nacionalnim organom v določenem časovnem okviru.

Izobraževanje in usposabljanje:

- Redno izobraževanje in usposabljanje zaposlenih glede kibernetске varnosti in obvladovanja incidentov.
- Spodbujanje ozaveščenosti zaposlenih o potencialnih kibernetских grožnjah.

Sodelovanje in izmenjava informacij:

- Aktivno sodelovanje z nacionalnimi organi za kibernetско varnost in drugimi zavezanci.
- Soudeležba pri skupnih pobudah za izboljšanje kibernetске varnosti in delitev informacij o grožnjah in incidentih.

Redni pregledi in testiranje:

- Redno preverjanje in testiranje učinkovitosti sprejetih varnostnih ukrepov.
- Izvajanje kriznih vaj in simulacij kibernetских napadov za preverjanje pripravljenosti na incidente.

Usklajevanje z nacionalnimi pravnimi okviri

- Prilagoditev interno sprejetih ukrepov z nacionalnimi zakoni in predpisi o kibernetiski varnosti, ki so sprejeti na osnovi direktive.
- Redno spremljanje sprememb v zakonodaji in prilagajanje varnostnih politik temu.

Upravljanje dobavne verige:

- Zagotavljanje, da tudi dobavitelji in poslovni partnerji izpolnjujejo določene standarde kibernetске varnosti.
- Vključitev določil o kibernetски varnosti v pogodbe in sodelovanja z zunanjimi izvajalci.

Prilagoditev potrebam direktive NIS2 zahteva celovit pregled obstoječih praks kibernetске varnosti in morebitne spremembe v organizacijski strukturi ter politiki podjetja. Ključno je, da zavezanci razvijejo **proaktiven pristop k obvladovanju kibernetске varnosti**, ki je usklajen z regulativnimi zahtevami in najboljšimi praksami v industriji.

Hvala za sodelovanje!