USPOSABLJAMO IN PRILAGAJAMO
TRAINING AND ADJUSTMENT
NOO | NAČRT ZA OKREVANJE IN ODPORNOST
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DELO, DRUŽINO, SOCIALNE ZADEVE IN ENAKE MOŽNOSTI
Financira Evropska unija
NextGenerationEU

Kibernetska varnost

Predavatelj: dr. Miha Dvojmoč
Naročnik: GRIFFIN d.o.o.
Izvajalec: MD svetovanje d.o.o.
Datum: 13. 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.

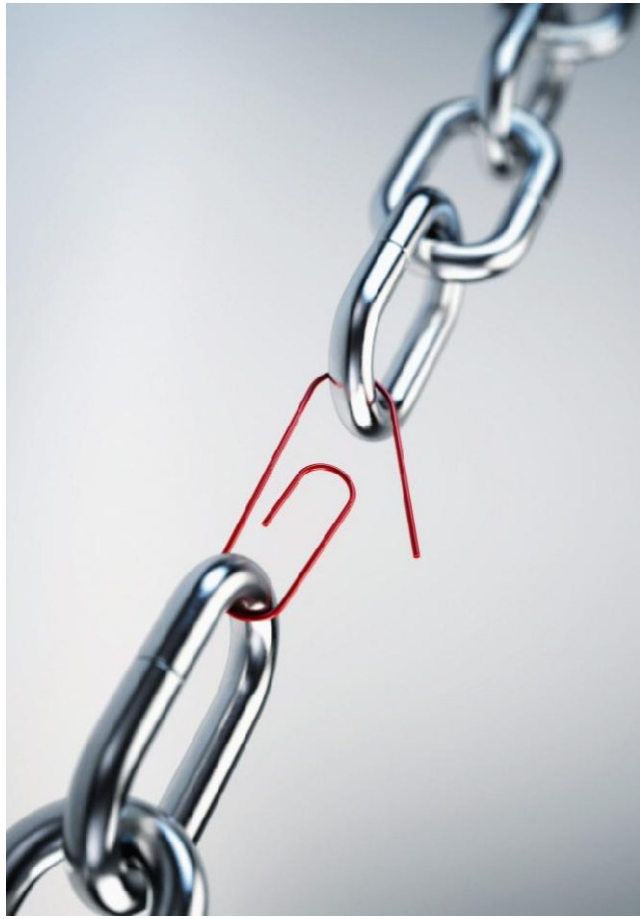
Socialni inženiring predstavlja resno grožnjo za IT-varnost, saj se zanaša na človeški element, ki je pogosto najšibkejši člen v varnostnem sistemu. Izkorišča človeška čustva in lastnosti, kot so: zaupanje, strah, naivnost, radovednost, osamljenost in pohlep.

Iskanje najšibkejšega člena v organizaciji

Ko razmišljamo o kibernetski varnosti, nas večina pomisli na obrambo pred virusi, črvi in hekerji, 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.

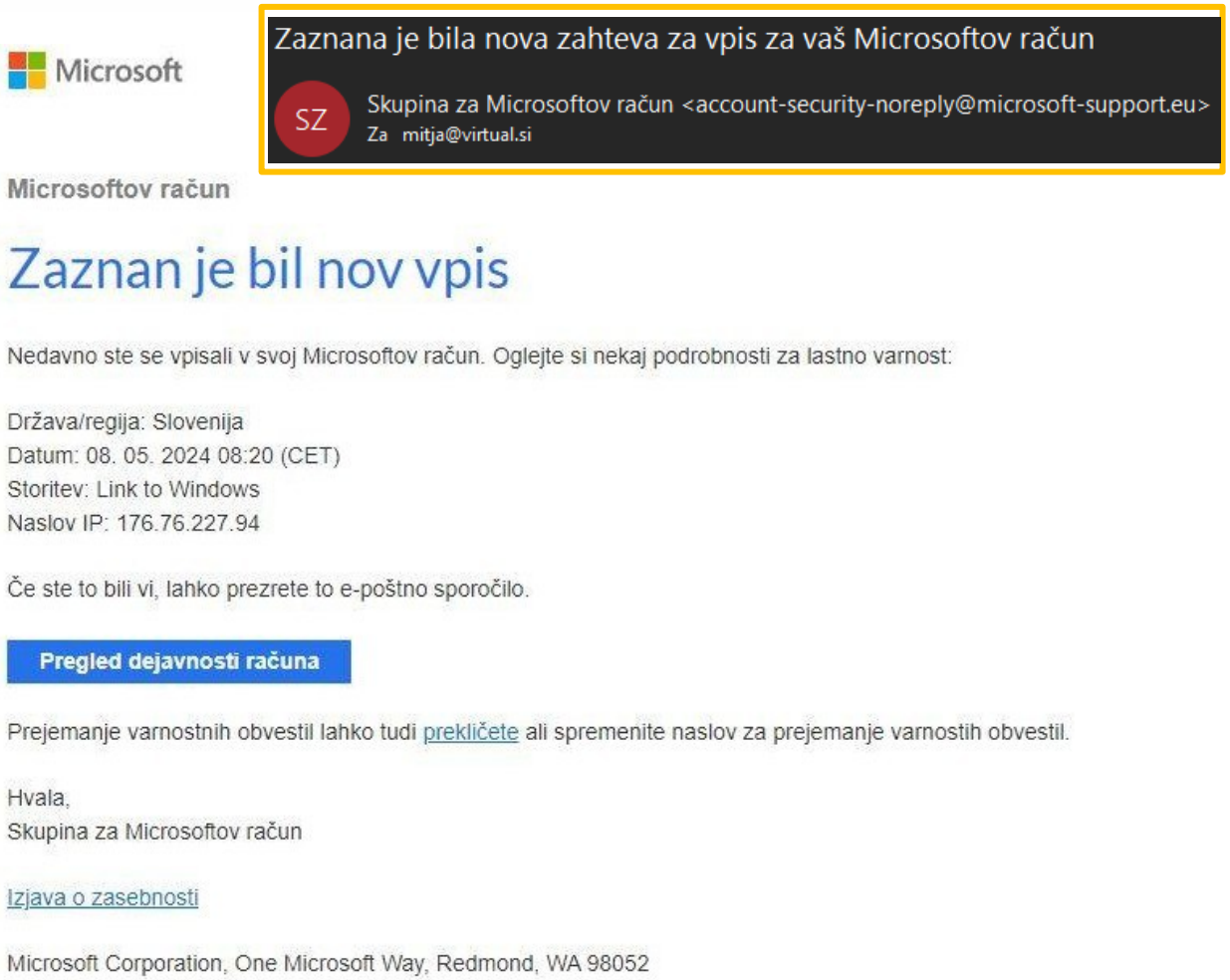
Zvabljanje – ribarjenje (phishing)

- 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.



Microsoft

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

Microsoftov račun

Zaznan 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 varnostih obvestil.

Hvala,
Skupina za Microsoftov račun

Izjava o zasebnosti

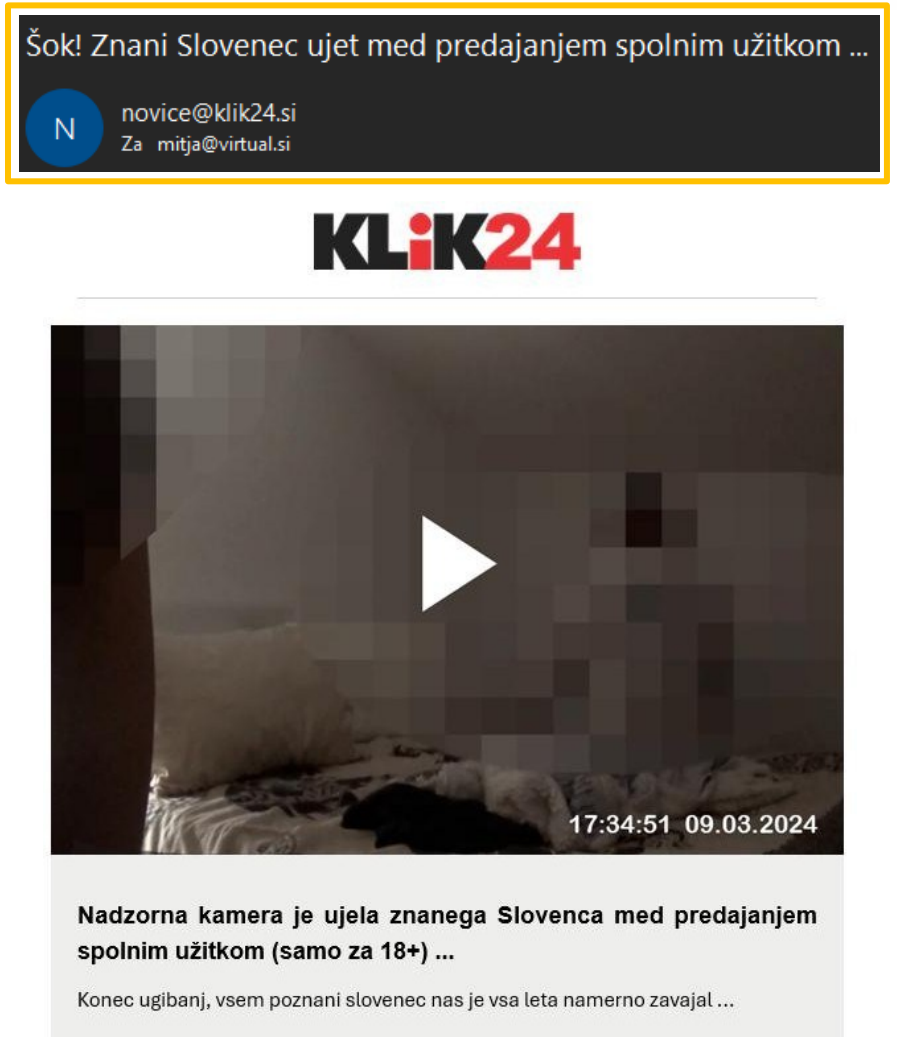
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Prevare prekoE-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**



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 ...

Serum mladosti po znižani ceni!

Več informacij ...

IZBERITE TERMIN

Pranje in voskanje vozila za 9,90 EUR

Več informacij ...

RE:RE: Naročilo M-HTECH

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

MATALJ Ponuda 30.05 2024 SMKTGTECH6346674788748738459853098O2Thayne.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,

MATALJ

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)

AV 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

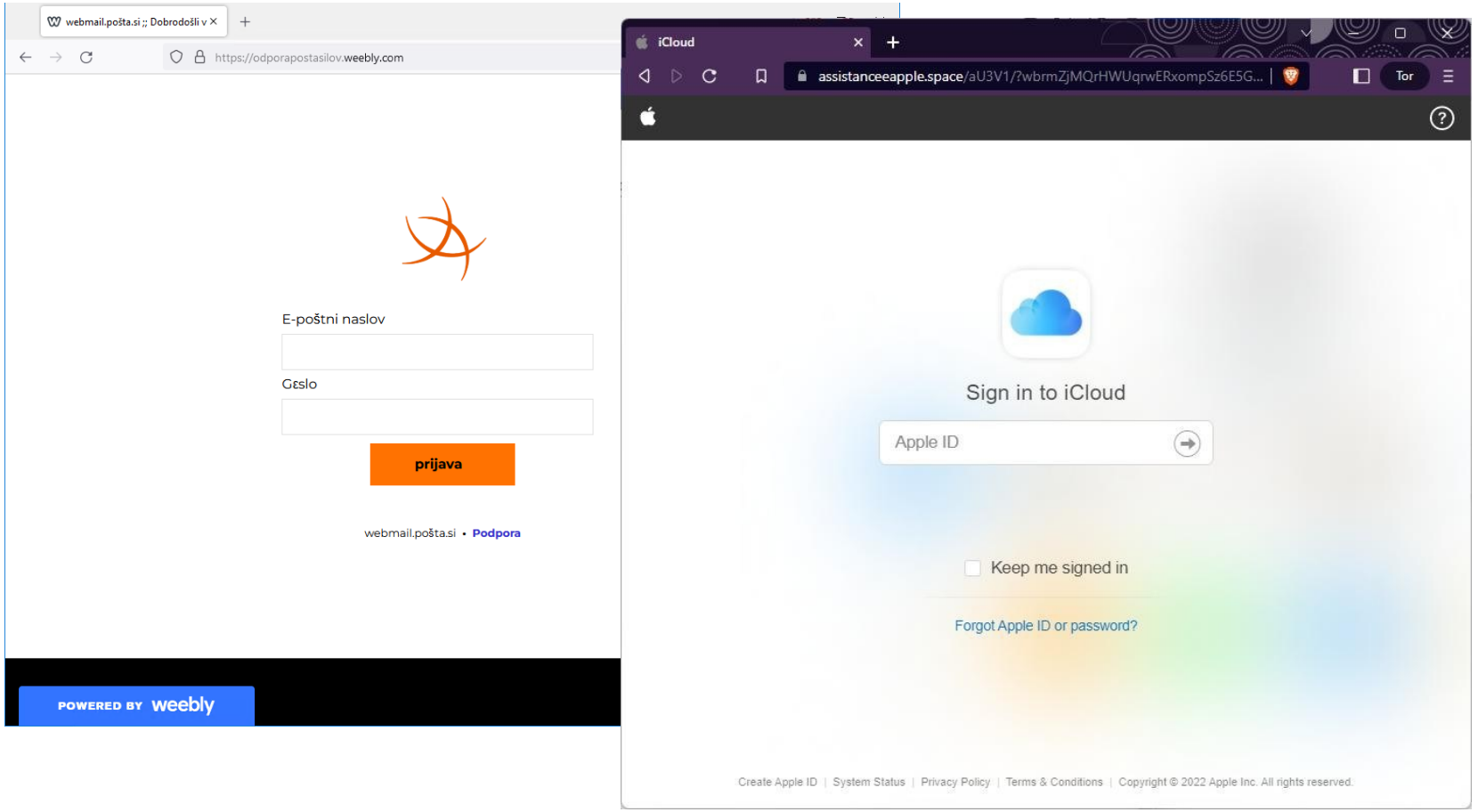
Livarna Titan doo Kovinarska cesta 28, SI-1240 Kamnik, Slovenia, www.livarna-titan.eu

LIVARNA TITAN KAMNIK

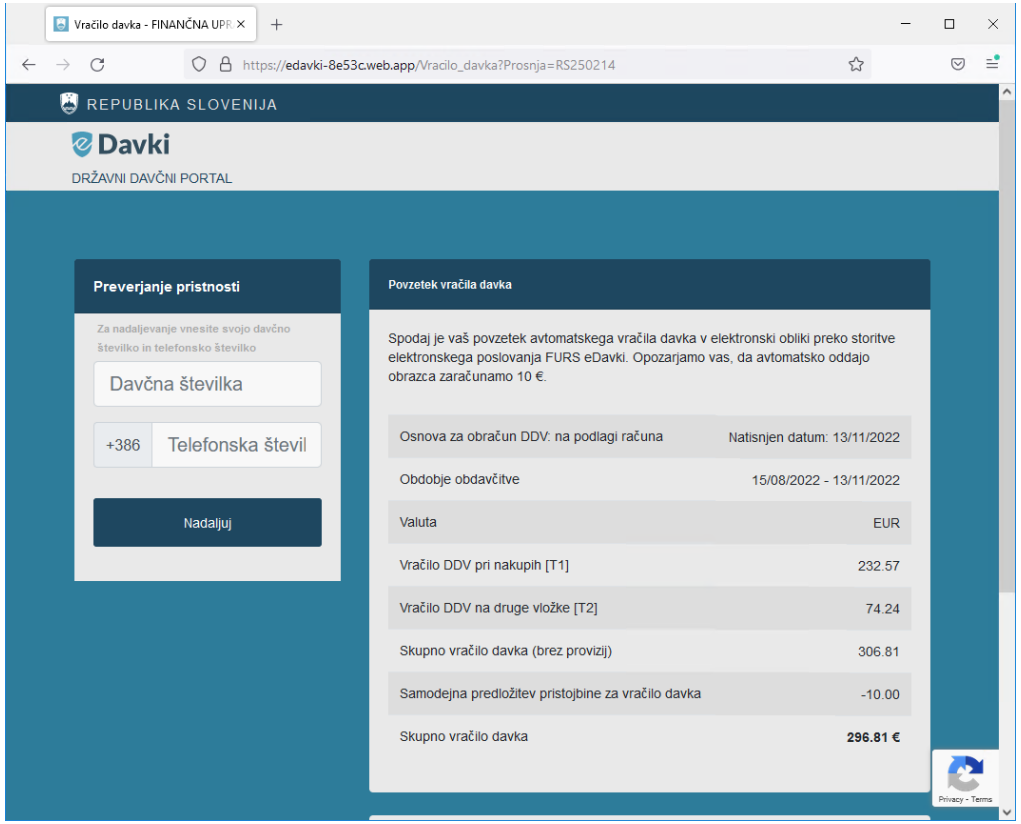
Livarna od 1920 · Foundry since 1920

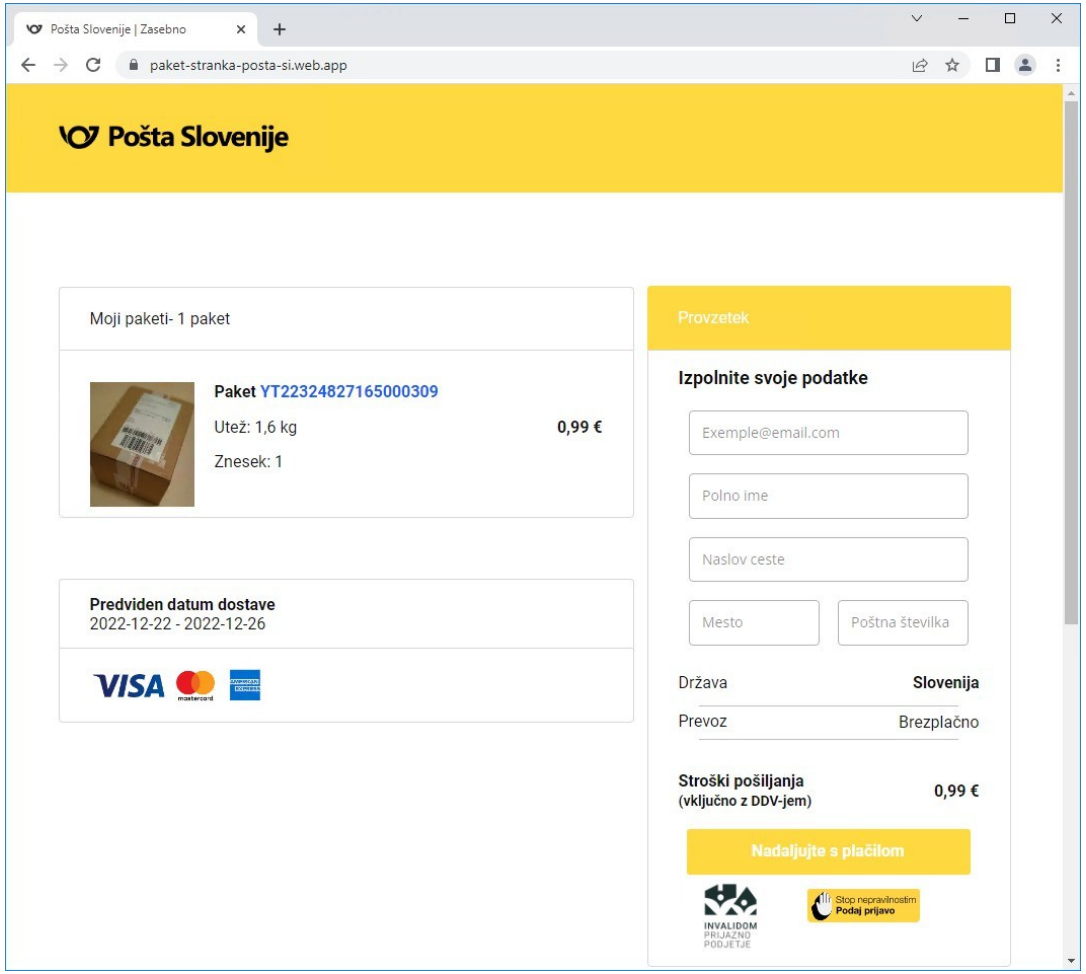
Lažne spletne strani

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

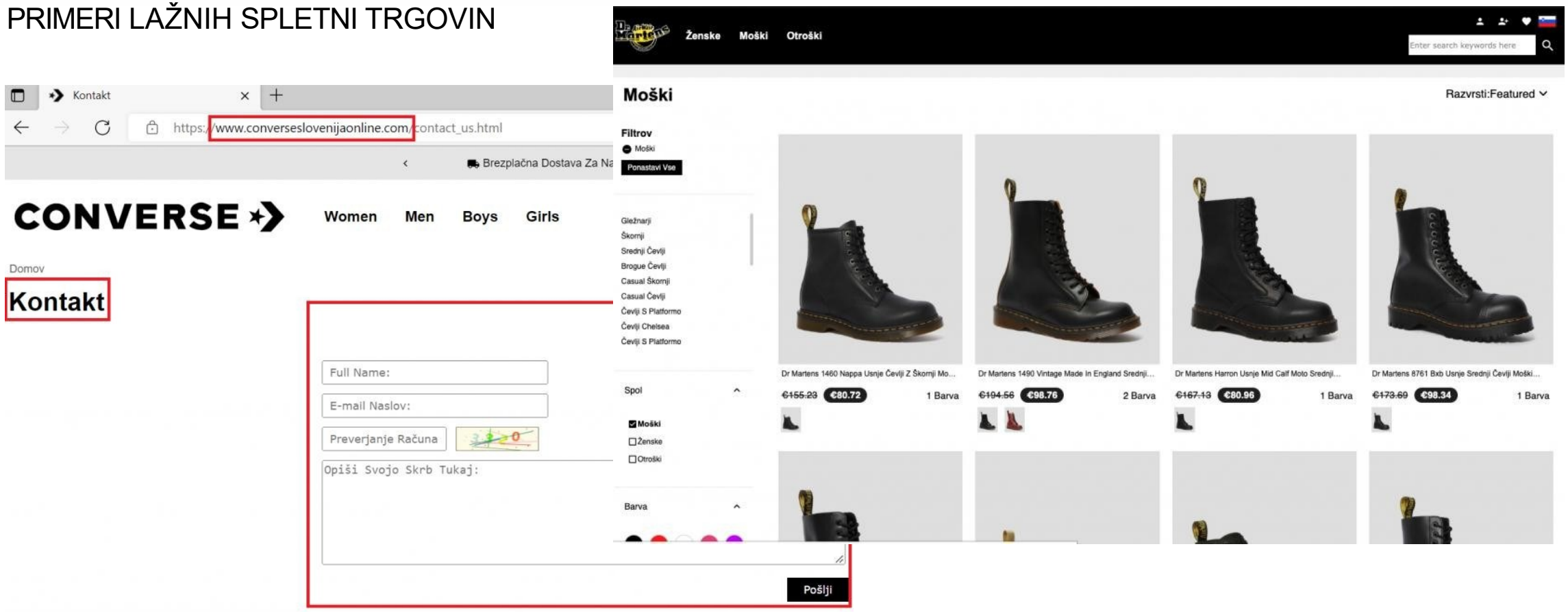


PRIMERI LAŽNIH SPLETNI STRANI





PRIMERI LAŽNIH SPLETNI TRGOVIN

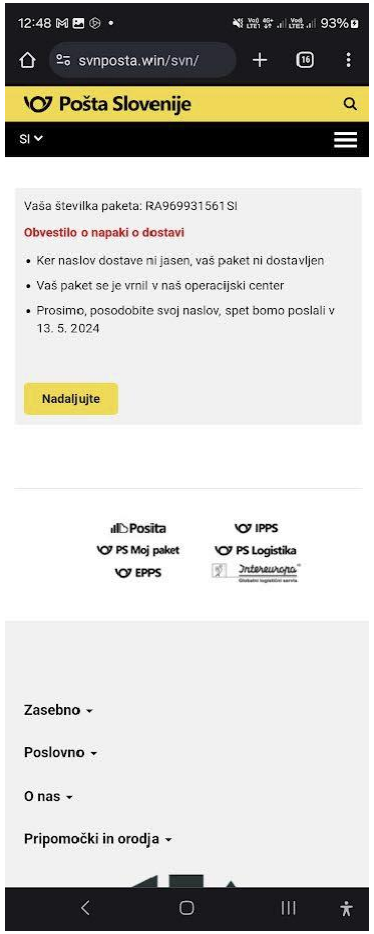


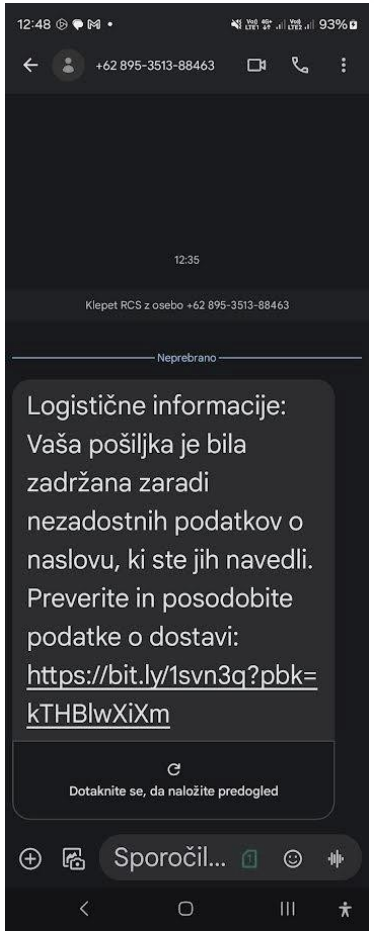
Prevare preko SMS sporočil

PRIMER PREVARE – „POŠTA SLOVENIJE“

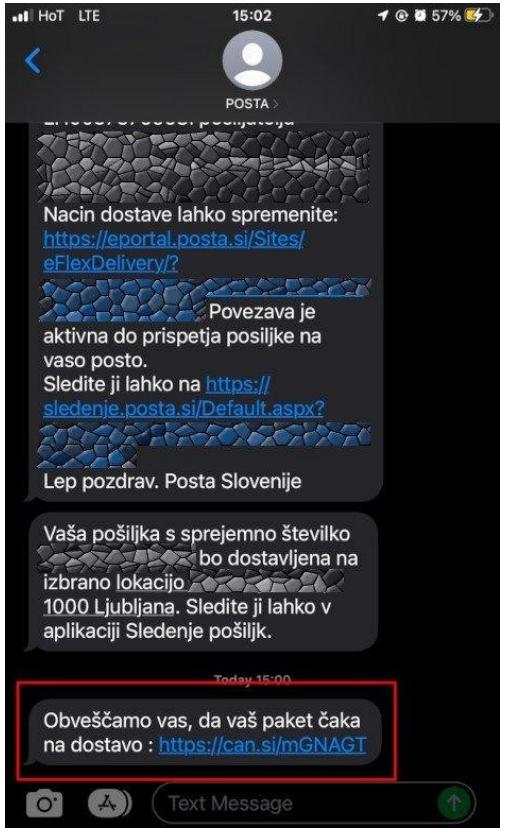
Hekerji oziroma prevaranti se poslužujejo tudi komunikacije preko SMS sporočili z namenov:

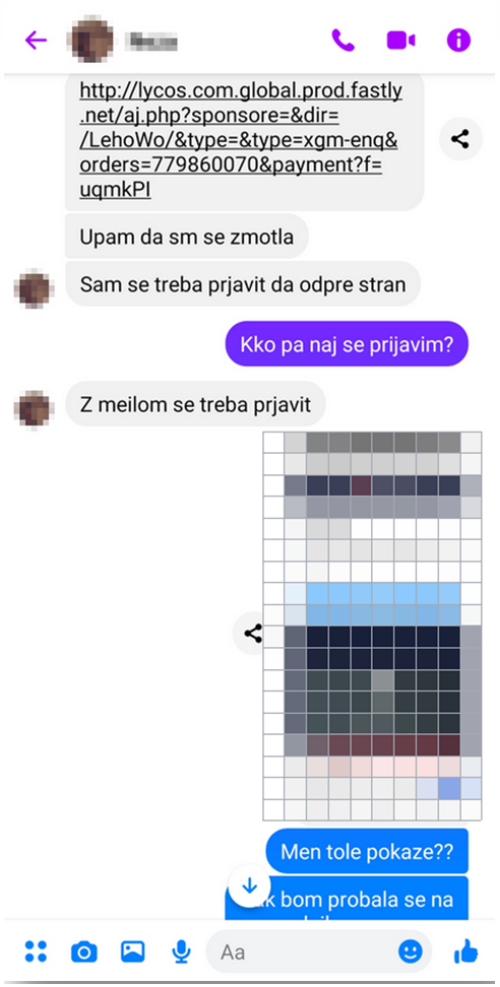
- pridobiti podatke o plačilni kartici;
- namestiti zlonamerno programsko kodo za dostop do telefona (kraja podatkov in kasneje izsiljevanje).





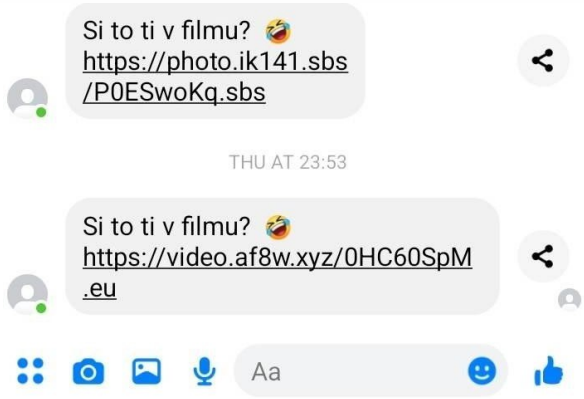
PRIMERI LAŽNIH SMS SPOROČIL





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.

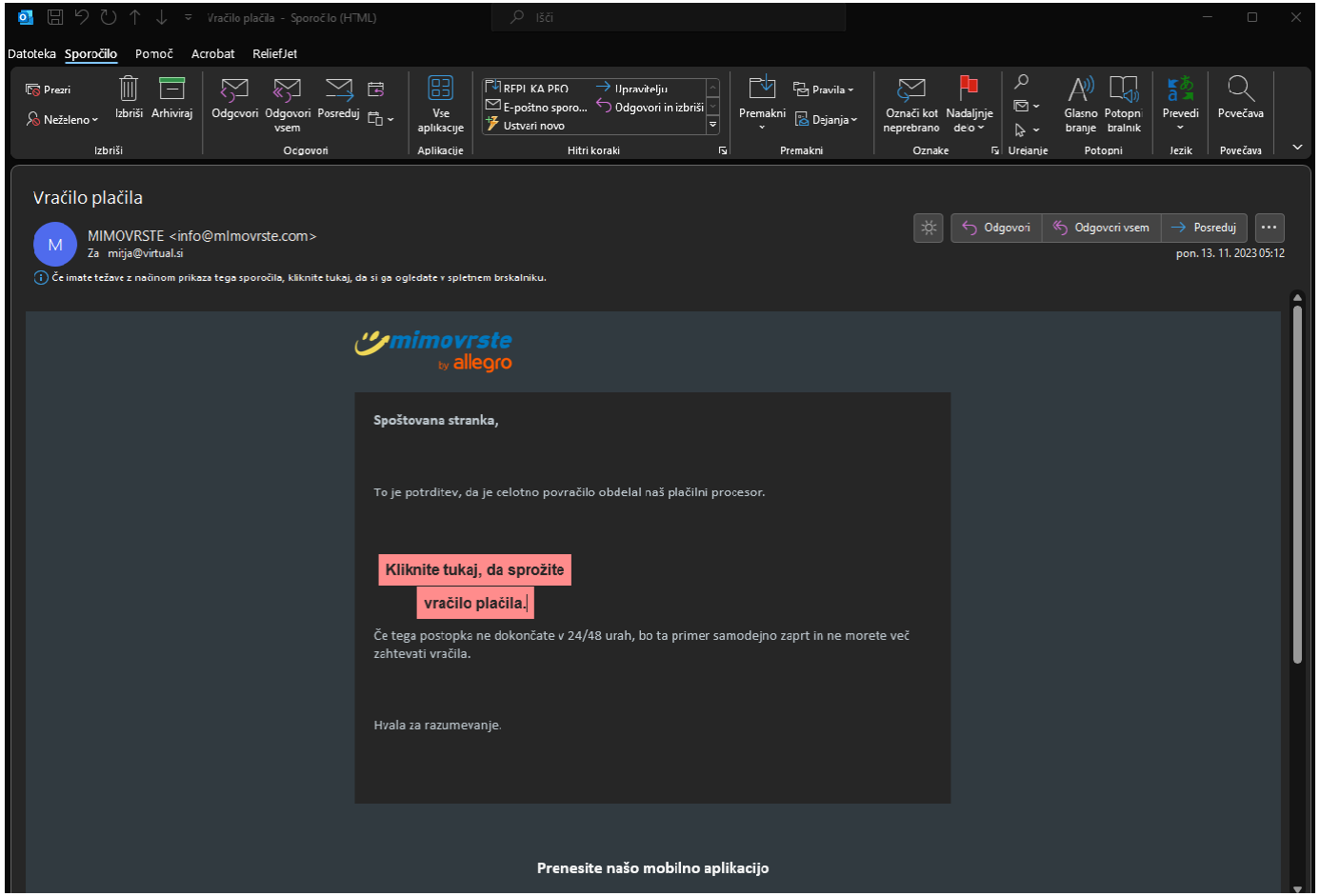
Prevare (scam, fraud ...)

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

Prevare s plačilnimi karticami

PRIMER PREVARE – „MIMOVRSTE“

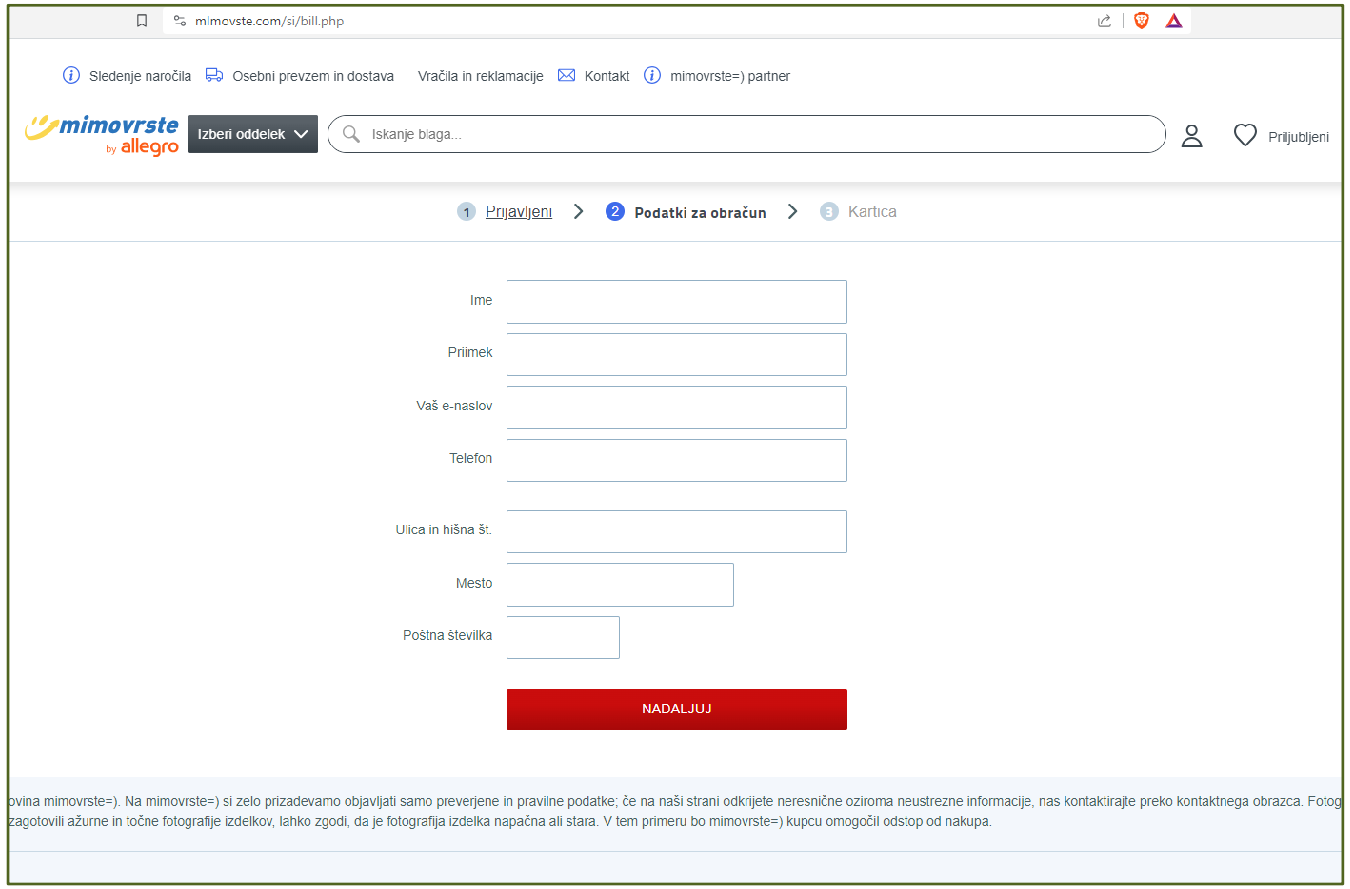
Od: MIMOVRSTE <info@mlmovrste.com>
Poslano: ponedeljek, 13. november 2023 05:12
Za: mitja@virtual.si
Zadeva: Vračilo plačila



Prevare s plačilnimi karticami

PRIMER PREVARE – „MIMOVRSTE“

https://mlmovste.com/si/bill.php



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.

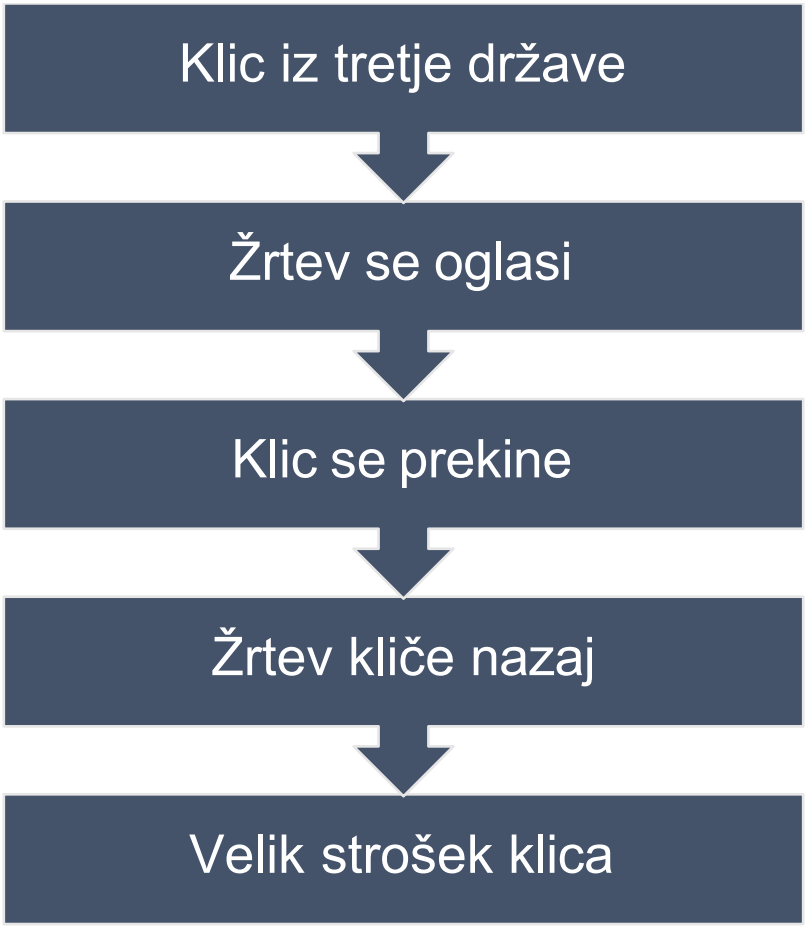
Lažni spletni krediti

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".

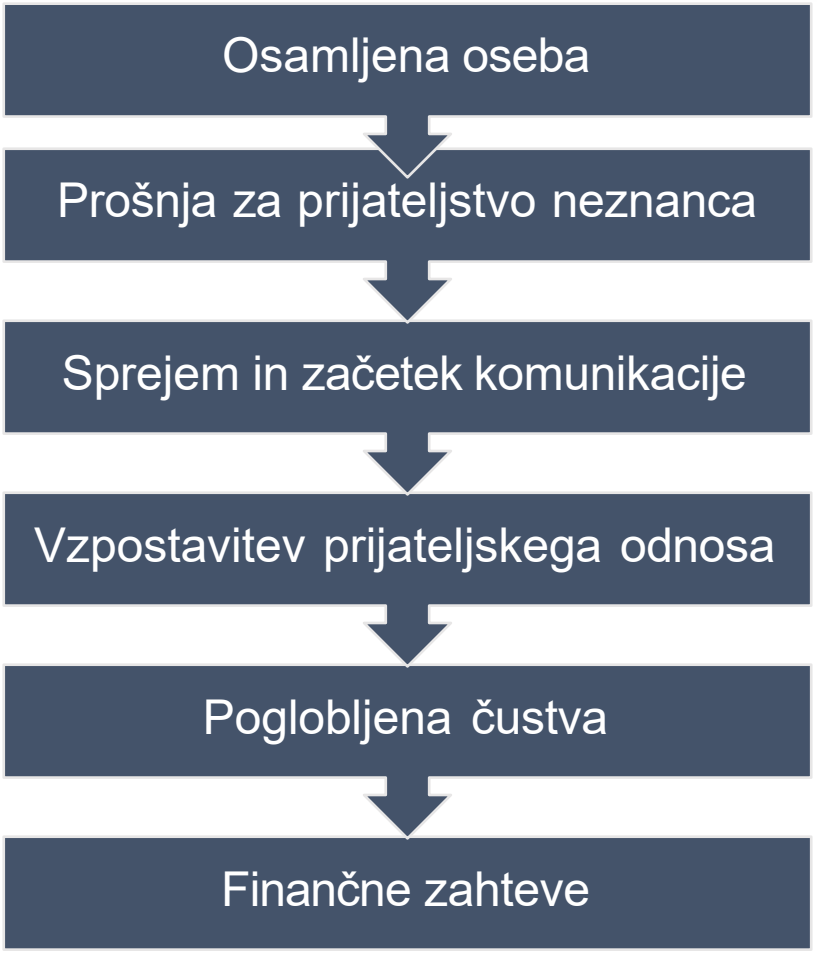
Robotizirane telefonske prevare

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 kibernetske 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 kibernetsko varnostjo.
- Subjekti morajo poročati o večjih kibernetskih incidentih v določenem časovnem okviru, kar omogoča hitrejše odzivanje in boljše obvladovanje incidentov.

- NIS2 poudarja pomembnost sodelovanja med različnimi sektorji in državami članicami za izmenjavo informacij in ukrepanje ob kibernetskih 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 kibernetske varnosti.

Katere so glavne naloge za zavezance?

Ocena tveganja in upravljanje:

- Izvajanje rednih ocen tveganja za identifikacijo in analiziranje potencialnih kibernetskih 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 kibernetskih incidentih.
- Poročanje o vseh pomembnih kibernetskih incidentih ustreznim nacionalnim organom v določenem časovnem okviru.

Izobraževanje in usposabljanje:

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

Sodelovanje in izmenjava informacij:

- Aktivno sodelovanje z nacionalnimi organi za kibernetsko varnost in drugimi zavezanci.
- Soudeležba pri skupnih pobudah za izboljšanje kibernetske 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 kibernetskih napadov za preverjanje pripravljenosti na incidente.

Usklajevanje z nacionalnimi pravnimi okviri

- Prilagoditev interno sprejetih ukrepov z nacionalnimi zakoni in predpisi o kibernetski 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 kibernetske varnosti.
- Vključitev določil o kibernetski varnosti v pogodbe in sodelovanja z zunanjimi izvajalci.

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

USPOSABLJAMO IN PRILAGAJAMO
TRAINING AND ADJUSTMENT

NAČRT ZA OKREVANJE IN ODPORNOST

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DELO, DRUŽINO, SOCIALNE ZADEVE IN ENAKE MOŽNOSTI

Financira Evropska unija
NextGenerationEU

Hvala za sodelovanje!

WWW.VARNOST-IT.SI

WWW.INFOCENTER.SI