EUROPEAN UNION AGENCY
FOR CYBERSECURITY

SOCIALNI INŽENIRING IN DIREKTORSKE PREVARE

VSEBINA

Socialni inženiring

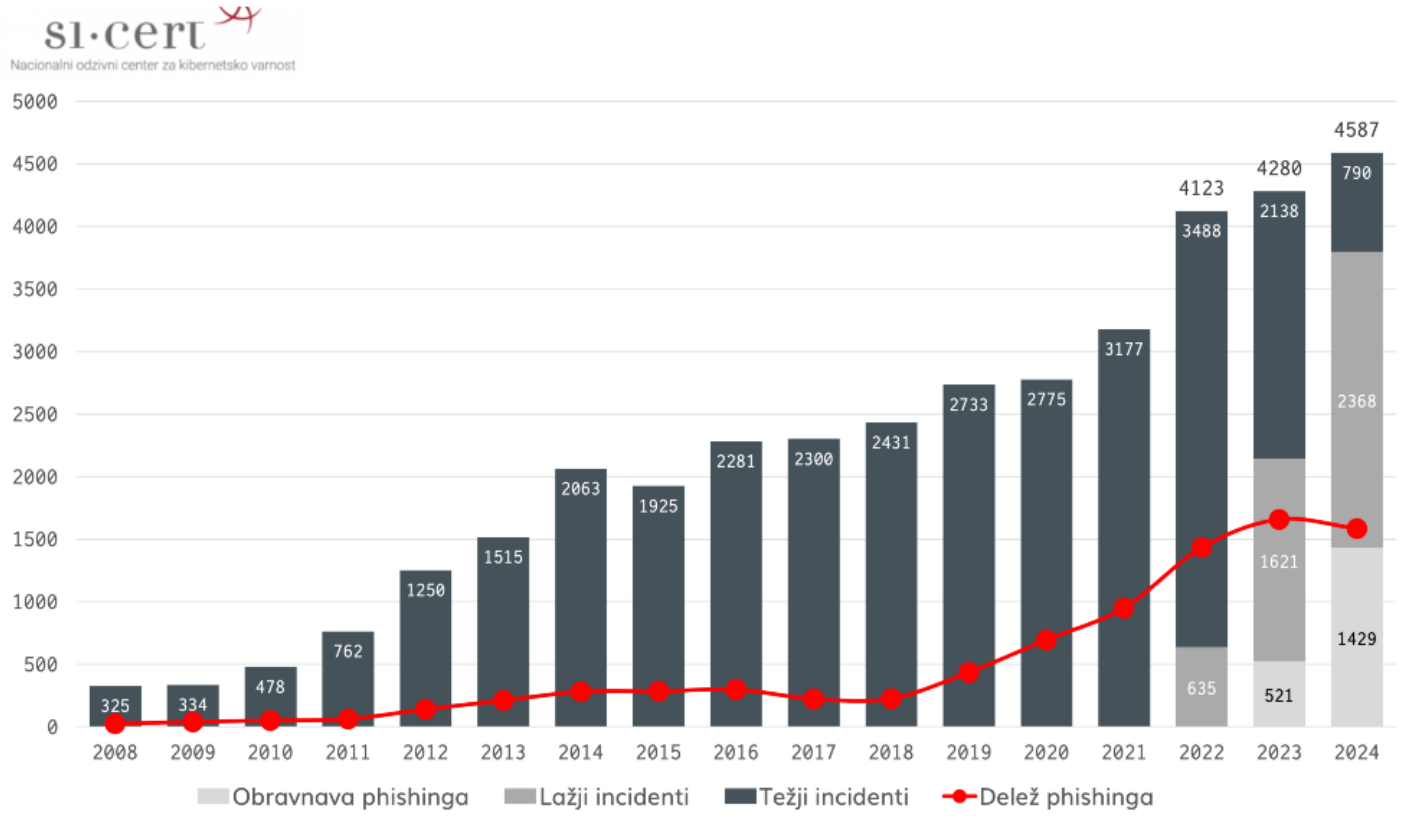
- Kaj je socialni inženiring
- Potek napada
- Vrste

Direktorska (ang. CEO) Prevara

- Znaki
- Potek
- Zaščita

KAJ JE SOCIALNI INŽENIRING

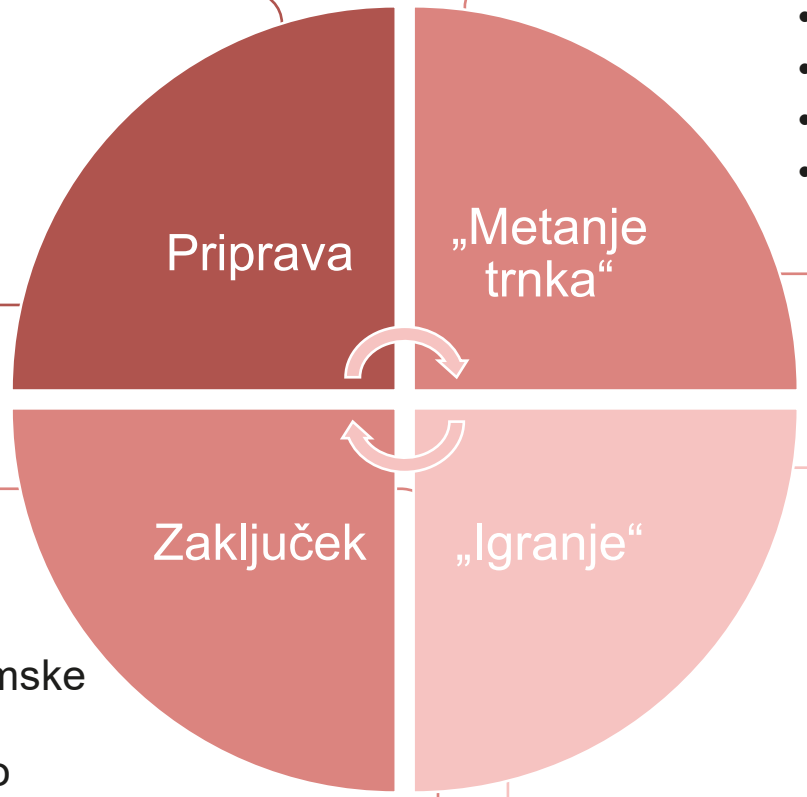
Socialni inženiring je niz tehnik, s katerimi napadalci manipulirajo uporabnike, da razkrijejo občutljive informacije ali izvedejo dejanja, ki ogrožajo varnost informacijskih sistemov.



Vir: Poročilo o kibernetski varnosti za leto 2024 - SI CERT

POTEK NAPADA

- Identifikacija tarč,
- zbiranje informacij,
- izbira metode za izvedbo.



- Prva komunikacija,
- predstavitev zgodbe,
- vzpostavitev zaupanja,
- nadzor nad interakcijo.

- Zakrivanje sledi,
- izbris sledi zlonamerne programske opreme,
- brez suma tarče, da je prišlo do izkoriščanja.

- Izvedba napada,
- zbiranje dodatnih informacij,
- dodatne tarče,
- oviranje poslovanja.

TIPI SOCIALNEGA INŽENIRINGA

Katere tipe socialnega inženiringa poznamo?

Vir: SI-CERT, Varni na internetu

Spletno ribarjenje (ang. *phishing*),
Pretvarjanje *(ang. pretexting)*,

Izmišljena zgodba, pridobitev zaupanja → občutljiva informacija.

Zvabljanje (ang. *baiting*),

Darilna kartica, brezplačen prenos datotek v zameno za osebne podatke.

Nekaj za nekaj *(ang. quid pro quo)*,

Nagrada v zameno za občutljive informacije (nekaj za nekaj – IT podpora)

Strašilna programska oprema (ang. *scareware*),

Okužen računalnik, ponudba lažnega programa za odstranitev.

Sledenje *(ang. tailgating)*

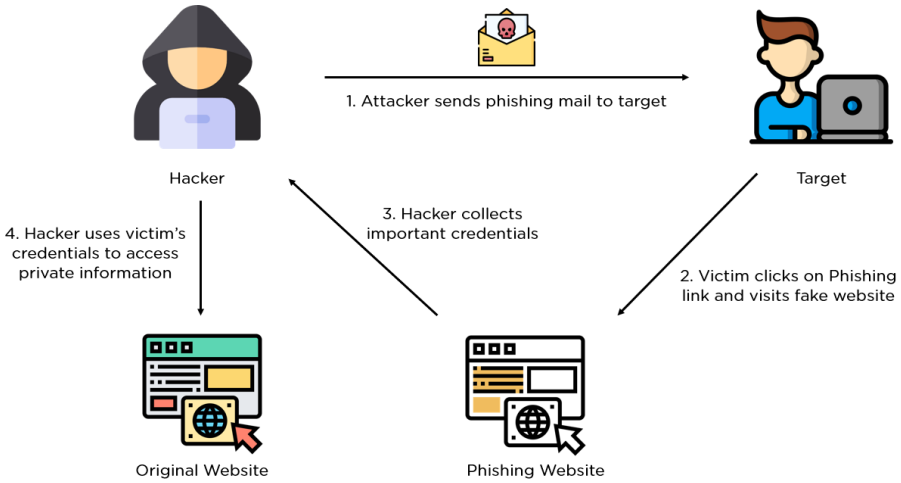
Sledenje legitimiranim osebam pri vstopu v objekt (kurir, stranka, vzdrževalec…).

TIPI SPLETNEGA RIBARJENJA

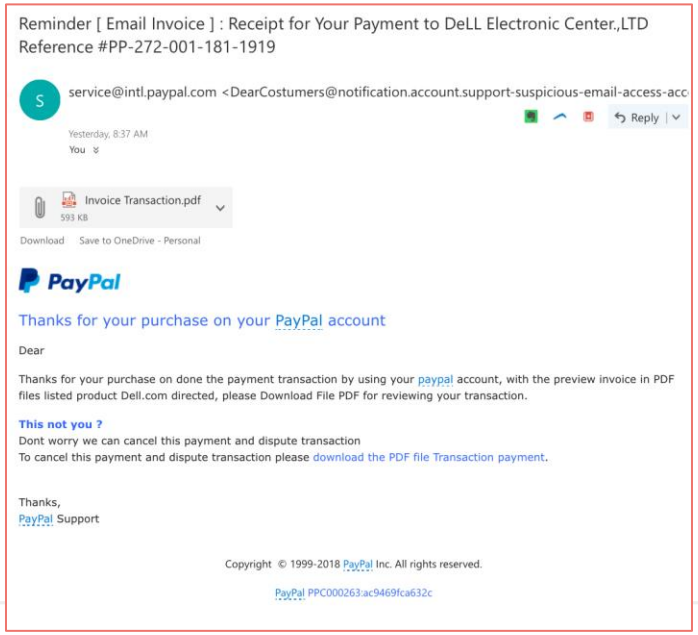
Katere tipe spletnega ribarjenja poznamo?

- E-poštno spletno ribarjenje (ang. phishing),
- SMS ribarjenje (ang. smishing),
- Usmerjen napad (ang. spear phishing),
- Glasovno ribarjenje (ang. vishing),
- Uporaba QR kode (ang. quishing)
- Ponaredek legitimnega e-poštnega naslova/spletne strani z zlonamerno vsebino (ang. clone phishing),
- Napad usmerjen na vodstvo (ang. whailing).

Vir: SI-CERT, Varni na internetu



Vir: What is Phishing Attack in Cyber Security - Complete Guide



Vir: https://ivarnost.si/spletne-goljufije-phishing-v-imenu-halcoma/?

PRIMERI SPLETNEGA RIBARJENJA

Vir: https://www.varninainternetu.si/klici-lazne-microsoftove-tehnicne-pomoci/

Vir: https://sosafe-awareness.com/glossary/quishing/

Zadeva: Obvestilo – napaka pri podpisovanju plačilnih nalogov
Datum: Wed, 12 Nov 2025 10:16:33 +0000
Od: Halcom d.d. <info@halcom-varnost.com>
Za:

Spoštovani,

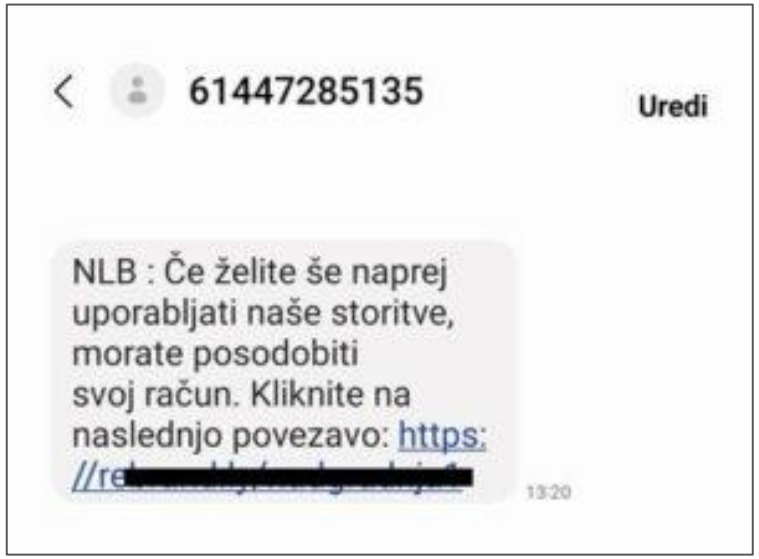
po zadnji nadgradnji sistema Windows je prišlo do napake pri podpisovanju plačil.
Napako odpravite z namestitvijo datoteke po navodilih na varni povezavi:

👉 **Odpravi napako tukaj**

Datoteko namestite **izključno** iz aplikacije **Hal E-Bank**. Namestitev iz drugih virov lahko pomeni zlorabo.

Lep pozdrav,
HALCOM PODPORA

Vir: https://ivarnost.si/spletne-goljufije-phishing-v-imenu-halcoma/



Vir: smishing banka - Varni na interhttps://www.varninainternetu.si/top-10-izgovorov-spletnih-goljufov-v-letu-2024/smishing-banka-2/netu

Vir: https://cofense.com/blog/threat-actors-taking-advantage-of-hr-initiatives/s

5 KOMPONENT SOCIALNEGA INŽENIRINGA

- **Avtoriteta** (banke, zavarovalnice ipd.),
- **Družbeni pritisk** (XY mi je že posredoval podatke),
- **Strah pred izločitvijo** (če ne ukrepaš, boš zamudil super priložnost…),
- **Nujnos**t (nagrado moraš prevzeti v 24 urah),
- **Zaupanje** (pretvarjanje privlačnosti, pridobitev zaupanja).

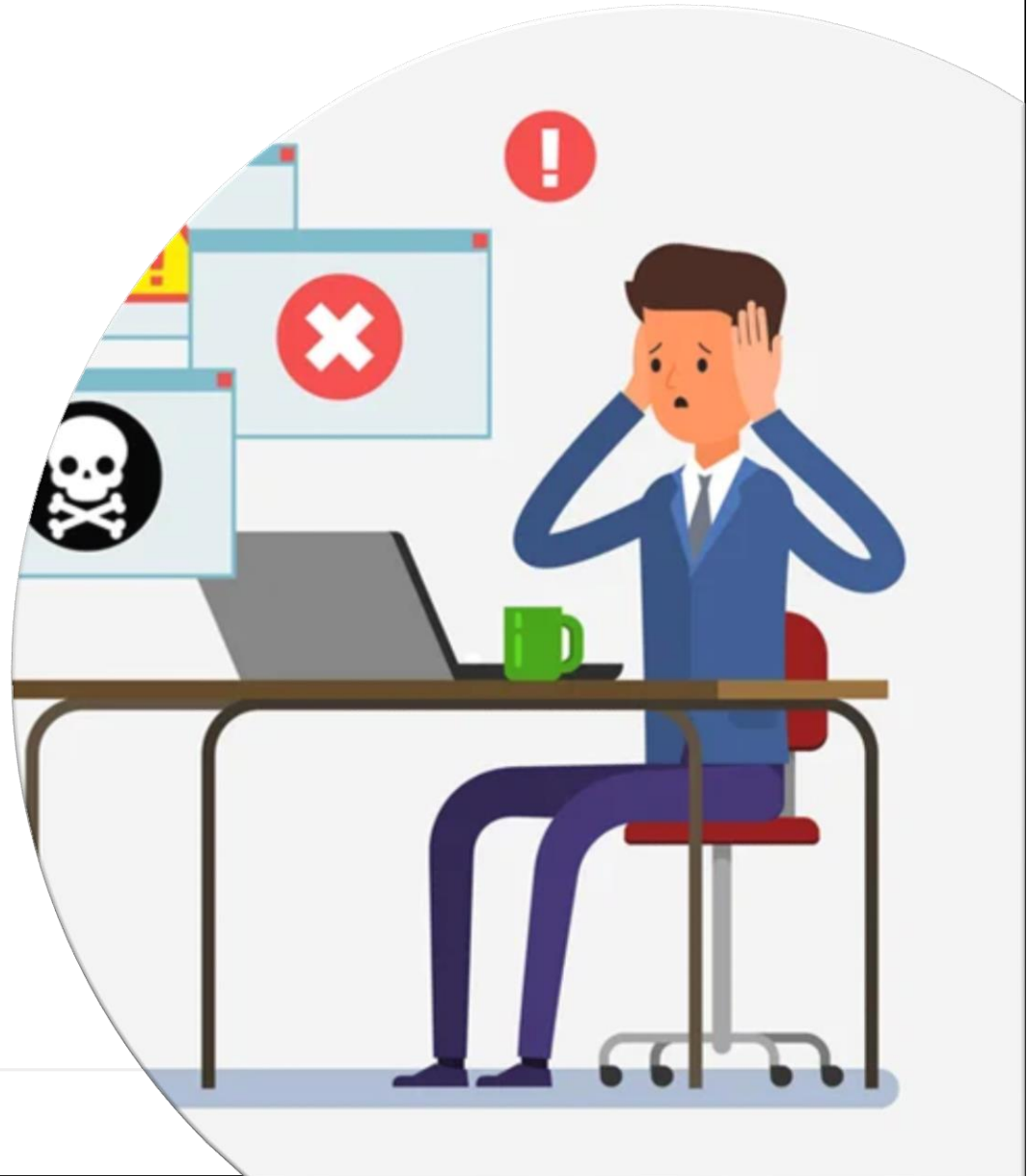
Vir: SI-CERT, Varni na internetu

Vir: https://ivarnost.si/spletne-goljufije-phishing-v-imenu-halcoma/s

USPEŠNOST PHISHINGA

Zakaj nasedemo?

- Nepazljivost,
- Trenutek nepozornosti,
- Radovednost,
- Prepričljivo sporočilo.



STRATEGIJE ZA OBRAMBO PRED SOCIALNIM INŽENIRINGOM

- Napadi ciljajo na psihologijo – obramba mora biti večplastna.
- Tehnični ukrepi + izobraževanje + psihološka pripravljenost.

Vir: SI-CERT, Varni na internetu

DIREKTORSKA (CEO) PREVARA

KAJ JE DIREKTORSKA PREVARA

Vir: https://www.policija.si/svetujemo-ozavescamo/varnost-na-internetu

Direktorske prevare, znane tudi kot **CEO fraud ali Business Email Compromise (BEC),** so oblika kibernetske prevare, pri kateri napadalci **posnemajo ali prevzamejo identiteto** višjega vodstvenega delavca (npr. direktorja ali finančnega direktorja) in **usmerjajo zaposlene**, običajno v finančnih oddelkih, da **izvedejo nepooblaščena plačila** ali prenose sredstev z namenom, da žrtev:

- izvede nujno plačilo,
- spremeni bančne podatke dobavitelja,
- posreduje zaupne finančne ali poslovne informacije

Vir: SI-CERT, Varni na internetu

KLJUČNE ZNAČILNOSTI DIREKTORSKE (CEO) PREVARE

Vir: https://powerdmarc.com/6-ways-to-stop-email-ceo-fraud/

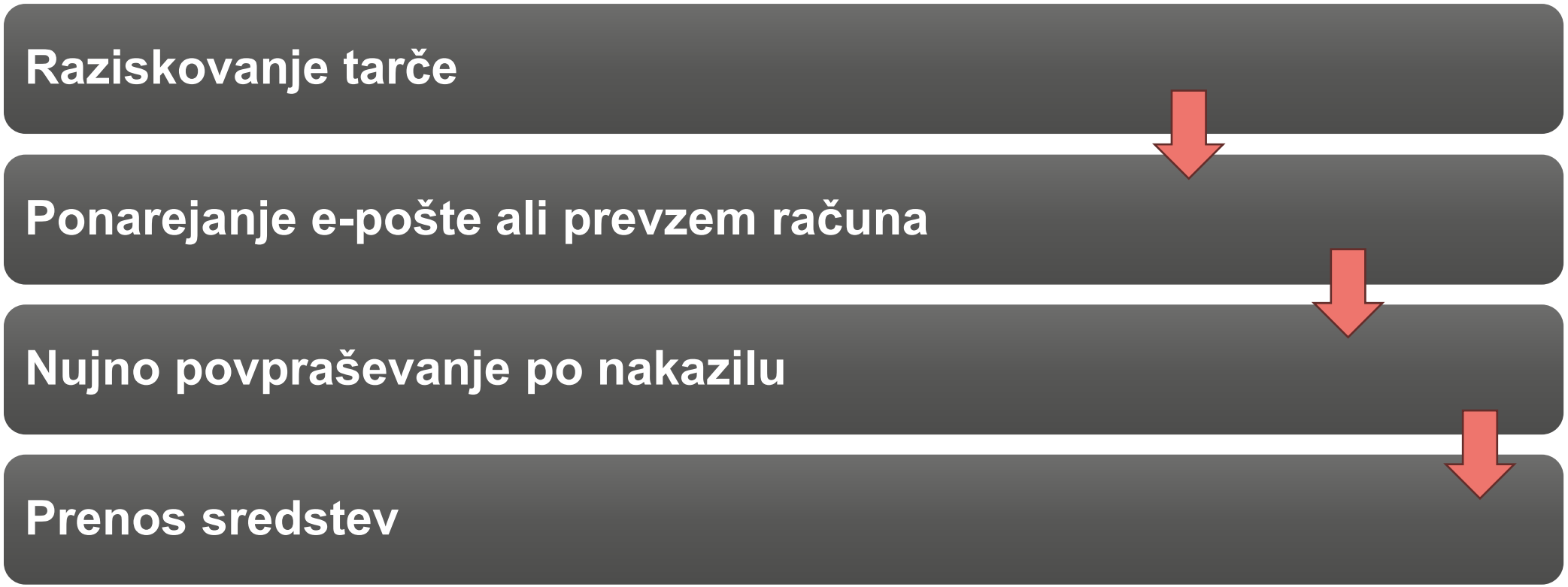
- **Lažno predstavljanje:** Napadalec uporabi zelo podobno domeno ali kompromitiran pravi račun.
- **Ciljanje finančnih in vodstvenih zaposlenih:** Računovodstvo, nabava, CFO, direktorji projektov.
- **Socialni inženiring kot primarni vektor:** Nujnost, avtoriteta, zaupnost („opravi takoj, prosim brez CC-ja“); pogosto kombiniran z vishing klicem.
- **E-pošta je običajno brez prilog** in brez zlonamerne programske opreme (ang. malware-a)
- **Pogosta tehnika:** „Sprememba TRR dobavitelja“ ali „nujno izplačilo pogodbe“.

ZNAKI DIREKTORSKE PREVARE

- „Direktor prosi za NUJNO plačilo“
- „Dobavitelj je spremenil TRR“
- „To je zaupno, prosim brez drugih“
- „Prosim potrdi nakazilo takoj, sem na poti“
- „Uporabi novi račun – star je v postopku zapiranja“
- AI in deeepfake

Vir: https://www.fortinet.com/resources/cyberglossary/deepfake

KAKO POTEKAJO DIREKTORSKE PREVARE



ZAŠČITA PRED DIREKTORSKIMI PREVARAMI

- Dvofaktorska avtentikacija (2FA) za dostop do e-pošte in aplikacij.
- Preverjanje identitete uporabnikov.
- Spremljanje e-poštnih računov.
- Jasni postopki za potrjevanje in izvedbo finančne transakcije.
- Izobraževanje zaposlenih.
- Ob prevari takojšnje sporočanje banki in policiji.

HVALA

+111 123 456 789

info@enisa.europa.eu