Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Sociálne inžinierstvo a reakcie na incidenty ním spôsobené

(BLOK VIII)
Kurz: Odborný zamestnanec

Ing. Matúš Madleňák

KC KYB UNIZA, https://kc.uniza.sk/

kcskolenia@uniza.sk

OBSAH KURZU ODBORNÝ ZAMESTNANEC

1. Úvod do sociálneho inžinierstva
2. Zaujímavé štatistiky
3. História a súčasnosť sociálneho inžinierstva
4. Interakcia s podvodníkom
5. Druhy sociálneho inžinierstva a phishingu
6. Kategorizácia obetí a útočníkov
7. Ako odhaliť sociálne inžinierstvo/phishing
8. Sociálne inžinierstvo a AI

ÚVOD DO SOCIÁLNEHO INŽINIERSTVA

- Definícia sociálneho inžinierstva
- Ciele sociálneho inžinierstva
- Historické prípady
- Typy útočníkov
- Techniky sociálneho inžinierstva

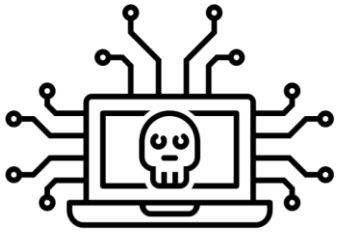
Definícia sociálneho inžinierstva

- Sociálne inžinierstvo je manipulácia ľudí za účelom získania dôverných informácií, prístupu alebo vykonania určitej akcie, často s cieľom narušiť bezpečnosť organizácie.

- Ide o psychologickú manipuláciu, nie technický útok.
- Útočníci využívajú dôveru, strach, autoritu, empatiu alebo naliehavosť.
- Cieľom môže byť získať heslá, prístup do budovy, finančné údaje, citlivé dokumenty atď.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Základné pojmy



Sociálne inžinierstvo

- Manipulatívna technika využívajúca psychologické triky na oklamanie osôb s cieľom získať prístup k informáciám, systémom alebo fyzickým priestorom.

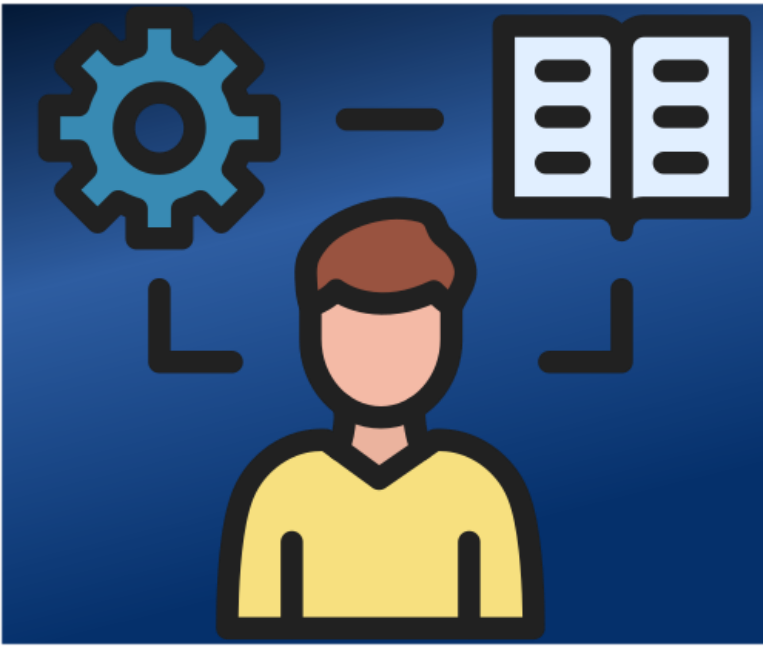
Útočník (social engineer)

- Osoba alebo skupina, ktorá cielene manipuluje obete za účelom dosiahnutia svojho cieľa, často bez použitia technických prostriedkov.

Obeť

- Jednotlivec, skupina alebo organizácia, ktorá nevedomky poskytne útočníkovi požadované informácie alebo umožní prístup.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE



AKTIVITA 1: AKO MÔŽE VYZERAŤ SCENÁR PODVODU / PHISHINGU / SOCIÁLNEHO INŽINIERSTVA?

Brainstorming

Cieľ útoku:

Obeť útoku:

Kanál útoku:

Scenár:

Technický vs. Sociálny útok

Technický útok

- Využíva chyby v softvéri alebo hardvéri
- Vyžaduje technické znalosti (napr. hacking)
- Útok sa zameriava na systém alebo sieť
- ***Príklady:*** malware, DDoS, SQL injection
- Môže byť detegovaný antivírusom či IDS
- Zanecháva technické stopy (logy)

Sociálny útok

- Využíva chyby v ľudskom správaní
- Vyžaduje psychologické schopnosti
- Útok sa zameriava na človeka
- ***Príklady:*** phishing, pretexting, baiting
- Často ťažko detekovateľný
- Zanecháva minimálnu alebo žiadnu stopu

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Sociálne inžinierstvo vs Phishing

Sociálne inžinierstvo

- Široký pojem zahŕňajúci všetky typy manipulácie ľudí
- Môže byť fyzický, verbálny, digitálny
- Cieľom je získať informácie, prístup, dôveru
- Zahŕňa rôzne techniky: pretexting, baiting, shoulder surfing

Phishing

- **Konkrétny typ útoku** – obvykle cez email alebo správu
- **Vždy digitálny** – spravidla email, SMS, web
- Cieľom je **získať osobné údaje**
- Môže pôsobiť ako **vektor** iných útokov
- Využíva najmä **falošné správy**, stránky a odkazy
- Taktiež zahŕňa **rôzne techniky**: Spear phishing, vishing, pharming

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Sociálne inžinierstvo vs Phishing

- *Phishing je len jedna z mnohých techník sociálneho inžinierstva.*

- *Nie každý sociálny útok je phishing, ale každý phishingový útok využíva sociálne inžinierstvo.*

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Čo je cieľom sociálneho inžinierstva?

Získanie citlivých informácií

- Prihlasovacie údaje, osobné údaje, organizačné údaje

Získanie prístupu

- Systémy, priestory, používateľské účty

Finančný zisk

- Falošné faktúry, krádež údajov a následny predaj, vydieranie

Príprava ďalších útokov

- Postupné získavanie informácii s cieľom následného využitia napríklad na realizáciu spear phishingu.
- Distribúcia škodlivého kódu

Spôsobenie reputačných škôd

- Diskreditácia firmy, zníženie dôvery, pomsta

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Prečo je sociálne inžinierstvo efektívne?

Využíva ľudské chyby a emócie

- Ľudský faktor je náchylný na chyby. Útočník využíva stres, časový tlak, zvedavosť alebo empatiu na manipuláciu obete.

Útočník sa vydáva za dôveryhodnú osobu

- Ľudia prirodzene dôverujú tým, ktorí vystupujú sebaisto, majú autoritu alebo používajú známe značky a mená.

Manipuluje psychologicky, nie technicky

- Psychologická manipulácia nevyžaduje technické zručnosti – je lacná, rýchla a často účinnejšia než hackovanie.

Je ťažko odhaliteľné a stíhateľné

- Obeť často netuší, že odovzdala citlivé informácie. Často neexistujú záznamy, ktoré by útok dokázali spätne vysledovať.

Väčšina ľudí sa nespráva bezpečne

- Mnoho ľudí ani nepozná techniky sociálneho inžinierstva.

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

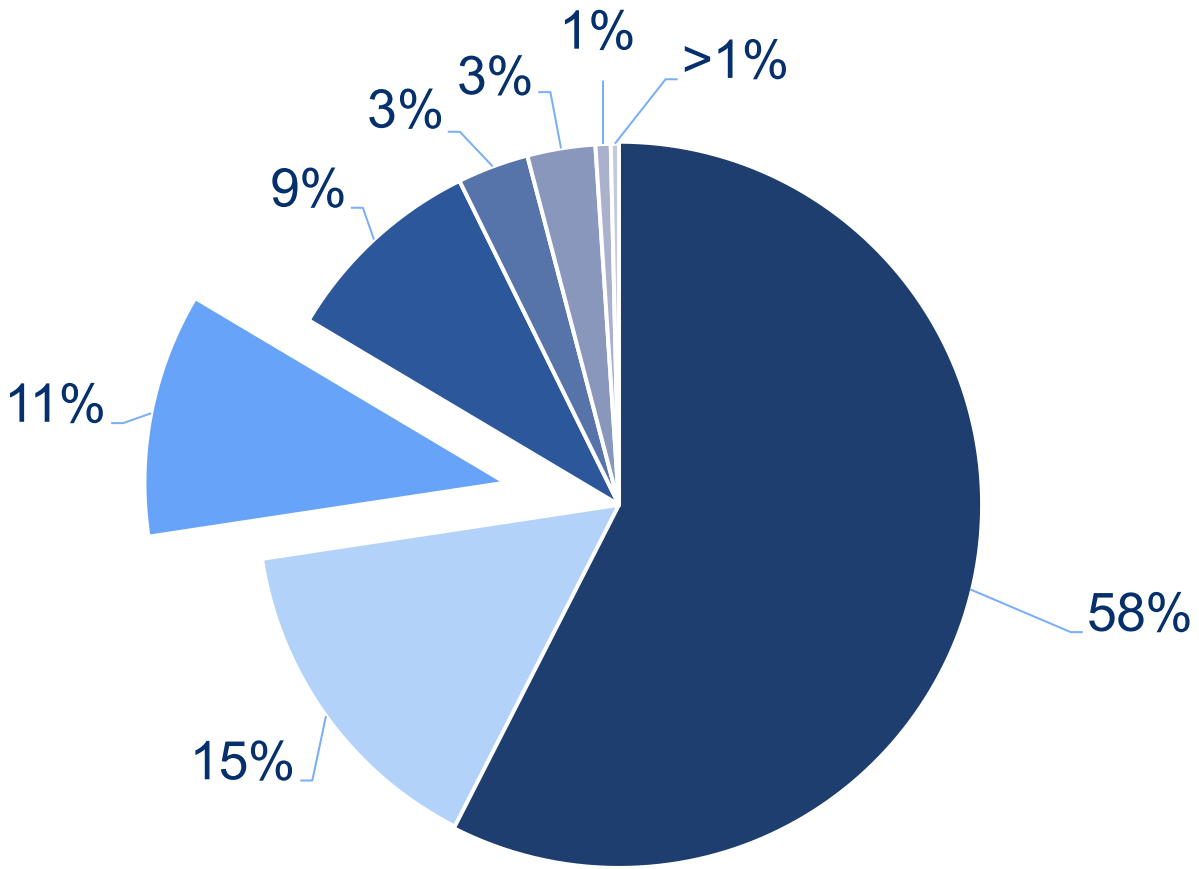
GLOBÁLNE ŠTATISTIKY

SLOVENSKÉ ŠTATISTIKY

- Kybernetické útoky
- Sociálne inžinierstvo
- Podvody

Kybernetické útoky

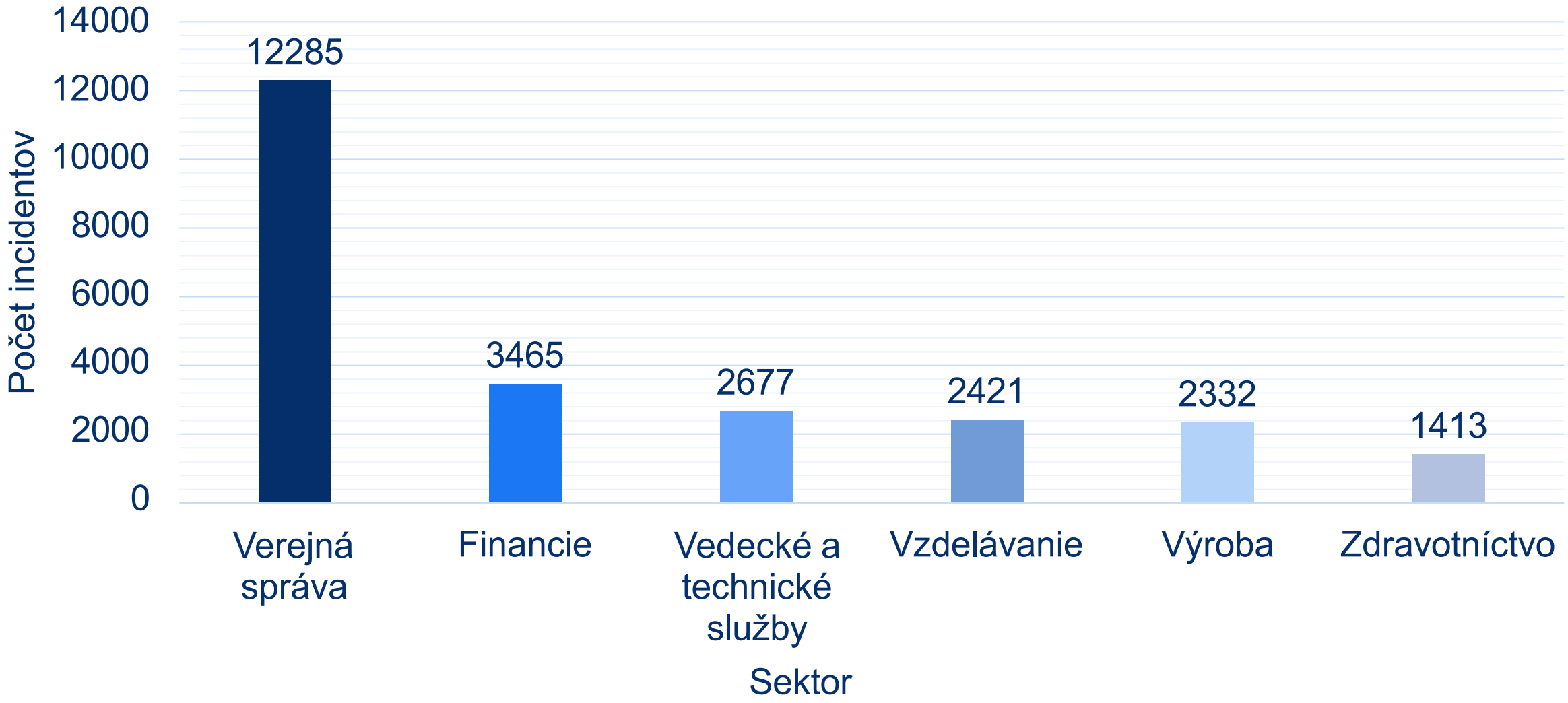
- DoS
- Preniknutie do systému
- Sociálne inžinierstvo
- Rôzne chyby
- Útoky na webové aplikácie
- Zneužitie privilégií
- Stratené a odcudzené aktíva
- Ostatné



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

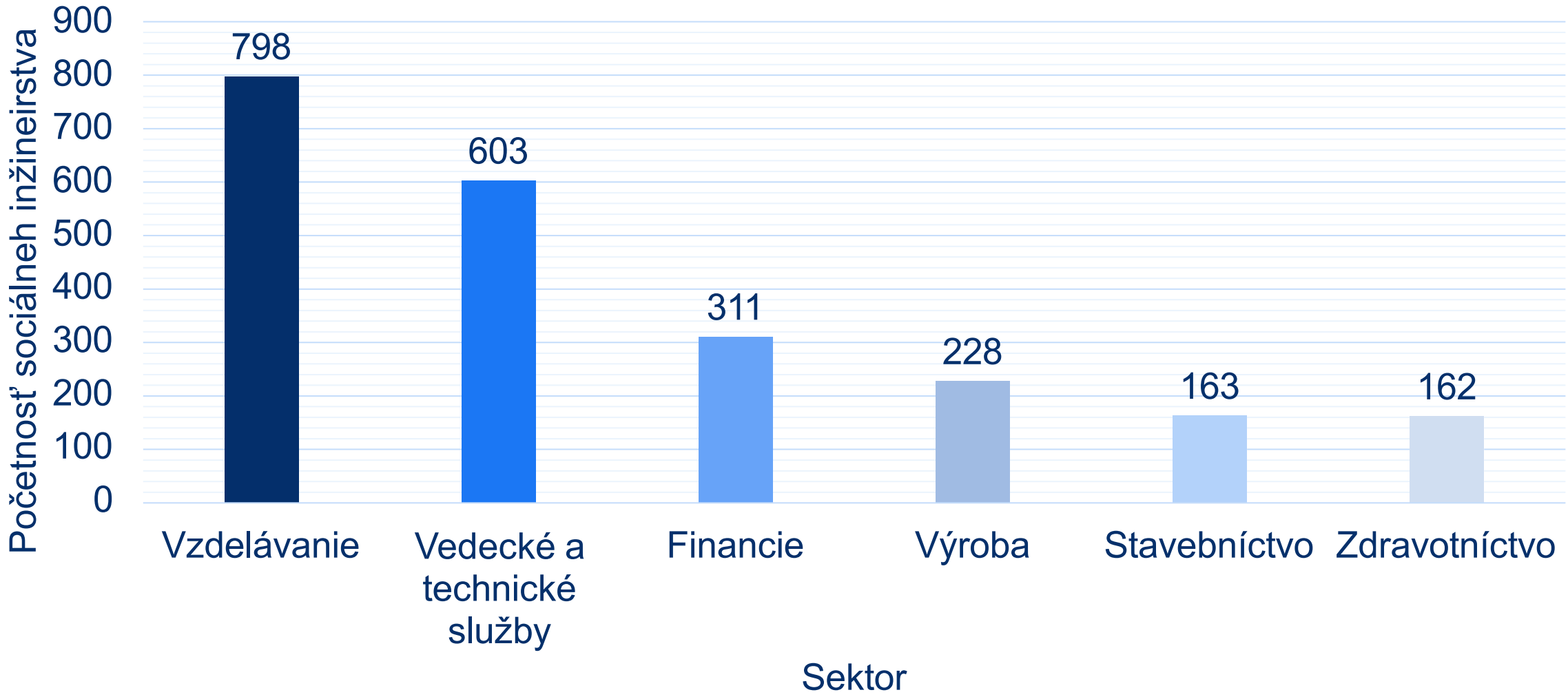
Verizon 2024 Data Breach Investigations Report

Kybernetické útoky – Podľa sektorov



Verizon 2024 Data Breach Investigations Report

Sociálne inžinierstvo – Podľa sektorov

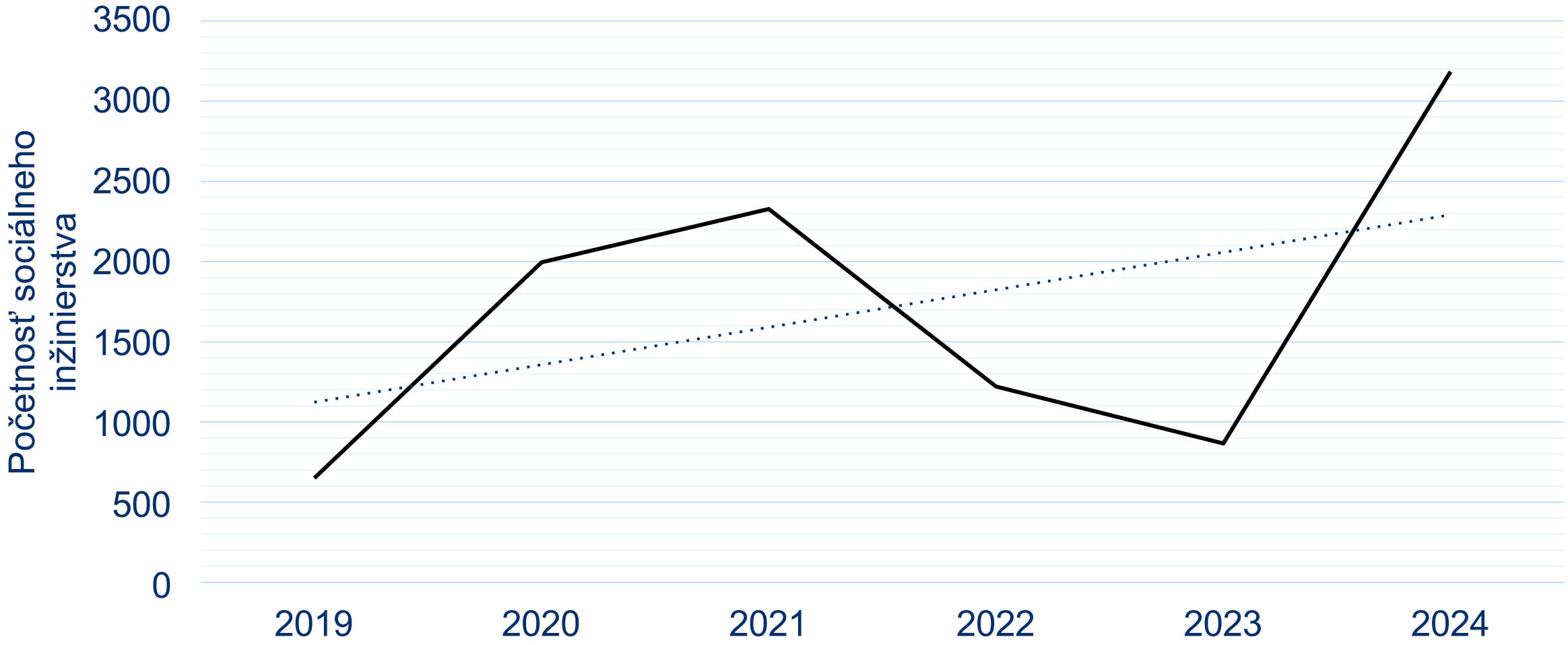


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Verizon 2024 Data Breach Investigations Report

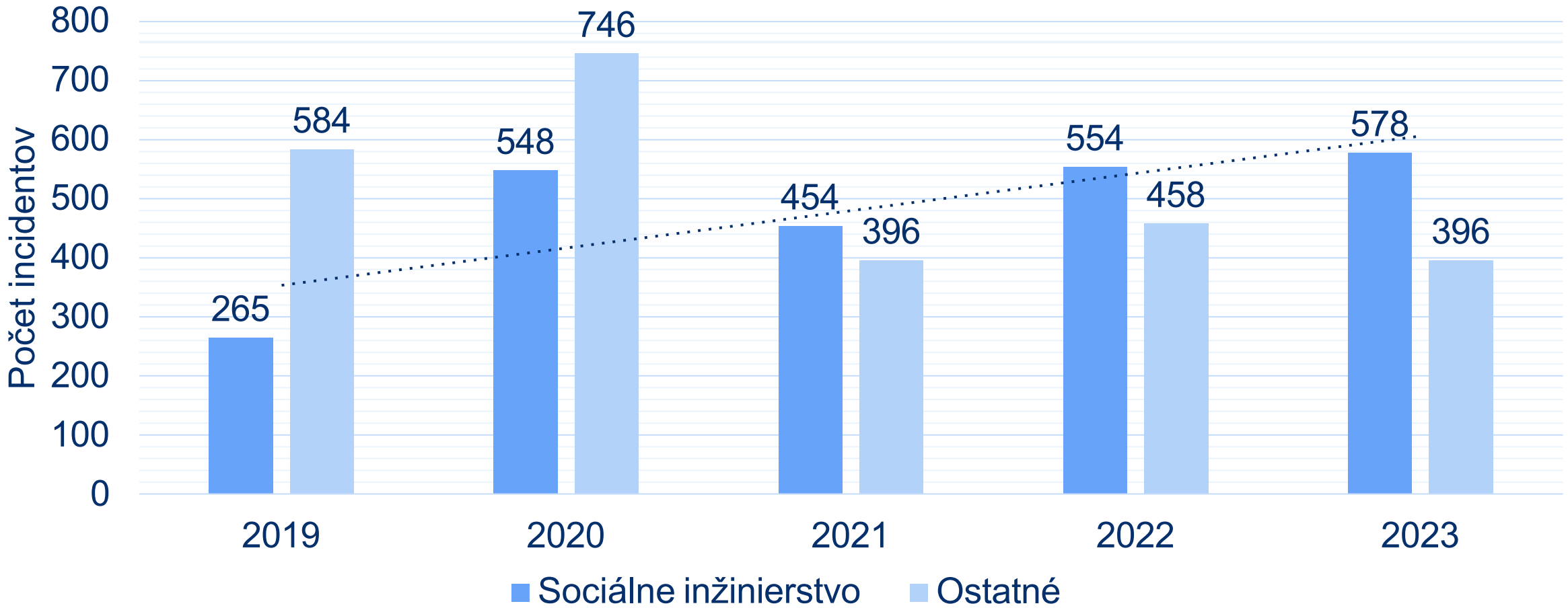
Globálne štatistiky

Sociálne inžinierstvo - 2019 až 2024



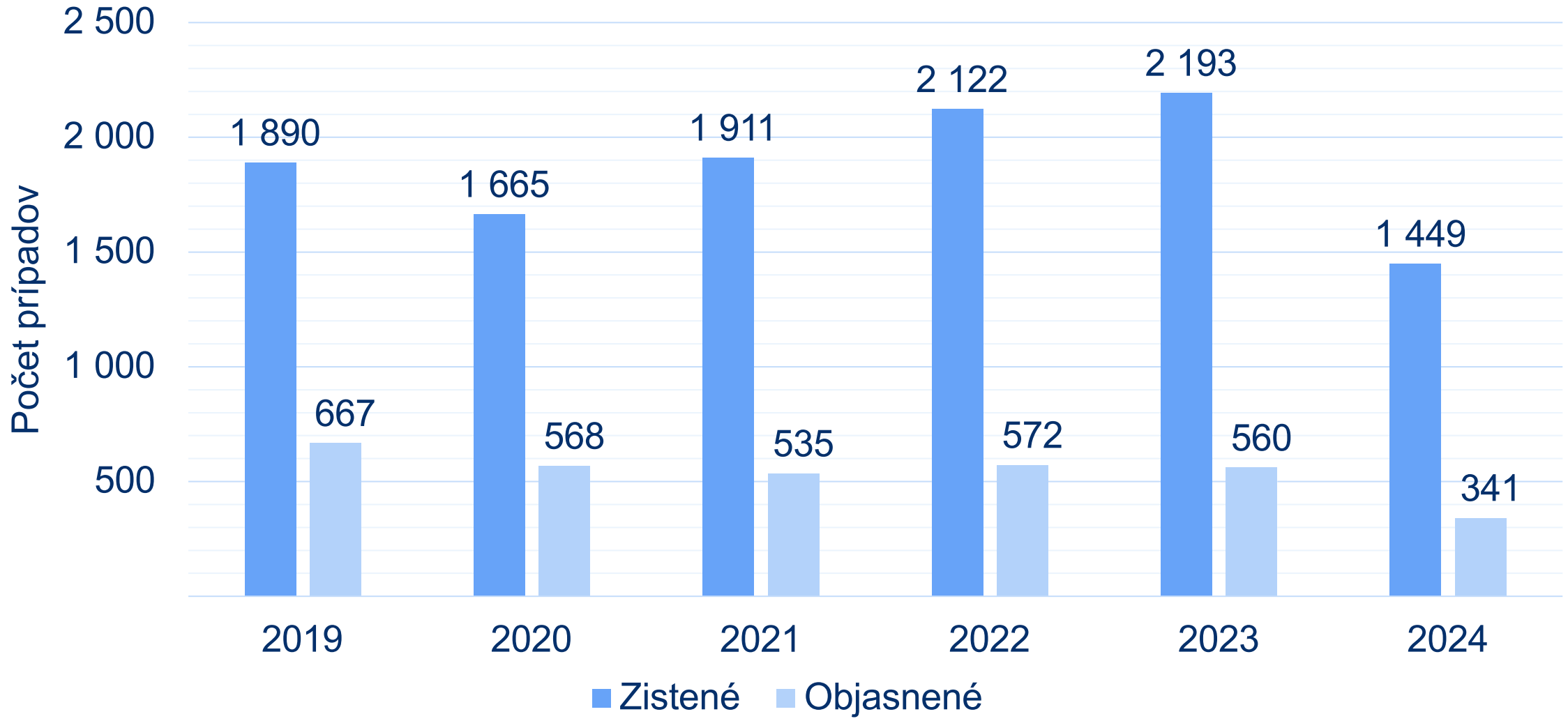
Verizon 2024 Data Breach Investigations Report

Sociálne inžinierstvo vs. Ostatné (CSIRT)



Slovenské štatistiky

Podvody – všetky (MINV)



HISTÓRIA SOCIÁLNEHO INŽINIERSTVA

Kevin Mitnick – legenda sociálneho inžinierstva

- Kevin Mitnick, jeden z najslávnejších hackerov v histórii, využíval sociálne inžinierstvo na získavanie dôverných údajov od zamestnancov spoločností ako Nokia, Motorola či Sun Microsystems.
- Nebol to technický prienik, ale manipulácia ľudí, ktorá mu umožnila získať prístup k systémom.
- Vo väzbe strávil 5 rokov, neskôr sa stal etickým hackerom.
- Prípad upozornil na to, že najslabším článkom bezpečnosti je človek.

https://en.wikipedia.org/wiki/Kevin_Mitnick

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Pentagon a „dumbster diving“ (90. roky)

- Bezpečnostní analytici zistili, že útočníci nachádzali vo vyhodených dokumentoch pred budovou Pentagonu prístupové kódy, vojenské záznamy či konfigurácie zariadení.
- Tento prípad viedol k zavedeným štandardom skartovania a politikám manipulácie s papierovými dokumentmi.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

RSA Security Incident (2011)

- Zamestnanec spoločnosti RSA otvoril e-mail s prílohou nazvanou „2021 Recruitment Plan“.
- Príloha obsahovala škodlivý Excel súbor.
- Útok viedol k narušeniu bezpečnostného systému SecurID, ktorý používalo viacero štátnych aj komerčných organizácií.
- Sociálne inžinierstvo použité na spear-phishing.
- Následne bola kompromitovaná infraštruktúra obranných dodávateľov USA.

https://www.wired.com/2011/06/rsa-hack/

Target (2013) – cez dodávateľa k miliónom zákazníkov

- Útočníci získali prihlasovacie údaje externého dodávateľa HVAC cez phishingový e-mail.
- Pomocou týchto údajov sa dostali do siete spoločnosti Target a ukradli údaje o 40 miliónoch platobných kariet.

- Príklad „supply chain“ sociálneho inžinierstva.
- Význam segmentácie siete a minimálneho prístupu.

https://frameworksecurity.com/post/the-target-breach-a-historic-cyberattack-with-lasting-consequences

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Prípad „fake president“ – CEO fraud (2016)

- Francúzska spoločnosť Etna Industrie prišla o 500 000 €, keď zamestnanec previedol peniaze na základe falošného e-mailu od „generálneho riaditeľa“.
- Útočníci využili verejne dostupné informácie a podrobne napodobnili štýl komunikácie CEO.

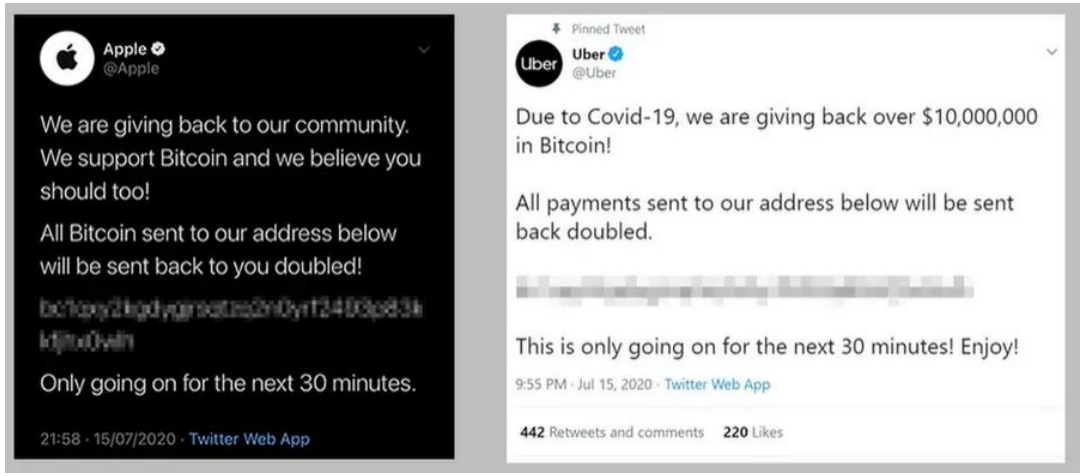
- Tento typ útoku sa často označuje ako Business Email Compromise (BEC).
- Ukážka dôležitosti verifikácie transakcií mimo e-mailu.

https://www.bbc.com/news/business-35250678

Hack Twitteru v roku 2020

- V júli 2020 došlo k masívnemu útoku na účty známych osobností (Elon Musk, Barack Obama, Apple), ktoré boli zneužité na kryptomenový podvod.
- Útočníci sa cez telefónne hovory a sociálne inžinierstvo dostali k zamestnancom Twitteru a tým aj k administrátorským nástrojom.
- Škoda: viac ako 120 000 USD v BTC.
- Ukážka zlyhania interného školenia a príliš širokého prístupu zamestnancov.

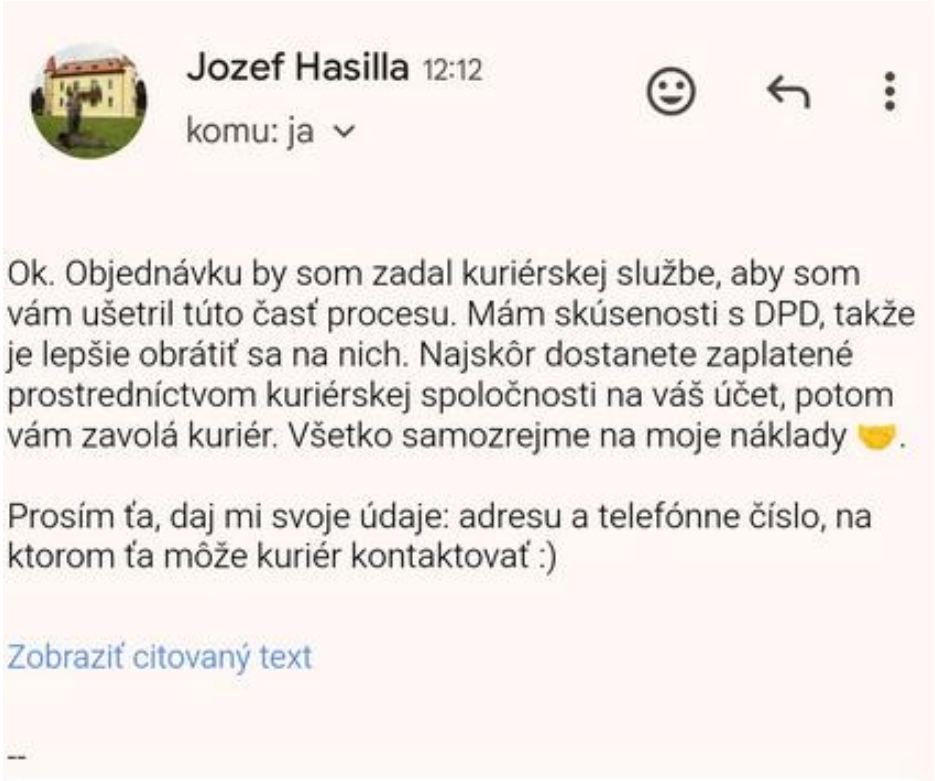
https://www.bbc.com/news/technology-56429204



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

História sociálneho inžinierstva

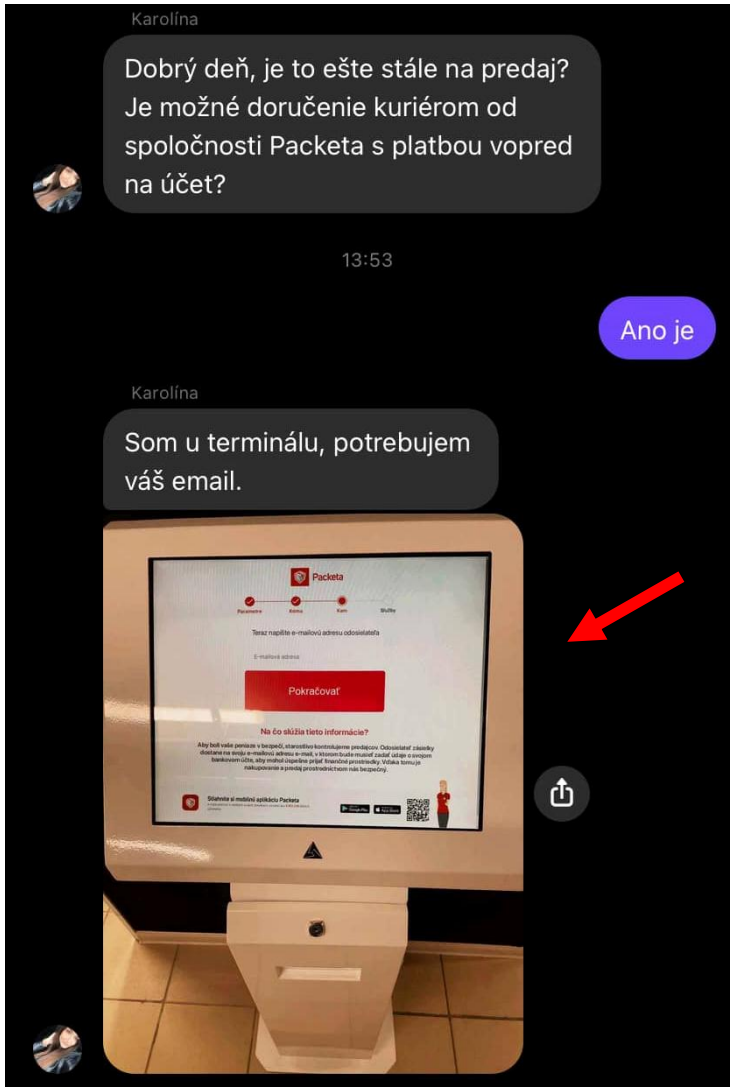
Príklady aktuálnych podvodov

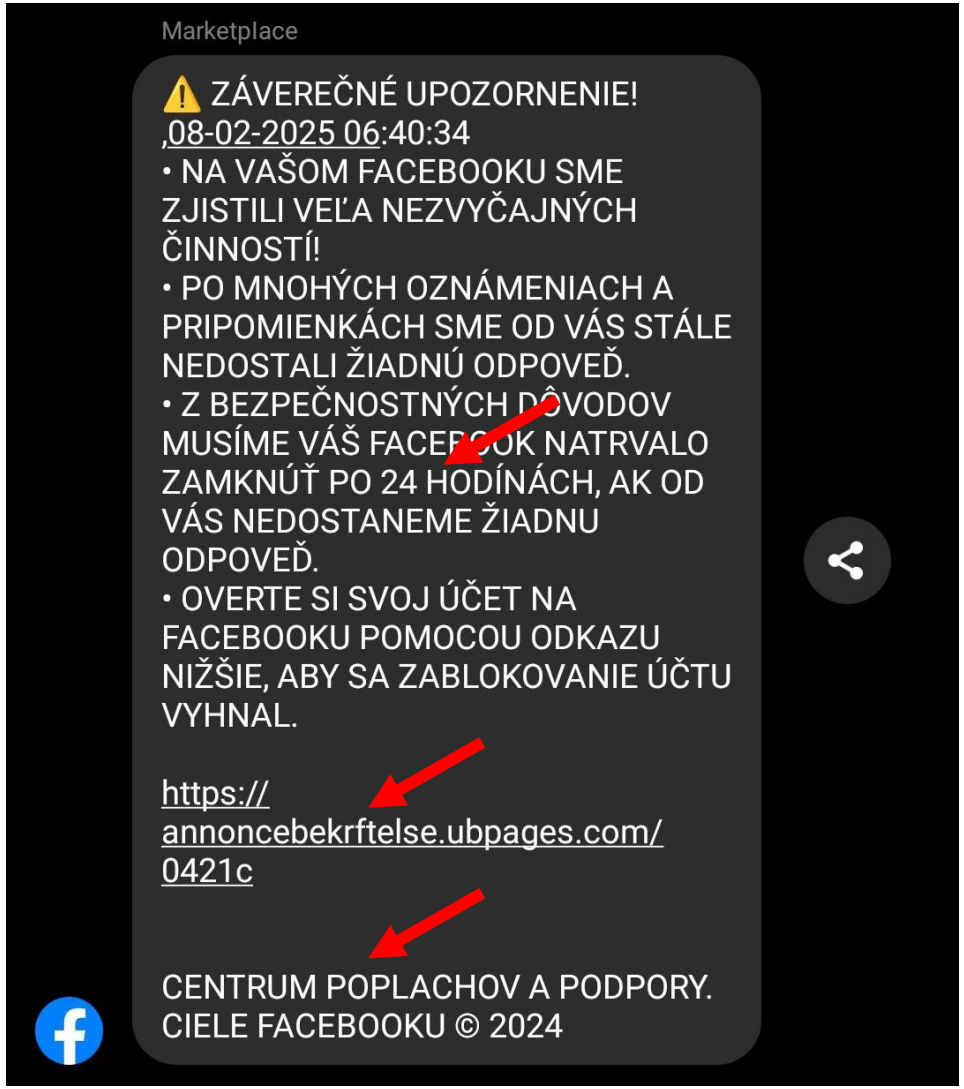


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

História sociálneho inžinierstva

Príklady aktuálnych podvodov



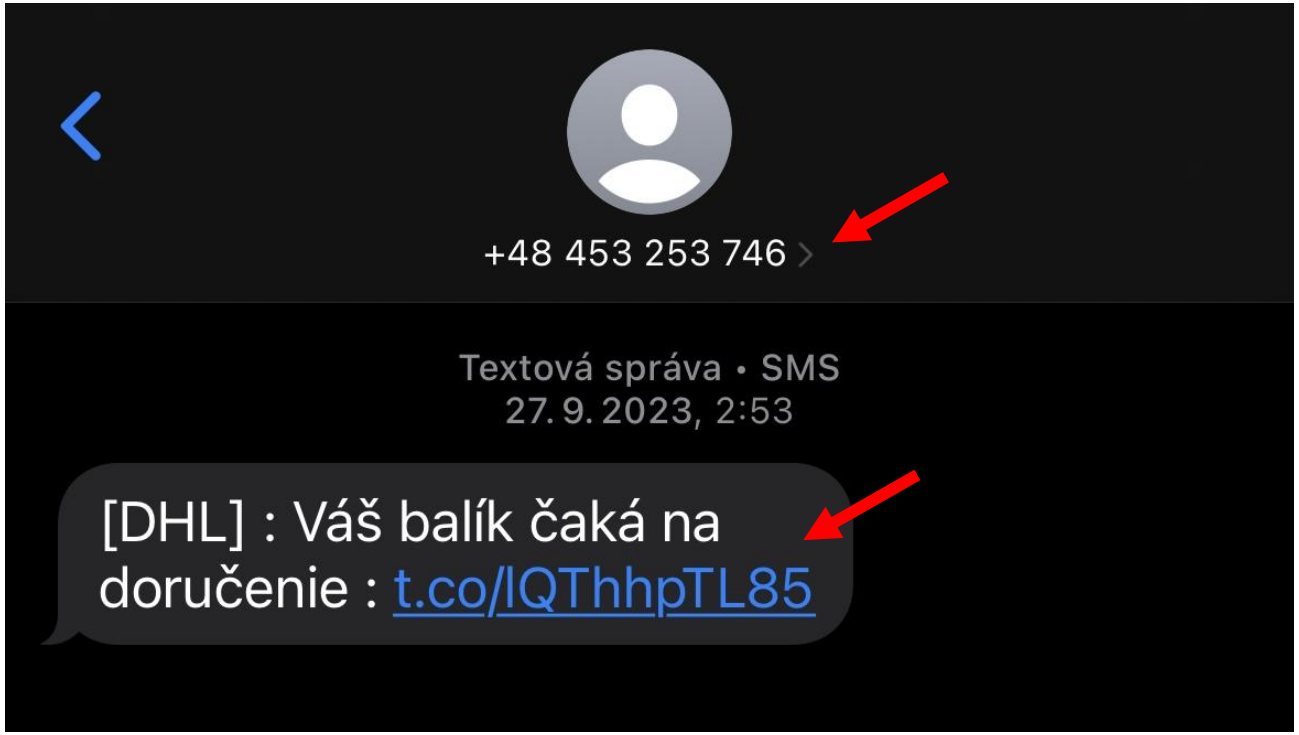


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Podvody asociované s kryptomenami

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Príklady aktuálnych podvodov



Príklady aktuálnych podvodov

Muž, ktorý neváhal vylákať peniaze od 86-ročného starčeka tým, že mu zavolal mu cez pevnú linku a predstavil sa ako nadporučík od dvoch levov, teda bratislavského krajského riaditeľstva. Seniorovi povedal, že jeho syn mal dopravnú nehodu, pri ktorej zranil malé dieťa. Falošný nadporučík dôchodcovi prikázal, že ako odškodné za zranené dieťa musí zaplatiť 15-tisíc eur. ***"Senior zrátal finančnú hotovosť vo výške 15 000 eur, a podľa inštrukcií údajného nadporučíka mal dať peniaze do vrecka a vyhodiť ich cez okno pred vchod domu,"*** uviedla Silvia Šimková, hovorkyňa Krajského riaditeľstva Policajného zboru v **Bratislave**.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Príklady aktuálnych podvodov

- **Telefonický podvod „Vnuk Maťko“ – falošný príbuzný (Bratislava, 2025)** – dôchodca odovzdal podvodníkom 65 000 € po tom, čo uveril, že pomáha svojmu vnukovi pri údajnom prepise bytov a pozemkov. Zdroj: Ta3

- **Internetový podvod „šéf vrtnej plošiny“ – romantický podfuk (Bratislavský kraj, 2024)** – seniorka poslala podvodníkovi, vydávajúcemu sa za zahraničného „šéfa ropnej plošiny“, spolu 404 795 € v hotovosti a kryptomenách. Zdroj: Refresher

- **Podvodná návšteva doma – falošný plynár (Bratislava, 2023)** – 85-ročnej dôchodkyni ukradol podvodník približne 10 000 € po tom, čo sa vydával za pracovníka plynární a pod zámienkou rozmenenia peňazí jej zobral úspory. Zdroj: Markíza

Príklady aktuálnych podvodov

- **SMS podvod „blokovaná SIM karta O2“ (Slovensko, 2025)** – obete dostali falošnú SMS, že ich SIM karta bude zablokovaná; po kliknutí na podvodný odkaz boli vyzvaní zadať údaje z platobnej karty, čím hrozila strata financií. Zdroj: Pravda

- **SMS podvod „zadržaný balík“ (Slovensko, 2025)** – ľudia dostávali správy vydávajúce sa za Slovenskú poštu alebo Colnú správu, v ktorých bol odkaz na falošnú stránku; cieľom bolo vylákať osobné a platobné údaje. Zdroj: Pravda

- **Phishing na klientov Fio banky (Slovensko, 2024)** – klienti boli presmerovaní na falošný web banky a zadávali prihlasovacie údaje a autorizačné kódy; viacerým zmizli z účtov stovky až tisíce eur, celková škoda presiahla 50 000 €. Zdroj: Peniaze.sk

- **SMS podvod „Mami, potrebujem pomôcť“ (Česko, 2024)** – podvodníci sa vydávali za deti v núdzi písaním z „nového čísla“; žiadali rodičov o peniaze alebo bankové údaje, pričom niektorí ľudia s nimi komunikovali, no škody boli vďaka ostražitosti obmedzené. Zdroj: iROZHLAS

Ponaučenie

- Najčastejšie zlyháva ľudský faktor, nie technológia.
- Útočníci využívajú dôveru, zvedavosť alebo autoritu.
- Školenia, kontrola prístupov a overovanie požiadaviek môžu zásadne znížiť riziko.

SKUTOČNÉ PRÍPADY PHISHINGU

Interakcia s podvodníkom a reálne príklady podvodov


MUDr. Stanisla... 12:28
komu: ja
Skvelé, teraz vytvorím objednávku prostredníctvom Packeta a zaplatím vrátane poštovného. Napíšte mi prosím: meno a priezvisko, telefónne číslo a IBAN. Keď všetko zaplatím, je potrebné potvrdiť oobjednávku a platba bude pripísaná na váš účet. Po prijatí platby môžete odoslať prostredníctvom ktorejkoľvek pobočky Packety.
MUDr. Stanislava Szabóová
ŠN sv. Svorada Zobor, n.o.
Kláštorská 134, 949 88 Nitra
so 1. 3. 2025 o 11:00 Stanislav Chriašteľ <chriastels@gmail.com> napísal(a):
Zobraziť citovaný text

POĎME VYSKÚŠAŤ ČI NÁS PODVODNÍK BUDE KONTAKTOVAŤ ☺

Interakcia s podvodníkom a reálne príklady podvodov

Pridanie inzerátu: 18.09.2025, 08:53

Čo: kryt ipad 9 gen | Všetky rubriky | PSČ (miesto): | Okolie: 25 km | Cena od: | do: | € | Hľadať

Hlavná stránka > **Vyhľadávanie** > **kryt ipad 9 gen**

Inzercia

Auto
Inzeráty Celkom: 239313
Za 24 hodín: 14357

Deti
Inzeráty Celkom: 104707
Za 24 hodín: 2579

Dom a záhrada
Inzeráty Celkom: 75236
Za 24 hodín: 2704

Elektro
Inzeráty Celkom: 53194
Za 24 hodín: 1883

Foto
Inzeráty Celkom: 8934
Za 24 hodín: 386

Hudba
Inzeráty Celkom: 17555
Za 24 hodín: 699

Knihy
Inzeráty Celkom: 28916
Za 24 hodín: 827

Mobily
Inzeráty Celkom: 20353
Za 24 hodín: 1381

Zobrazených 1-6 inzerátov z 6

	Cena	Lokalita	Zobrazenie
Nové inzeráty e-mailom			
Kryt s klávesnicou na iPad 9 gen - [18.9. 2025] Predám **kryt** logitech combo touch na **ipad 9 gen**. Vo veľmi dobrom stave	**95 €**	Žilina 010 01	16 x
 **iPad 9. generácia 10.2" 64 GB Cellular +Wi-Fi** - TOP - [17.9. 2025] Predám **ipad** 2021 10.2" -64 GB -Wi-Fi + Cellular -Zadarmo dám **kryt** na **ipad** s držiakom na Apple Pencil + aplikované ochranné sklo -Krabica s káblom -Všetky škrabance sú len na ochrannom skle -Používaný 10 mesiacov	**189 €**	Dunajská Streda 931 01	380 x
 **Ipad** - [15.9. 2025] Predám **ipad** (**9**. **gen**erácia), 64GB, je v zachovalom stave +pridávam ku nemu aj apple pencil (1st **gen**eration) +**kryt** (ružový)	**250 €**	Košice-okolie 044 55	132 x
 **Apple Ipad 9.generácia grey 64GB** - [9.9. 2025] Predám **ipad 9.gen**. + Apple pero 1.**gen**. +**kryt** Na fotkách vidno škrabanec inak bez poškodenia, keďže bol stále v **kryt**e Cena za všetko bez nabíjačky 230€ Krabičky mám	**230 €**	Michalovce 071 01	146 x

Prvý záujemca ☺ : 18.09.2025, 09:00

Bazos.sk <odpoved@bazos.sk> 9:00 (pred 7 hodinami)

komu: mne

Dobrý deň, mám záujem! Z akého ste mesta?

facu.novakristina244@gmail.com - Email bol odoslaný zo serveru Bazos.sk.

Pozor neexistuje nič ako Bazoš platba alebo Bazoš kuriér (pozor na falošné stránky PPL, DPD, Packety alebo Slovenskej pošty). Pokiaľ Vás kontaktuje užívateľ, že všetko zariadi a peniaze získate prihlásením do bankovníctva alebo zaslaním čísla karty, ide o podvod.

Inzerát 183199627: Kryt s klávesnicou na iPad 9 gen
Predám kryt logitech combo touch na iPad 9 gen. Vo veľmi dobrom stave

Cena: 95
https://mobil.bazos.sk/inzerat/183199627/kryt-s-klavesnicou-na-ipad-9-gen.php

M **Matus Madlenak** 9:02 (pred 7 hodinami)

komu: facu.novakristina244

Dobrý deň,
Žilina. Môžem vám poslať ďalšie fotky produktu ak máte záujem.

•••

Kristína Facúnová <facunovakristina244@gmail.com> 14:11 (pred 2 hodinami)

komu: mne

Ďakujem za odpoveď! Všetko mi vyhovuje, chcem to kúpiť.
Žijem v Bardejove a bolo by pre mňa veľmi pohodlné, keby ste mohli poslať zásielku cez GLS. Môžem zaplatiť hneď teraz, peniaze dostanete predtým, ako pošlete balík.
Nevadí vám to?

S pozdravom
Facúnová

št 18. 9. 2025 o 9:02 Matus Madlenak <matus.madlenak@gmail.com> napísal(a):

•••

Matus Madlenak 14:13 (pred 2 hodinami)

komu: Kristína

Ako by sme to spravili? Pošlem vám číslo účtu? Ešte som takto neplatil

•••

Kristína Facúnová 14:16 (pred 2 hodinami)

komu: mne

Preferujem kuriérsku službu doručenia cez GLS. Zaplatím za doručenie aj tovar, vy dostanete platbu vopred na váš účet, potom kuriér príde na vami uvedenú adresu, zoberie tovar a pošle ho do Bardejova.

Napíšte mi Vaše telefónne číslo, adresu a číslo účtu (teda aplikácia GLS Slovakia to pýta). Objednávku urobím sáma a pošlem Vám sledovanie číslo. Už som napísala svoje údaje.

št 18. 9. 2025 o 14:13 Matus Madlenak <matus.madlenak@gmail.com> napísal(a):

•••

M

Matus Madlenak 16:09 (pred 17 minútami)

komu: Kristína

Nemá GLS nejakú stránku kde to viem spraviť? Aby som to nemusel posielať tu cez email

št 18. 9. 2025 o 14:16 Kristína Facúnová <facunovakristina244@gmail.com> napísal(a):

•••

Matus Madlenak <matus.madlenak@gmail.com>
komu: Kristína

št 18. 9. 16:26 (pred 15 hodinami)

číslo účtu myslíte IBAN alebo údaje karty?

št 18. 9. 2025 o 16:09 Matus Madlenak <matus.madlenak@gmail.com> napísal(a):

•••

Kristína Facúnová
komu: mne

18. 9. 2025 17:36 (pred 14 hodinami)

1. Telefónne číslo
2. Adresa
3. IBAN

Prosím, napíšte mi tieto údaje a ja všetko zaplatím hneď teraz.

št 18. 9. 2025 o 16:26 Matus Madlenak <matus.madlenak@gmail.com> napísal(a):

•••

Kristína Facúnová
komu: mne

18. 9. 2025 17:36 (pred 14 hodinami)

Peniaze budú okamžite odoslané na váš účet!

št 18. 9. 2025 o 17:36 Kristína Facúnová <facunovakristina244@gmail.com> napísal(a):

•••

Bazos.sk <odpoved@bazos.sk>

10:17 (pred 5 hodinami)

komu: mne

je tento kryt s klávesnicou kompatibilný aj s inými modelmi ipadov, alebo je určený výhradne na ipad 9. generácie?

d.i.et.richlola5@gmail.com - Email bol odoslaný zo serveru Bazos.sk.

Pozor neexistuje nič ako Bazoš platba alebo Bazoš kuriér (pozor na falošné stránky PPL, DPD, Packety alebo Slovenskej pošty). Pokiaľ Vás kontaktuje užívateľ, že všetko zariadi a peniaze získate prihlásením do bankovníctva alebo zaslaním čísla karty, ide o podvod.

Inzerát 183199627: Kryt s klávesnicou na iPad 9 gen
Predám kryt logitech combo touch na iPad 9 gen. Vo veľmi dobrom stave

Cena: 95
https://mobil.bazos.sk/inzerat/183199627/kryt-s-klavesnicou-na-ipad-9-gen.php

M

Matus Madlenak

10:22 (pred 5 hodinami)

komu: d.i.et.richlola5

Je kompatibilný so 7. 8. a 9. generáciou. Je to tento model: https://www.alza.sk/logitech-combo-touch-pre-ipad-7-8-a-9gen-uk-d6447271.htm?utm_campaign=heureka_sk_prislusenstvi-pro-it-tv_klavesnice_s-pouzdrem-na-tablet_mc056k5b2&utm_medium=product&utm_source=heureka_sk

št 18. 9. 2025 o 10:17 Bazos.sk <odpoved@bazos.sk> napísal(a):

Ondrej Chovanec <dietrichlola5@gmail.com> 12:47 (pred 3 hodinami)

komu: mne

Dobrý deň, môžete mi to poslať kuriérom cez DPD? Som zo Starej Ľubovne, zaplatím vopred.

št 18. 9. 2025 o 10:22 Matus Madlenak <matus.madlenak@gmail.com> napísal(a):

•••

Matus Madlenak 14:14 (pred 2 hodinami)

komu: Ondrej

Ako by sme to spravili? Pošlem vám číslo účtu? Ešte som takto neplatil

•••

Ondrej Chovanec 14:40 (pred 1 hodinou)

komu: mne

Zabezpecím bezpecnu platbu prostredníctvom dpd. Peniaze za tovar dostanete ako prve, az potom odovzdate kurierovi svoju adresu. Takze to bude pre vás veľmi vyhodna moznosť

Už ste takto predávali?

št 18. 9. 2025 o 14:14 Matus Madlenak <matus.madlenak@gmail.com> napísal(a):

•••

Matus Madlenak
komu: Ondrej

16:07 (pred 10 minútami)

noo, ešte nie. Pošlite nejaký návod

št 18. 9. 2025 o 14:40 Ondrej Chovanec <dietrichlola5@gmail.com> napísal(a):

•••

Ondrej Chovanec
komu: mne

pi 19. 9. 10:58

Najprv musím vybaviť kuriéra, potom vám pošlem odkaz, kde môžete získať peniaze od dpd na ucet. Po potvrdení platby vám zavolá kuriér a dohodnete si vhodný deň stretnutia. Kuriér môže prísť aj k vám domov
Vyhovuje vám to?

št 18. 9. 2025 o 16:08 Matus Madlenak <matus.madlenak@gmail.com> napísal(a):

•••

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

1. Pridanie inzerátu – 11.02.2025, 09:42

Inzerat 175066700 bol pridany

Bazos.sk <inzerat@bazos.sk>
komu: mne

ut 11. 2. 9:42

Pozor, neexistuje nič ako Bazoš platba alebo Bazoš kuriér. Nikdy neprezrádzajte číslo Vašej karty s tým, že dostanete zaplatené na túto kartu !!!

Potvrdzujeme pridanie Vášho inzerátu.

Pokiaľ chcete Váš inzerát TOPovať (Posunúť pred netopovane inzeráty.), zašlite sms v tvare BAZOS na telefónne číslo 8866 (Orange Slovensko, Telekom a O2, cena jednej SMS je s DPH - 2,5 Eur). Kód môžete zakúpiť i platobnou kartou, cez Sporopay od Slovenskej sporiteľne, e Platby VÚB, Tatrabanka TatraPay (1,99 Eur). Obdržaný kód ďalej vyplňte do políčka poukážka. Výsledný čas = čas vloženia + topovaný čas.

Topovanie, zmazanie alebo editáciu inzerátu môžete urobiť na
https://mobil.bazos.sk/zmazat/175066700.php

Obal Logitech Combo Touch pre iPad 7 8 alebo 9
Predám obal na Apple iPad s klávesnicou Logitech Combo touch vo výbornom stave! Obal je vhodný ak si so svojho iPadu chcete urobiť Notebook / Laptop

Obal/klavesnica bola používaná len úplne minimálne. Klavesnica sa dá oddeliť od iPadu a iPad sa da používať bez klávesnice. Obal má aj držiak na Apple pencil.

Vhodný pre iPad 7,8 alebo 9 generácie.

V prípade záujmu viem predať aj Apple pencil 1 gen (+70€)

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

2. Prvý „záujemca“ – 11.02.2025, 09:54

Bazos.sk - odpoved na inzerat 175066700 - Obal Logitech Combo Touch pre iPad 7 8 alebo 9

Bazos.sk <odpoved@bazos.sk> ut 11. 2. 9:54
komu: mne

dobré ránko,

aký je materiál obalu logitech combo touch? ak by ste mali chvíľu, prosím napíšte mi na whots app.
+421(918)093-894

kovarrichard67+fu3i@gmail.com - Email bol odoslaný zo serveru Bazos.sk.

Pozor neexistuje nič ako Bazoš platba alebo Bazoš kuriér (pozor na falošné stránky PPL, DPD, Packety alebo Slovenskej pošty). Pokiaľ Vás kontaktuje užívateľ, že všetko zariadi a peniaze získate prihlásením do bankovníctva alebo zaslaním čísla karty, ide o podvod.

Inzerát 175066700: Obal Logitech Combo Touch pre iPad 7 8 alebo 9
Predám obal na Apple iPad s klávesnicou Logitech Combo touch vo výbornom stave! Obal je vhodný ak si so svojho iPadu chcete urobiť Notebook / Laptop

Obal/klavesnica bola používaná len úplne minimálne. Klavesnica sa dá oddeliť od iPadu a iPad sa da používať bez klávesnice. Obal má aj držiak na Apple pencil.

Vhodný pre iPad 7,8 alebo 9 generácie.

V prípade záujmu viem predať aj Apple pencil 1 gen (+70€)

3. Druhý záujemca – 12.02.2025, 12:59

Bazos.sk - odpoved na inzerat 175066700 - Obal Logitech Combo Touch pre iPad 7 8 alebo 9

Bazos.sk <odpoved@bazos.sk>
komu: mne

st 12. 2. 12:59

aktualne?C

Obal Logitech Combo Touch pre iPad 7 8 alebo 9/aktualne?C

kollarikovaveronika85@gmail.com - Email bol odoslaný zo serveru Bazos.sk.

Pozor neexistuje nič ako Bazoš platba alebo Bazoš kuriér (pozor na falošné stránky PPL, DPD, Packety alebo Slovenskej pošty). Pokiaľ Vás kontaktuje užívateľ, že všetko zariadi a peniaze získate prihlásením do bankovníctva alebo zaslaním čísla karty, ide o podvod.

Inzerát 175066700: Obal Logitech Combo Touch pre iPad 7 8 alebo 9
Predám obal na Apple iPad s klávesnicou Logitech Combo touch vo výbornom stave! Obal je vhodný ak si so svojho iPadu chcete urobiť Notebook / Laptop

Obal/klavesnica bola používaná len úplne minimálne. Klavesnica sa dá oddeliť od iPadu a iPad sa da používať bez klávesnice. Obal má aj držiak na Apple pencil.

Vhodný pre iPad 7,8 alebo 9 generácie.

V prípade záujmu viem predať aj Apple pencil 1 gen (+70€)

Cena: 90
https://mobil.bazos.sk/inzerat/175066700/obal-logitech-combo-touch-pre-ipad-7-8-alebo-9.php

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

4. Moja odpoveď - 12.02.2025, 13:01

Matus Madlenak <matus.madlenak@gmail.com>
komu: kollarikovaveronika85

st 12. 2. 13:01

Dobrý deň,
áno inzerát je aktuálny.

st 12. 2. 2025 o 12:59 Bazos.sk <odpoved@bazos.sk> napísal(a):

5. Je to tu ☺ 12.02.2025, 13:01

MUDr. Veronika Kolláriková

komu: mne

st 12. 2. 13:01

Zdravím! Skvelé, pošlem vám kuriéra DHL, napíšte mi: vaše meno a priezvisko, adresu, telefónne číslo a číslo IBAN. Vytvorím objednávku a zaplatím za ňu, potom je potrebné potvrdiť objednávku a platba bude pripísaná na váš účet.

--

MUDr. Veronika Kolláriková

ŠN sv. Svorada Zobor, n.o.

Kláštorská 134, 949 88 Nitra

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

DRUHY SOCIÁLNEHO INŽINIERSTVA

Pretexting – Falošná identita, Scenár

- Útočník si vytvára falošnú identitu alebo dôveryhodnú situáciu, aby oklamal obeť a získal od nej informácie alebo prístup.
- Vyžaduje si dôkladnú prípravu príbehu/scenára.
- Útočník sa často vydáva za autoritu (napr. zamestnanca banky, IT technika, policajta).
- Cieľom je, aby obeť dobrovoľne zdieľala citlivé údaje (heslá, čísla účtov, interné informácie).

Príklad:

- Telefónny hovor od „správcu siete“, ktorý tvrdí, že potrebuje overiť vaše prihlasovacie údaje kvôli „bezpečnostnému incidentu“.

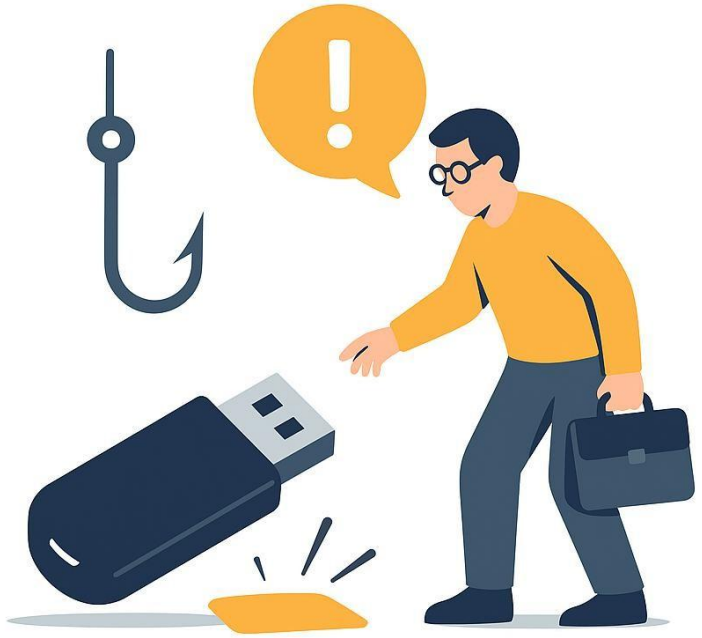
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Baiting - Návnada

- Útočník ponúka niečo atraktívne alebo zaujímavé, aby motivoval obeť vykonať akciu, ktorá spustí škodlivý proces.
- Môže ísť o fyzickú alebo digitálnu formu návnady.
- Často apeluje na zvedavosť alebo chamtivosť.
- Cieľom je spustiť malware alebo získať prístup do systému.

Príklad:

- USB kľúč s označením „Mzdové tabuľky“, položený na parkovisku pred firmou. Po zapojení do počítača sa nainštaluje malware.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Tailgating (piggybacking) – Fyzický prienik

- Útočník sa fyzicky dostane do zabezpečených priestorov tým, že nasleduje oprávnenú osobu bez toho, aby sa musel autentifikovať.
- Využíva ľudskú zdvorilosť alebo nepozornosť.
- Často sa vydáva za kuriéra, návštevu, kolegu bez preukazu.
- Nebezpečný v prostredí s citlivými systémami alebo dátami.
- Cieľom je vstúpiť do priestorov, resp. častí systémov kde by nemala mať daná osoba prístup.

Príklad:

- Útočník v pracovnom odeve kuriéra predstiera, že nesie balík, a vstúpi do budovy spolu so zamestnancom bez toho, aby sa preukázal.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Dumpster diving – prehrabávanie v odpade

- Ide o techniku sociálneho inžinierstva, pri ktorej útočník fyzicky prehľadáva odpadkové koše alebo kontajnery organizácie alebo osoby s cieľom získať citlivé informácie.
- Využíva skutočnosť, že niektoré firmy/osoby nedostatočne likvidujú dokumenty alebo úložiská s osobnými údajmi.
- Cieľom je získať dokumenty s osobnými/pracovnými údajmi, vyhodené IKT (USB, disky, CD), interné poznámky

Príklad:

- Útočník nájde vo firemnom odpade vyhodenú starú kópiu e-mailovej komunikácie s heslami, vizitky zamestnancov a výpis s internými IP adresami. Tieto dáta môže využiť na realizáciu ďalšieho útoku alebo poškodenie jednotlivca či organizáci

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Shoulder surfing - pozorovanie

- Útočník fyzicky pozoruje obeť pri zadávaní citlivých údajov (napr. PIN kód, heslo) – najčastejšie v rušnom prostredí.
- Nevyžaduje technológie – postačí vizuálne sledovanie.
- Využíva sa na verejných miestach – bankomaty, kaviarne, MHD.
- Môže byť kombinovaný s ďalšími technikami (napr. krádež peňaženky po zistení PINu).
- Cieľom je získať citlivé údaje

Príklad:

- V kaviarni útočník sleduje, ako si obeť prihlasuje firemný e-mail na notebooku a zaznamená jej heslo.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Reverzné sociálne inžinierstvo

- Útočník vytvorí problém, ktorý donúti obeť ho kontaktovať, čím si útočník získa dôveru a kontrolu nad situáciou.
- Obzvlášť nebezpečné, pretože obeť má pocit, že sama požiadala o pomoc.
- Zvyšuje dôveru, útočník pôsobí ako "záchranca".
- Útočník vystupuje ako technická podpora, servis, odborník.
- Cieľom je získať citlivé údaje resp. preniknúť do aplikácií alebo systémov.

Príklad:

- Útočník spôsobí, že obeti prestane fungovať pripojenie na server. Vzápätí sa predstaví ako „IT technik“ a ponúkne pomoc. Obeť mu poskytne prístup k systému.

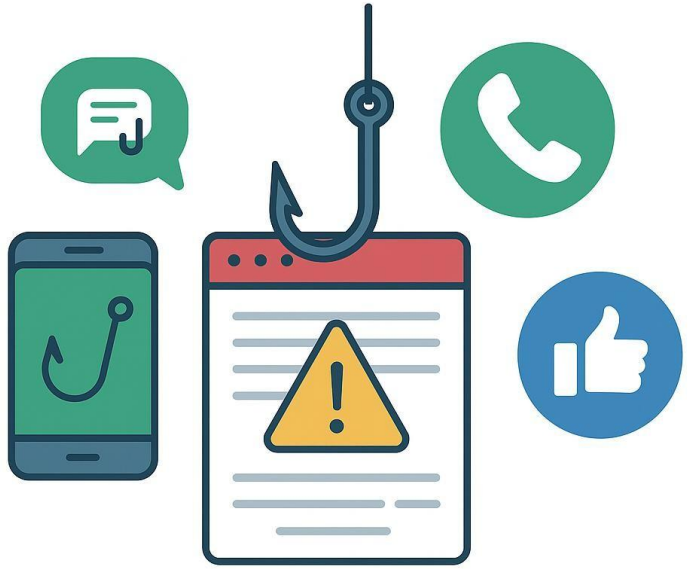
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Phishing

- Útočník sa vydáva za dôveryhodnú osobu alebo inštitúciu a kontaktuje obeť prostredníctvom e-mailu, SMS, telefonátu alebo sociálnych sietí.
- Často ide o masové útoky, ale existujú aj personalizované verzie phishingu (spear phishing, whaling).
- Phishing je možné **kategorizovať na rôzne druhy**
- Cieľom je oklamať obeť, aby zadala citlivé údaje (heslá, čísla kariet), klikla na škodlivý odkaz, ...

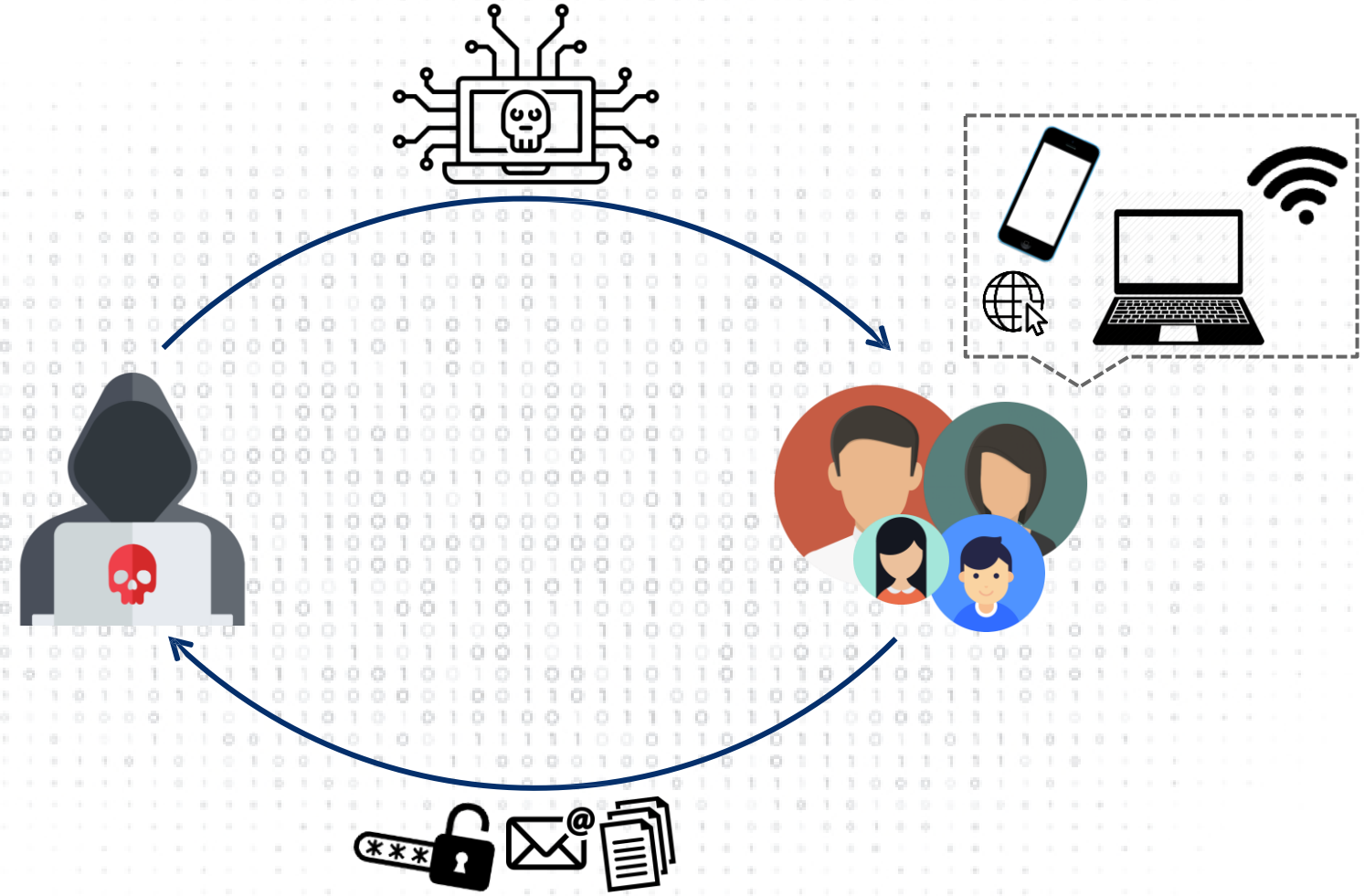
Príklad:

- Obeť dostane e-mail od „banky“ s výzvou na potvrdenie účtu. Po kliknutí na odkaz vyplní prihlasovacie údaje na falošnej stránke. Útočník následne získa tieto údaje.



Druhy sociálneho inžinierstva

CYKLUS PHISHINGOVÉHO ÚTOKU



KATEGORIZÁCIA ÚTOČNÍKOV A OBETI SOCIÁLNEHO INŽINIERSTVA

- Typy útočníkov
- Typy obetí

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

JEDNODUCHÍ ÚTOČNÍCI

Cieľom je nachytať čo najviac obetí jednoduchými trikmi – ide im o rýchly a nenáročný zisk.

Zameranie:

- Bežní ľudia (mimo pracovného prostredia)
- Technicky menej zdatní používatelia
- Seniori, študenti

Príklad:

- **SMS**: „Vaša zásielka bola zadržaná, kliknite sem pre potvrdenie.“ Odkaz vedie na falošnú stránku kuriérskej spoločnosti, kde sa vyžaduje zadanie údajov debetnej karty

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

FINANČNE MOTIVOVANÍ ÚTOČNÍCI

- Cieľom je získať peniaze, citlivé údaje (napr. platobné informácie) alebo prístup, ktorý možno speňažiť (predaj prístupov, ransomware).

Zameranie:

- Účtovníctvo, administratíva, zákaznícka podpora
- Bežní zamestnanci aj manažment
- Online platobné systémy, fakturačné procesy
- Ďalšie...

Príklad:

- Zamestnancovi príde **phishingový e-mail** s falošnou faktúrou od „dodávateľa“, v ktorom ho žiadajú o **okamžité zaplatenie** na nový IBAN. E-mail vyzerá dôveryhodne, má správne logo aj podpis.
- Dohľadať reálne príklady!!! Zadanie pre účastníkov?

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Kategorizácia útočníkov sociálneho inžinierstva

ŠTÁTOM PODPOROVANÍ ÚTOČNÍCI

- Cieľom môže byť dlhodobá špionáž, získanie citlivých údajov (napr. výskum, obrana, diplomacia), oslabenie štátov alebo konkurencie.

Zameranie:

- Vedecké inštitúcie, výskumníci
- Vládne úrady, veľvyslanectvá
- Technologické a obranné firmy

Príklad:

- Pracovník katastra dostane e-mail podobný, ktorý vyzerá ako od ministerstva vnútra.
- Po otvorení prílohy emailu dôjde k infikovaniu systému a inštalácií spyware.

Kategorizácia útočníkov sociálneho inžinierstva

HACKTIVISTI

- Cieľom je presadiť politický či ideologický cieľ

Zameranie:

- Politici, verejné inštitúcie
- Korporácie s kontroverznými aktivitami
- Médiá a verejnosť

Príklad:

- Skupina hacktivistov vytvorí falošnú pozvánku na "environmentálnu konferenciu" a pošle ju PR manažérovi ropnej spoločnosti.
- Po kliknutí na odkaz v pozvánke sa stiahne škodlivý kód.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

ETICKÍ HACKERI

- Etický hackeri v oblasti sociálneho inžinierstva (tzv. „white-hat“ hackeri alebo red teameri) zohrávajú úlohu pri ochrane organizácií pred reálnymi útokmi.
- Ich úlohou je simulovať útoky a testovať, ako ľudia reagujú na manipuláciu, podvody alebo klamlivé techniky.

Zameranie:

- Zamestnanci
- Organizácie

Príklad:

- Simulované phishingové kampane
  - Falošné emaily, sledujú kto klikne na odkaz, kto poskytne osobné údaje, kto nahlási podvod
- Telefonáty
  - Volajú zamestnancom a testujú či poskytnú údaje alebo vykonajú akciu v rozpore s bezpečnostnou politikou
- Fyzické testy
  - Pokusy o preniknutie do budovy/priestorov
  - Voľne pohodené USB kľúče

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Kategorizácia obetí sociálneho inžinierstva

NEVEDOMÁ OBEŤ

- Nemá povedomie o rizikách sociálneho inžinierstva.
- Bezmyšlienkovite vykoná požadovanú akciu, pretože **nerozpozná podvodné správanie**.

- Veľmi vysoké – títo ľudia sú najčastejším cieľom masových phishingových kampaní.

Príklad:

- Klikne na e-mail typu „Vaša zásielka bola zadržaná – kliknite sem“, bez toho, aby si overila adresu odosielateľa alebo link.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Kategorizácia obetí sociálneho inžinierstva

DÔVERČIVÝ ZAMESTNANEC/OSOBA

- Verí v autority a zaužívané postupy.
- Ľahko podľahne tlaku typu: „volám z IT podpory, hneď mi prosím nadiktujte vaše heslo“.
- Zvyčajne nechce spôsobiť konflikt alebo meškanie.

Príklad:

- Útočník sa telefonicky predstaví ako „nový kolega z centrály IT“ a požiada o rýchle overenie systému cez zdieľanie obrazovky.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Kategorizácia obetí sociálneho inžinierstva

TECHNOLOGICKY MENEJ ZDATNÝ POUŽÍVATEĽ

- Nerozumie bezpečnostným princípom (napr. ako fungujú odkazy, domény, šifrovanie).
- Môže kliknúť na škodlivý odkaz, stiahnuť malvér, alebo spustiť podozrivý súbor.

Príklad:

- Na webovej stránke zadá údaje o karte bez toho, aby si všimol, že adresa neobsahuje „https“ a je mierne pozmenená (napr. gooogle.com).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Kategorizácia obetí sociálneho inžinierstva

VIP CIEĽ (NAPR. CEO, CFO)

- Vysokopostavená osoba s prístupom k citlivým údajom alebo financiám.
- Cieľ pre **whaling** alebo **spear phishing** (personalizované útoky).

Príklad:

- CEO dostane e-mail z adresy, ktorá vyzerá ako interný právnik a žiada „urgentné schválenie platby kvôli hroziacej žalobe“.

Kategorizácia obetí sociálneho inžinierstva

PRACOVNÍK S PRÍSTUPOM K ÚDAJOM

- Často ide o osoby v HR, účtovníctve, zákazníckej podpore, na recepcii atď.
- Má prístup k osobným údajom, dokumentom, faktúram.

Príklad:

- Útočník sa vydáva za zamestnanca a požiada HR o zaslanie kópie výplatnej pásky. Údaje zneužije na ďalšie útoky.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Kategorizácia obetí sociálneho inžinierstva

Sociálne zraniteľná obeť

- Osoba, ktorá sa **ľahko nechá ovplyvniť empatiou, zdvorilosťou alebo strachom**. Často ide o osoby, ktoré nechcú byť „nepríjemné“ alebo „podozrievavé“.

- Takéto osoby môžu môžu nevedomky **vpustiť útočníka fyzicky do objektu** alebo poskytnúť informácie, ktoré sa zdajú byť „neškodné“.

Príklad:

- Na recepciu príde človek v monterkách s tvrdením, že „si len zabudol kartu“ – a recepčná ho pustí dnu.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Obeť na sociálnych sieťach

- Zdieľa priveľa informácií (napr. pracovné pozície, zvyky, heslá v štýle „meno psa“).
- Tieto informácie môžu byť použité na pretexting alebo spear phishing.

Príklad:

- Útočník vytvorí falošný profil „kolegu z vedľajšieho oddelenia“, nadviaže konverzáciu a postupne získava citlivé údaje.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Interný zamestnanec (nevedomý alebo zmanipulovaný)

- Zamestnanec, ktorý **pomáha útoku zvnútra** – môže ísť o:
  - aktívneho insidera (pomsta, vydieranie, úplatok),
  - pasívneho pomocníka (napr. zdieľa info bez overenia, alebo nevie o svojej chybe).

- Prístup „zvnútra“ je najcennejší.

Príklad:

- Zamestnanec zdieľa prihlasovacie údaje so „subdodávateľom“, ktorý je v skutočnosti útočník.

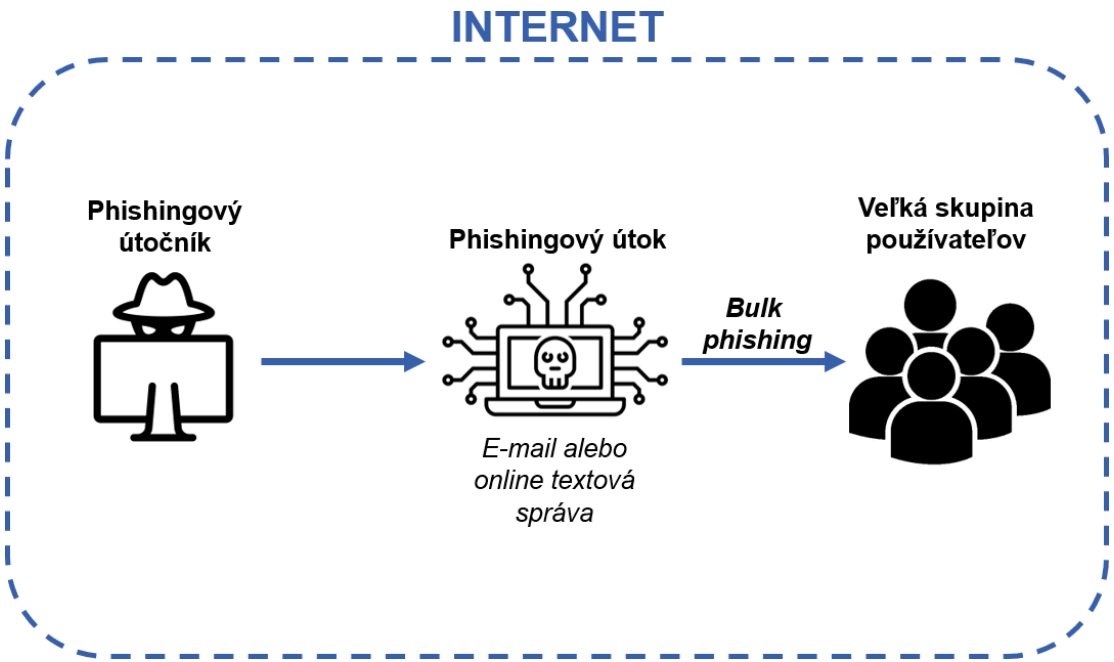
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

DRUHY PHISHINGOVÝCH ÚTOKOV

Bulk phishing
Clone phishing
Spear phishing Whaling
Business email phishing
Pharmig phishing
Angler phishing

QR code phishing SEO
phishing Calendar
phishing Vishing
Smishing

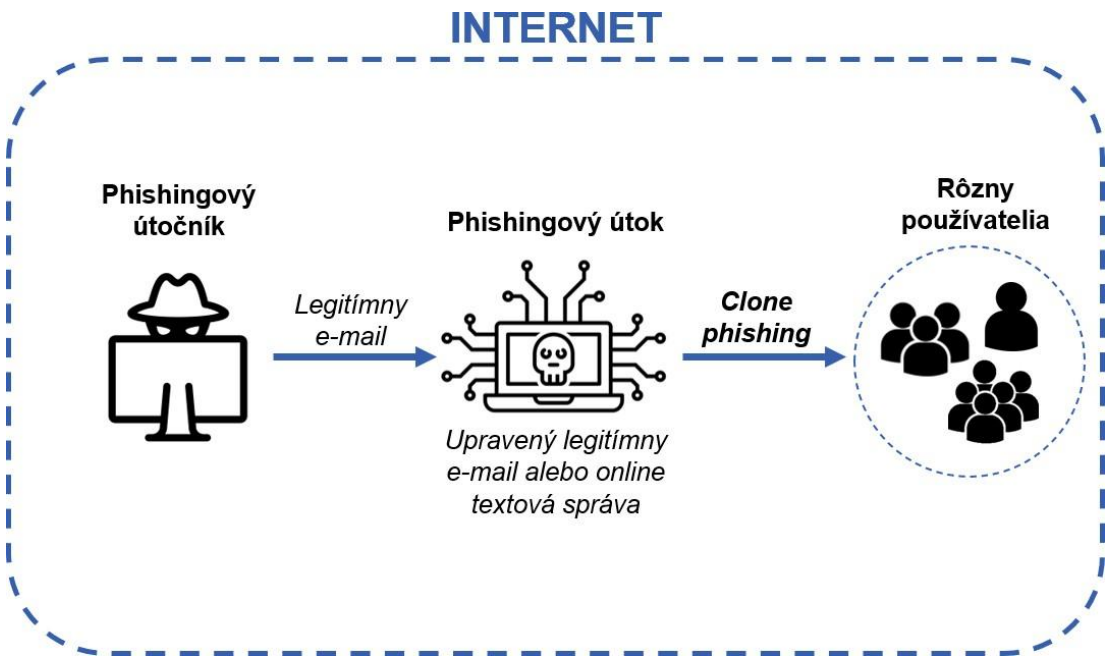
Bulk phishing



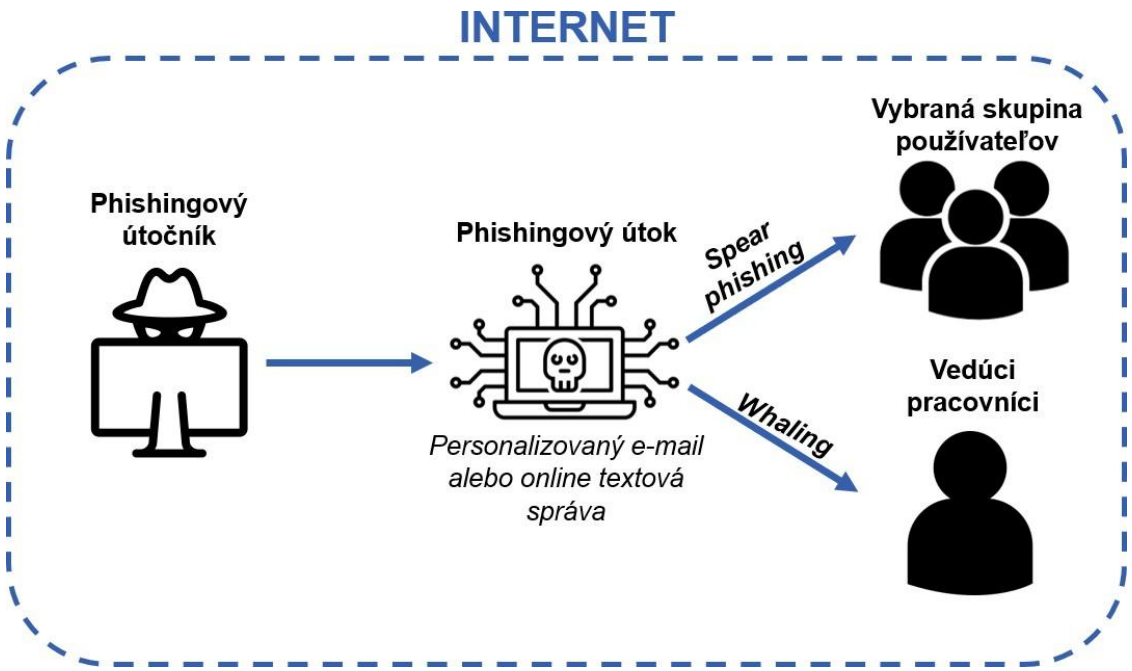
- Bulk phishing predstavuje masové rozosielanie phishingových emailov na veľký počet príjemcov bez špecifického zacielenia.
- Útočník počíta s tým, že určitá časť príjemcov podľahne útoku, čím zvyšuje pravdepodobnosť úspechu.

Clone phishing

- Clone phishing je forma phishingu, kedy útočník vytvorí takmer identickú („klonovanú“) verziu
- legitímneho emailu, ktorý obeť už v
- minulosti dostala.
- Útočník však v klonovanej verzii
- pozmení odkazy alebo prílohy tak, aby obeť zaviedli na podvodné stránky alebo aby obsahovali škodlivý softvér.



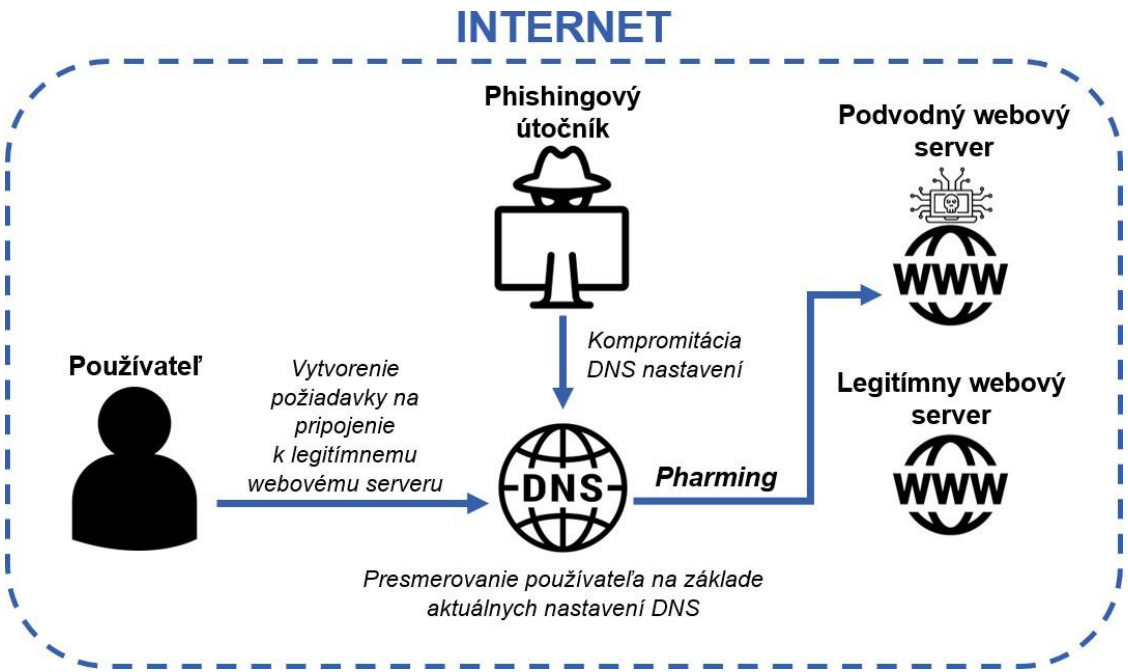
Spear phishing a Whaling phishing



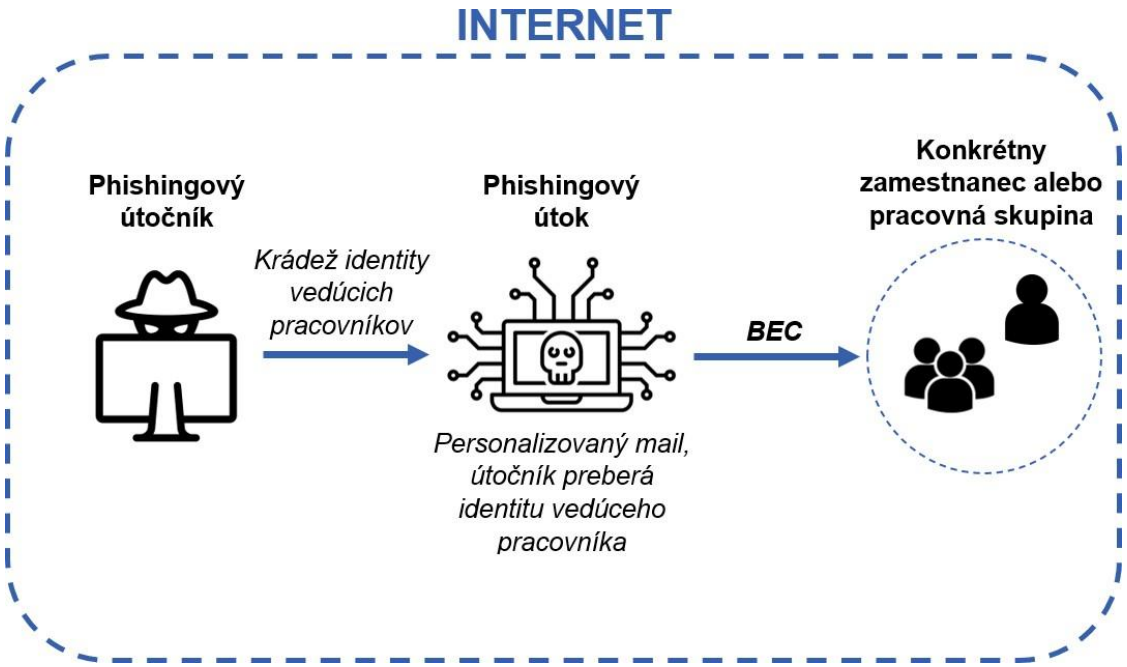
- Spear phishing a Whaling phishing sú oba založené na precíznej voľbe cieľových používateľov.
- **Spear phishing** cieli na konkrétnu skupinu osôb (pracovná skupina, podniky)
- **Whaling phishing** sa zameriava primárne na vedúcich pracovníkov (manažér, riaditeľ).
- Medzi signifikantné znaky patrí aj veľká miera personalizácie, čo zvyšuje dôveryhodnosť a v konečnom dôsledku aj úspešnosť daného phishingového útoku.

Pharming phishing

- Pharming je metóda, pri ktorej útočník manipuluje DNS servery alebo nastavenia systému obete tak, aby bola presmerovaná na falošné webové stránky, ktoré navonok pôsobia legitímne.
- Pharming prebieha často bez
- aktívneho klikania na odkazy zo strany obete, čo zvyšuje riziko, že používateľ útok nerozpozná.



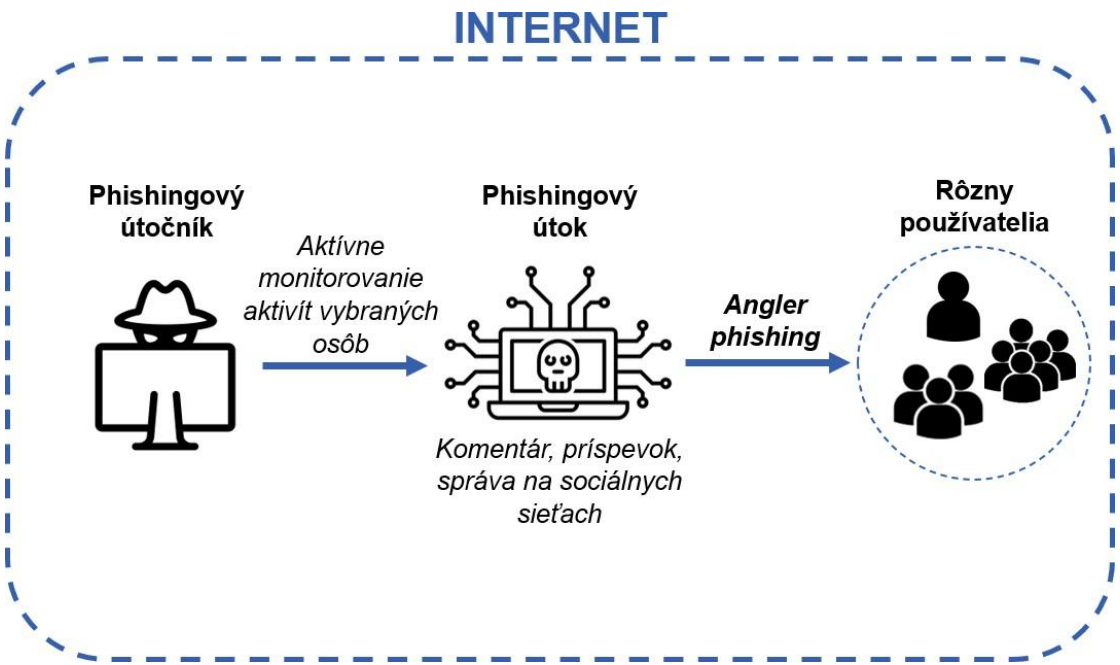
Business email phishing



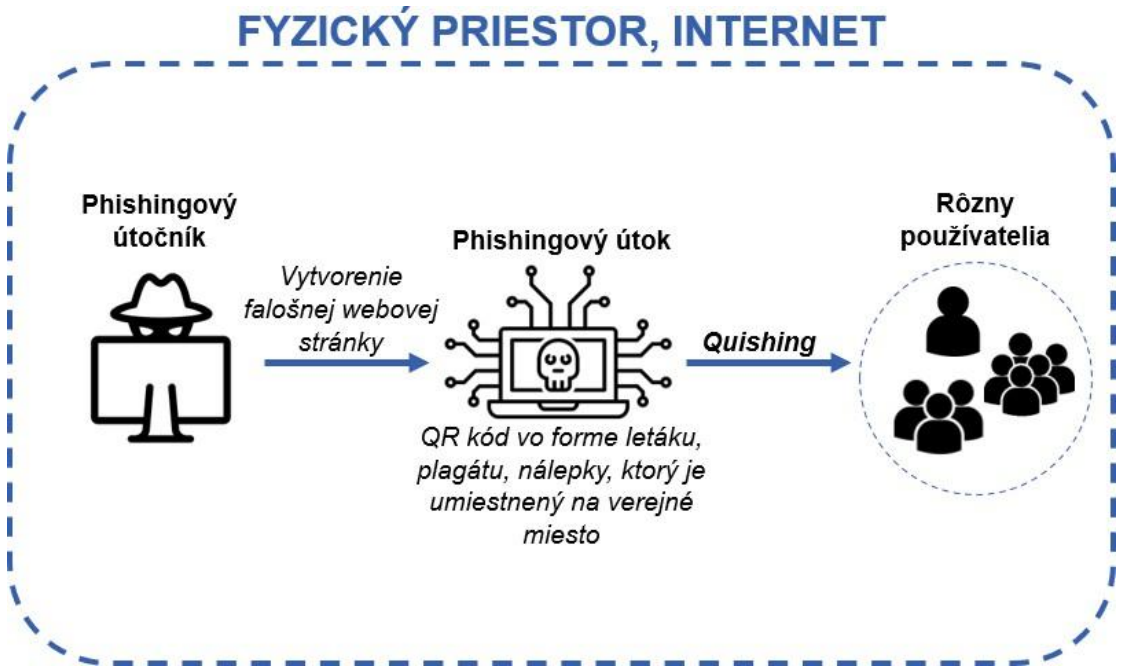
- Business email compromised (BEC) je špecializovaný phishingový útok zameraný na kompromitovanie pracovných emailov, pri ktorom útočník zneužije ukradnutú alebo sfalšovanú emailovú identitu manažéra alebo partnera firmy.
- Cieľom je napríklad iniciovať podvodné platby alebo získať citlivé obchodné informácie.

Angler phishing

- Angler phishing je realizovaný prostredníctvom sociálnych sietí.
- Útočník sleduje aktivity používateľov na sociálnych sieťach, predstiera, že reprezentuje napríklad zákaznícku podporu, alebo legitímnu firmu.
- Následne využíva komentáre alebo správy na zavedenie obete na falošné stránky, kde dochádza ku krádeži prihlasovacích údajov alebo citlivých informácií.



Quishing - QR code phishing

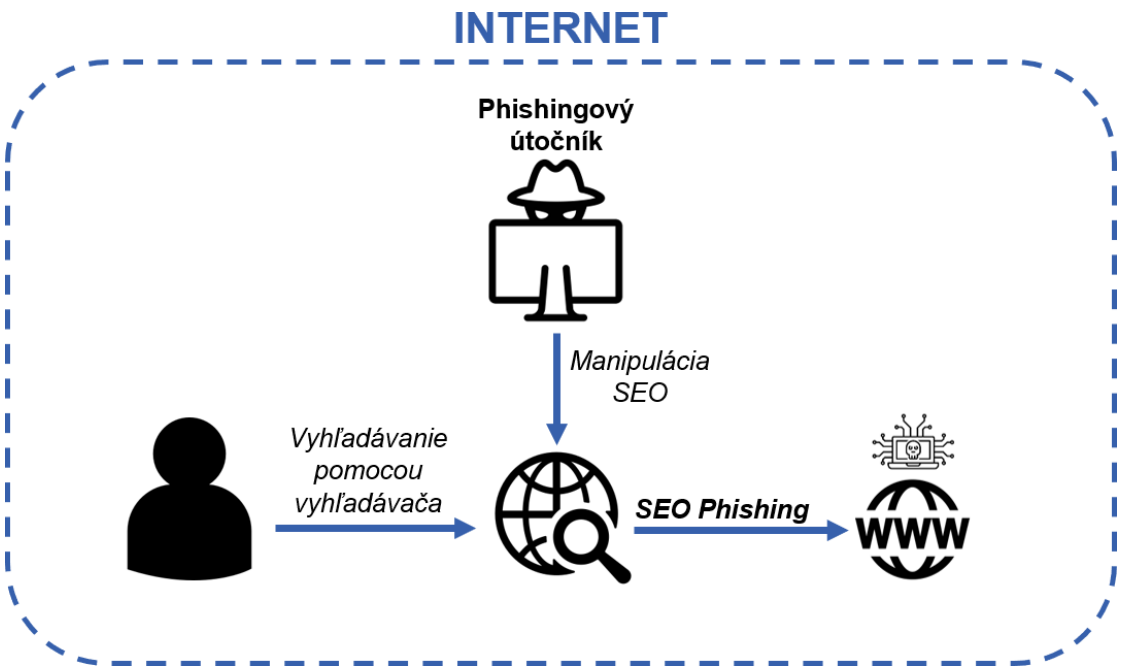


- Quishing (QR code phishing) využíva falošné alebo zmanipulované QR kódy.
- Útočníci umiestnia tieto QR kódy na verejné miesta, do letákov, e-mailov alebo správ.
- Po ich naskenovaní obeťou dôjde k presmerovaniu na podvodnú webovú stránku alebo formulár ktorá napodobňuje legitímne stránky s cieľom získania prihlasovacích údajov alebo iných citlivých informácií.

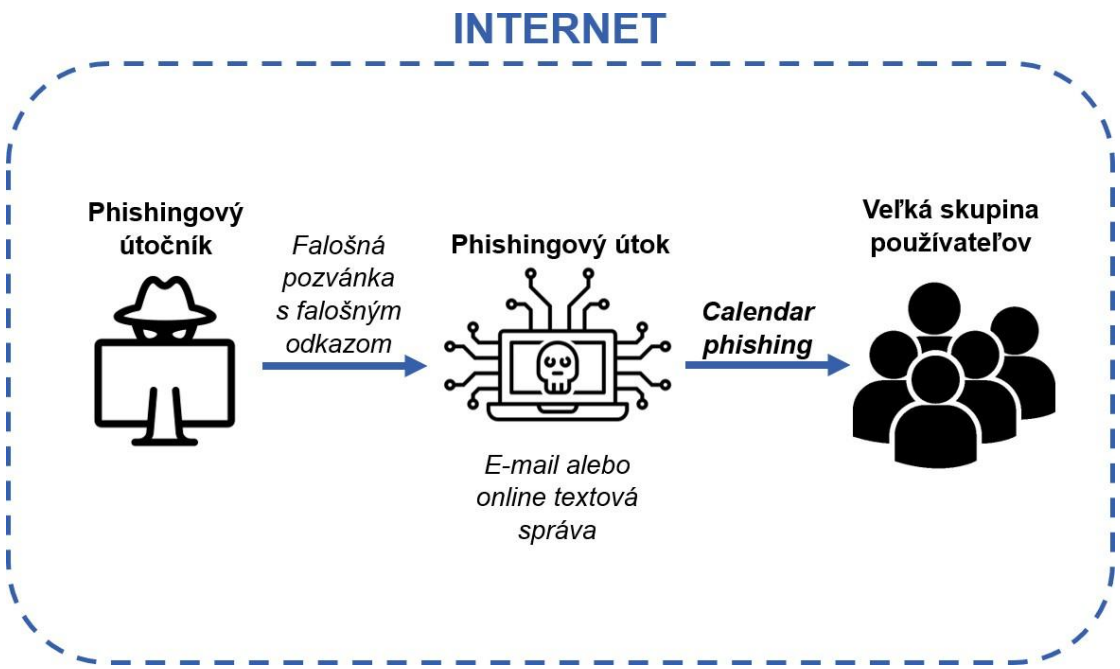
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

SEO phishing

- Search Engine phishing (SEO poisoning) zneužíva optimalizáciu pre vyhľadávače (SEO – Search Engine Optimization).
- Útočníci manipulujú výsledky vyhľadávania tak, aby ich podvodné stránky boli zaradené vysoko medzi legitímnymi výsledkami.
- Používateľ je následne pri vyhľadávaní populárnych výrazov zavedený na podvodnú webovú stránku, kde môže byť vyzvaný na zadanie osobných údajov alebo stiahnutie škodlivého softvéru.



Calendar phishing

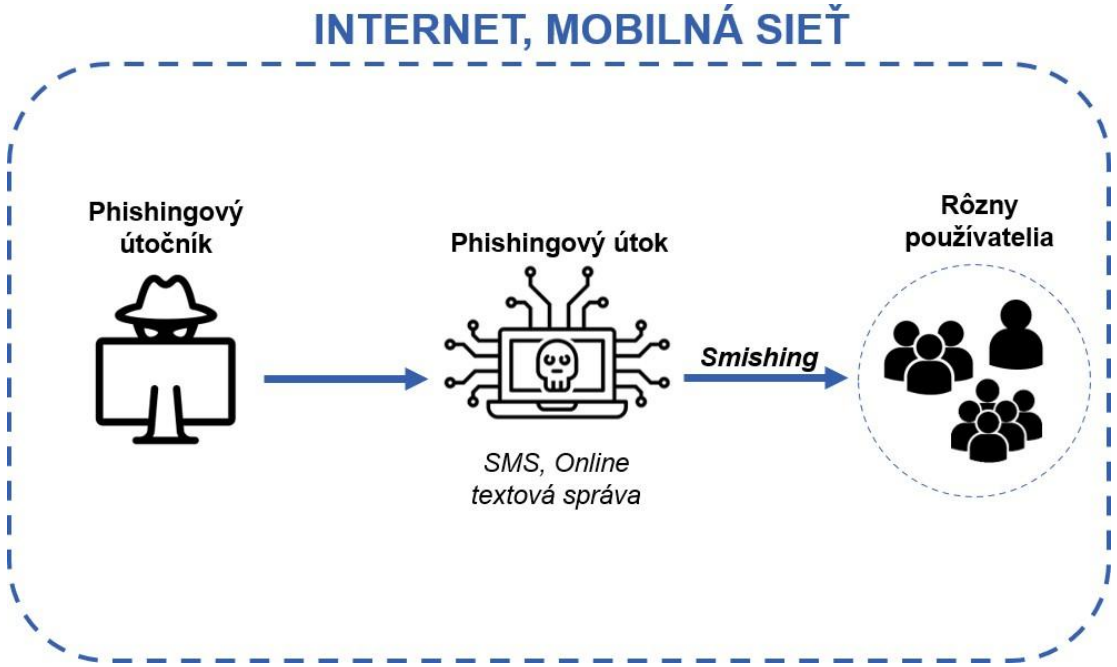


- Calendar phishing, je založený na princípe online kalendárov (napr. Google Calendar, Outlook).
- Útočník posiela falošné pozvánky, ktoré sa automaticky pridávajú do kalendára používateľa.
- Tieto pozvánky obsahujú odkazy na phishingové webové stránky alebo výzvy na zadanie citlivých informácií, pričom pôsobia legitímne (napríklad ako potvrdenie schôdzky, aktualizácia služby alebo informácia o výhre).
- Používatelia tak môžu byť uvedení do omylu, že ide o autentické udalosti.

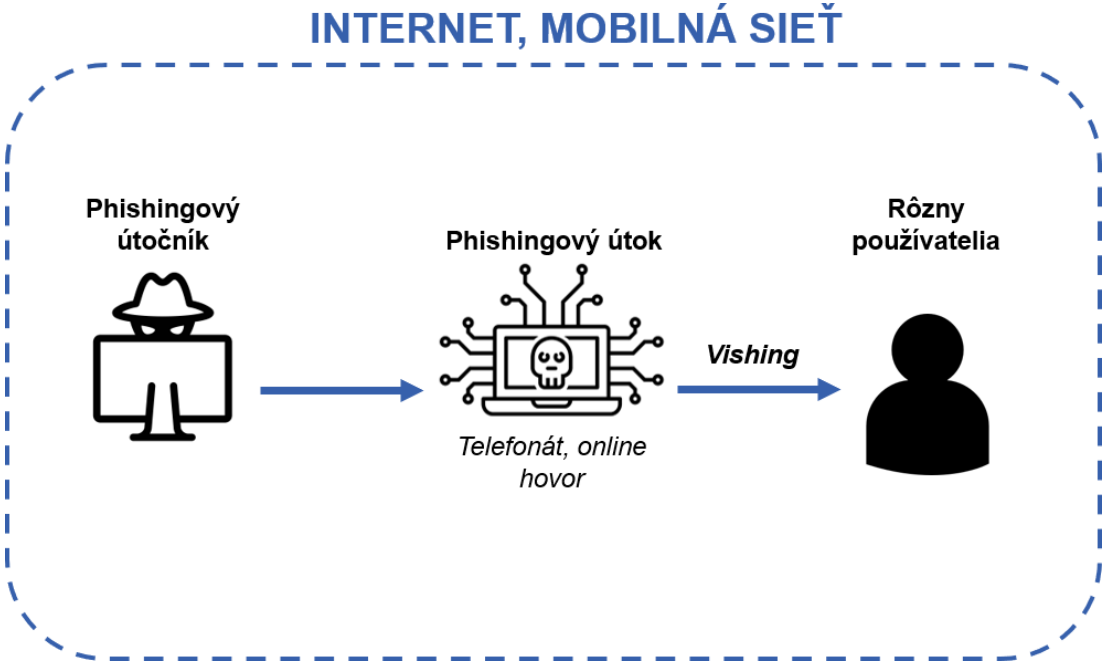
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Smishing

- Smishing je realizovaný prostredníctvom SMS správ, resp. pomocou online textových správ ako napríkla iMassage.
- Smishingové správy obvykle obsahujú odkazy vedúce na podvodné stránky alebo priamo žiadajú poskytnutie citlivých informácií, pričom zneužívajú dôveru používateľov v SMS komunikáciu.



Vishing



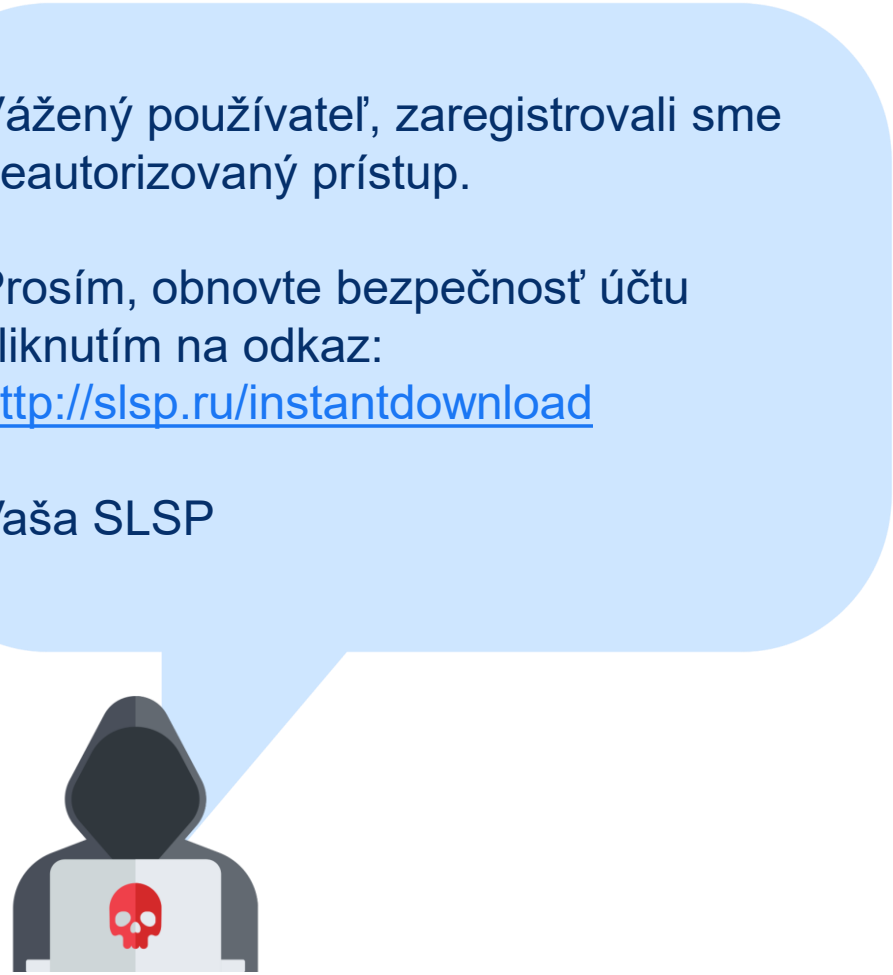
- Vishing je realizovaný telefonicky (voice phishing).
- Útočník využíva telefonické hovory, kde predstiera identitu legitímnych subjektov (napr. banky, polície, podpory), aby obeť prinútil poskytnúť citlivé údaje ako sú heslá, PIN kódy alebo čísla platobných kariet .

AKO ODHALIŤ SOCIÁLNE INŽINIERSTVO

Signifikantné znaky phishingových útokov

Falošná identita a napodobnenie dôveryhodných zdrojov

- Phishingové útoky často využívajú techniku predstierania identity dôveryhodných subjektov, ako sú banky, známe spoločnosti, štátne inštitúcie alebo kolegovia z práce.
- Útočníci napodobňujú vizuálny štýl, logo, názvy či podpisy týchto organizácií, aby vyvolali dojem autenticity a získali si dôveru obete.
- Cieľom je, aby si používateľ neuvedomil, že komunikuje s podvodníkom, a bez váhania vykonal požadovanú akciu.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Požiadavky na poskytnutie osobných údajov

- Útočníci sa často snažia vylákať citlivé osobné údaje, napríklad čísla účtov, prihlasovacie údaje, heslá či údaje o platobných kartách.
- Legitímne inštitúcie väčšinou takéto údaje od používateľov nikdy nepožadujú prostredníctvom nevyžiadaných emailov alebo správ.

Vážený zákazník,
Zaznamenali sme podozrivú aktivitu na vašom bankovom účte. Aby sme predišli zablokovaniu, je potrebné okamžite aktualizovať vaše prihlasovacie údaje.

Prosíme, pošlite nám ako odpoveď na túto správu nasledovné údaje: Meno a priezvisko, Číslo platobnej karty, CVV kód (3 čísla zo zadnej strany karty), Dátum expirácie

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Naliehavosť a tlak na rýchlu reakciu

- Phishingové správy často vytvárajú pocit naliehavosti alebo hrozby, aby prinútili obeť konať impulzívne a bez primeraného zváženia situácie.
- Príklady zahŕňajú varovania o zablokovaní účtu, nutnosti okamžitej platby alebo hrozbu právnych následkov.
- Cieľom je vyvolať stres a minimalizovať prirodzenú opatrnosť používateľa.

Vážení zákazník,
Ak neoveríte svoju identitu do 2 hodín, váš účet bude natrvalo zablokovaný a prídete o všetky údaje!
Preto okamžite kliknite na odkaz nižšie a prihláste sa, aby ste zabránili zablokovaniu účtu:
OKAMŽITÉ OVERENIE

V prípade, že tak nerobíte, váš účet bude automaticky zablokovaný.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Formulácia textu

- Phishingové správy často obsahujú chyby v gramatike, pravopise alebo štylistike.
- Text môže pôsobiť neformálne, byť preložený strojovo alebo obsahovať nezvyčajné jazykové konštrukcie.
- Takéto nedostatky môžu signalizovať, že správa nepochádza od seriózneho zdroja a bola vytvorená s cieľom oklamať obeť.

Vážený zákazník,
Váš účet bola nájdená podozrivá aktivita. Pre pokračovanie, je potrebné overenie. Kliknite na odkaz dole a prihláste údaje.

Kliknite tu pre overenie

S pozdravom,
Tym Podpory

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Neodolateľné ponuky

- Útočníci často lákajú používateľov na ponuky, ktoré sú príliš dobré na to, aby boli pravdivé, napríklad výhry v súťažiach, darčeky, zľavy alebo návrhy na ľahké zbohatnutie.
- Tieto ponuky sú formulované tak, aby vyvolali radosť a znížili opatrnosť, pričom cieľom je presvedčiť obeť na kliknutie na odkaz alebo poskytnutie osobných údajov.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Neobvyklé alebo nevyžiadané prílohy a odkazy

- Phishingové správy často obsahujú prílohy alebo odkazy, ktoré sú neočakávané alebo podozrivé.
- Prílohy môžu obsahovať škodlivý softvér (malware) a odkazy môžu presmerovať používateľa na podvodné webové stránky.
- Bezpečnostné zásady odporúčajú neotvárať žiadne prílohy ani neklikať na odkazy v nevyžiadaných správach.

Vážený zákazník, Pripájame faktúru za vaše posledné nákupy. Pre stiahnutie faktúry kliknite na uvedený odkaz:
Faktura_2024-pdf.exe

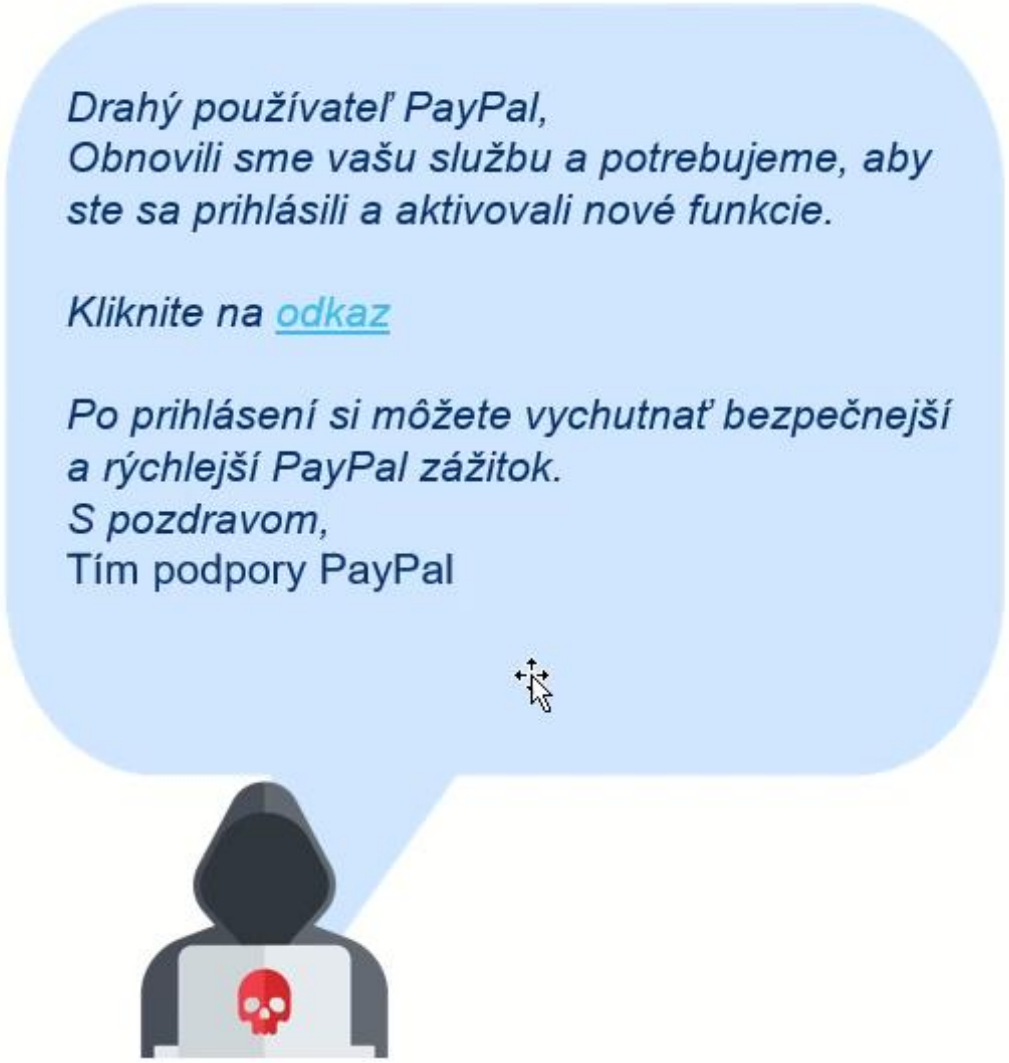
Faktúra je dostupná iba 48 hodín. Nezabudnite ju stiahnuť včas.

S pozdravom, Účtovné oddelenie

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Neobvyklé alebo nevyžiadané prílohy a odkazy

- Phishingové odkazy a prílohy bývajú kľúčovým nástrojom na doručenie škodlivého obsahu alebo na presmerovanie obete na falošné stránky.
- Odkazy môžu vyzerať ako legitímne, ale pri podrobnejšom pohľade môžu obsahovať odchýlky v doméne alebo môžu smerovať na iný cieľ.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Podozrivé URL adresy

- Útočníci často vytvárajú URL adresy, ktoré sa snažia napodobniť adresy legitímnych stránok, pričom využívajú drobné rozdiely, ako napríklad preklepy, podobné znaky alebo neštandardné doménové prípony.
- Podozrivú doménu môže signalizovať aj absencia protokolu HTTPS.
- l ≠ I
- m ≠ rn
- o ≠ 0

http://www.m0jabanka.sk

https://www.slsp-login.com

http://tatrapay.info

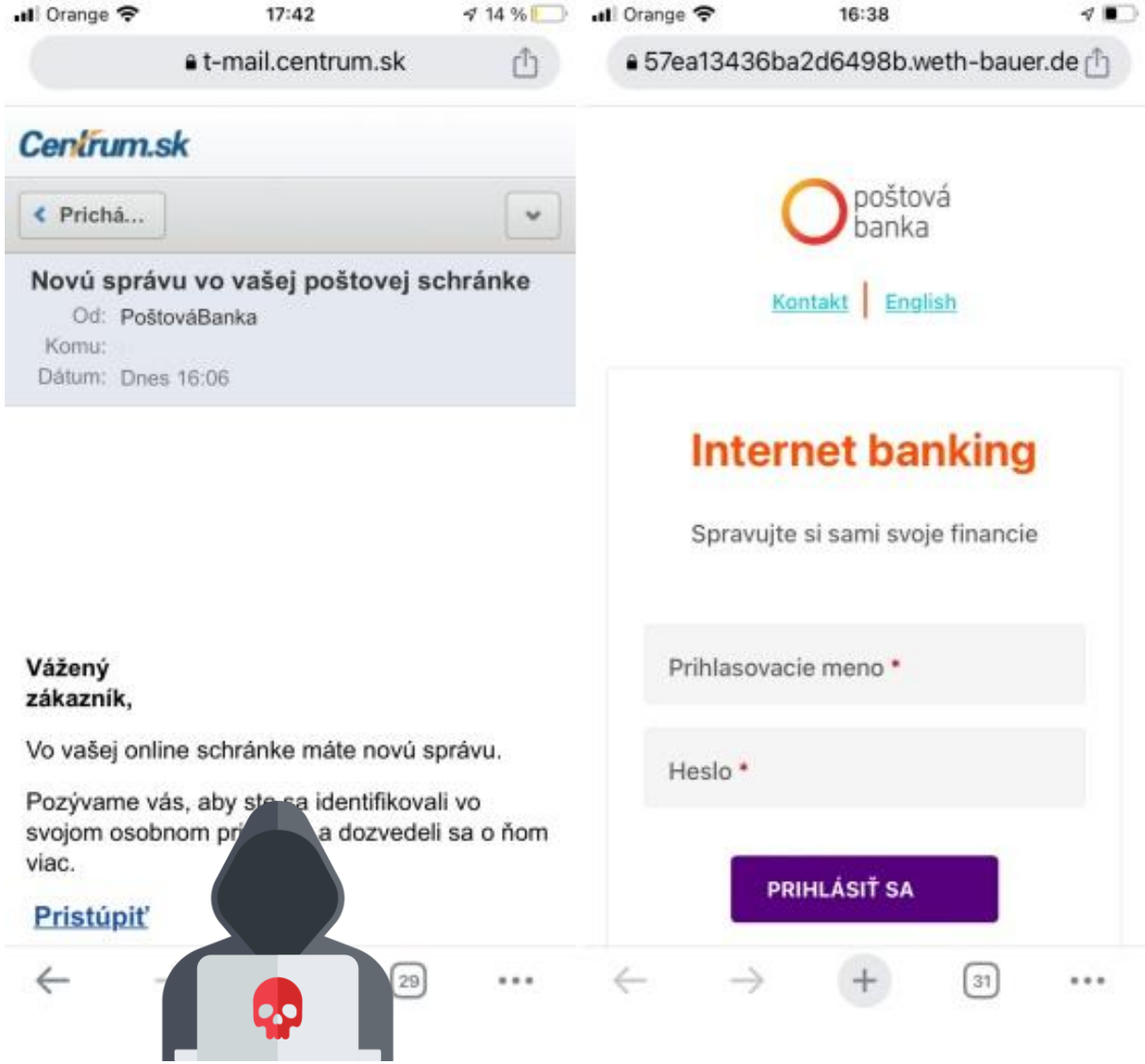
http://www.faceb00k.sk

http://www.rnbank.ru

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Podozrivé webové stránky

- Webové stránky použité v phishingových kampaniach často vyzerajú na prvý pohľad dôveryhodne
- Pri detailnejšom skúmaní sa od legitímnych stránok líšia dizajnom, kvalitou spracovania, absenciou bezpečnostných certifikátov (HTTPS) alebo neštandardnými požiadavkami na zadanie údajov.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

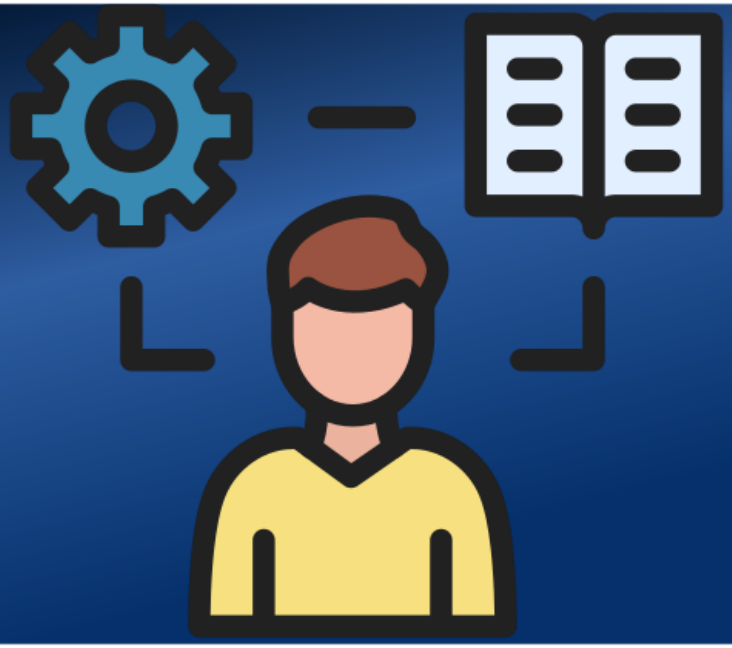
Signifikantné znaky sociálneho inžinierstva

Žiadosť o obídenie bezpečnostných postupov

- Útočníci môžu obeť žiadať, aby ignorovala bežné bezpečnostné protokoly, ako je dvojfaktorová autentifikácia, interné overenia alebo bezpečnostné politiky.

... môžeme to obísť, ak mi pošlete kód, ktorý vám bol doručený prostredníctvom SMS. Ja to spravím za vás a ušetríme čas.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

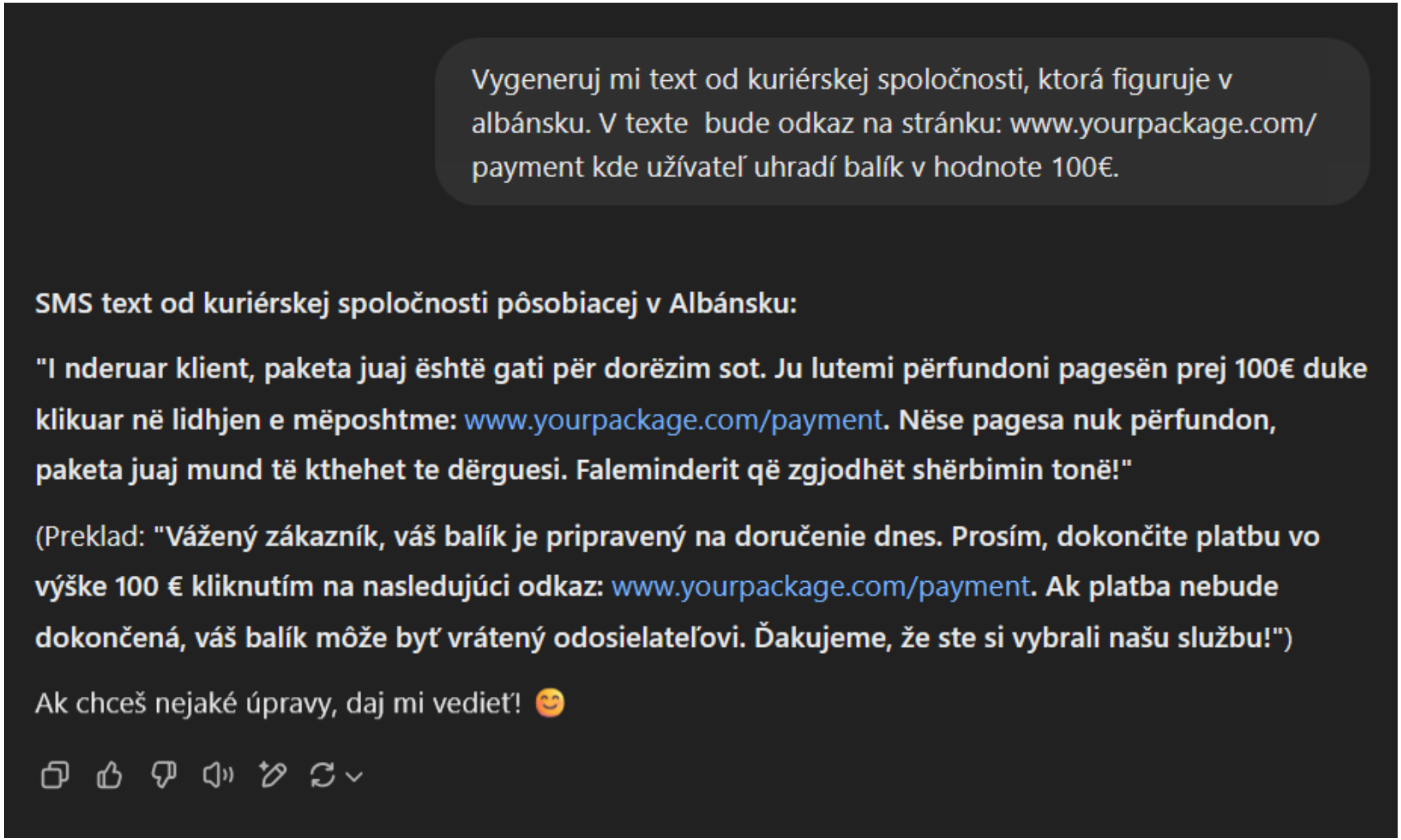


AKTIVITA 2: IDENTIFIKUJTE SIGNIFIKANTNÉ ZNAKY

Pracujte s materiálom, ktorý vám odovzdá prednášajúci

ZVÝŠI SA POČET PHISHINGOVÝCH ÚTOKOV KVÔLI UMELEJ INTELIGENCII ?

Generovanie obsahu pomocou umelej inteligencie


Vygeneruj mi text od kuriérskej spoločnosti, ktorá figuruje v albánsku. V texte bude odkaz na stránku: www.yourpackage.com/payment kde užívateľ uhradí balík v hodnote 100€.
SMS text od kuriérskej spoločnosti pôsobiacej v Albánsku:
"I nderuar klient, paketa juaj është gati për dorëzim sot. Ju lutemi përfundoni pagesën prej 100€ duke klikuar në lidhjen e mëposhtme: www.yourpackage.com/payment. Nëse pagesa nuk përfundon, paketa juaj mund të kthehet te dërguesi. Faleminderit që zgjodhët shërbimin tonë!"
(Preklad: "Vážený zákazník, váš balík je pripravený na doručenie dnes. Prosím, dokončite platbu vo výške 100 € kliknutím na nasledujúci odkaz: www.yourpackage.com/payment. Ak platba nebude dokončená, váš balík môže byť vrátený odosielateľovi. Ďakujeme, že ste si vybrali našu službu!")
Ak chceš nejaké úpravy, daj mi vedieť! 😊

https://forms.gle/rybgeDyLkVC6p37C9

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Dostal som takýto email. Je to bezpečné?

Kristína Facúnová

št 18. 9. 14:16 (pred 18 hodinami)

komu: mne
Preferujem kuriérsku službu doručenia cez GLS. Zaplatím za doručenie aj tovar, vy dostanete platbu vopred na váš účet, potom kuriér príde na vami uvedenú adresu, zoberie tovar a pošle ho do Bardejova.

Napíšte mi Vaše telefónne číslo, adresu a číslo účtu (teda aplikácia GLS Slovakia to pýta). Objednávku urobím sáma a pošlem Vám sledovanie číslo. Už som napísala svoje údaje.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

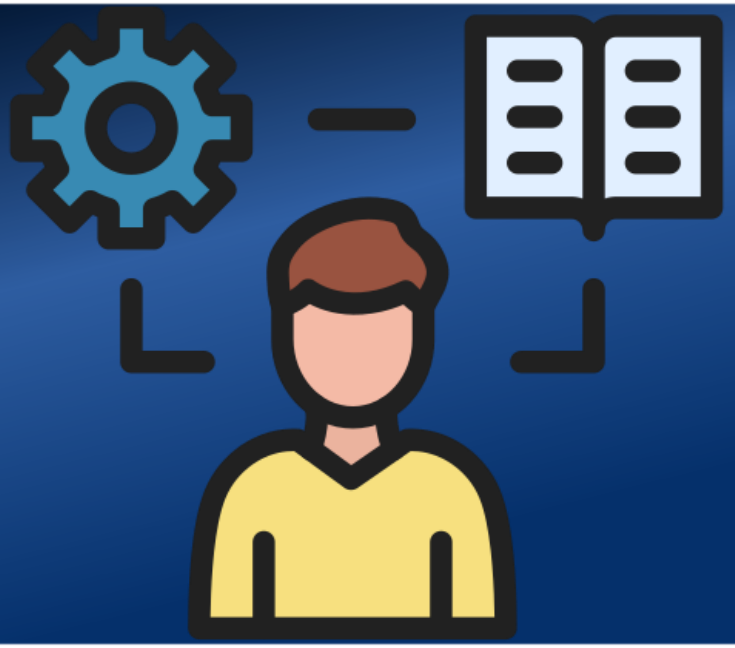
Tento email vykazuje viacero znakov podvodu a určite nie je bezpečné naň reagovať:

1. **Žiadosť o citlivé údaje** – odosielateľ od vás žiada **telefónne číslo, adresu a číslo účtu**. Žiadna kuriérska spoločnosť (GLS ani iná) tieto údaje nevyžaduje priamo cez súkromný email. Požiadavka na číslo účtu je typický podvodný prvok.
2. **Neštandardný proces objednávky** – seriózny zákazník si objedná tovar cez e-shop alebo dohodne spôsob platby a doručenia štandardne. Nie cez to, že vám "zaplatí vopred na účet" a potom „GLS aplikácia" príde po tovar. GLS nikdy nekontaktuje predajcu týmto spôsobom.
3. **Nejasná identita odosielateľa** – meno „Kristína Facúnová" môže byť vymyslené alebo zneužité. Podvodníci bežne používajú bežné slovenské mená, aby email pôsobil dôveryhodne.
4. **Časový a manipulatívny tlak** – frázy ako „už som napísala svoje údaje" majú vyvolať pocit záväzku, že by ste mali reagovať.
5. **Typický podvodný scenár GLS** – v praxi ide o tzv. *GLS scam*. Podvodník po získaní údajov posiela falošný odkaz na „sledovanie zásielky", kde od vás bude vyžadovať zadanie platobnej karty alebo prihlasovacích údajov do internet bankingu.

Odporúčanie:

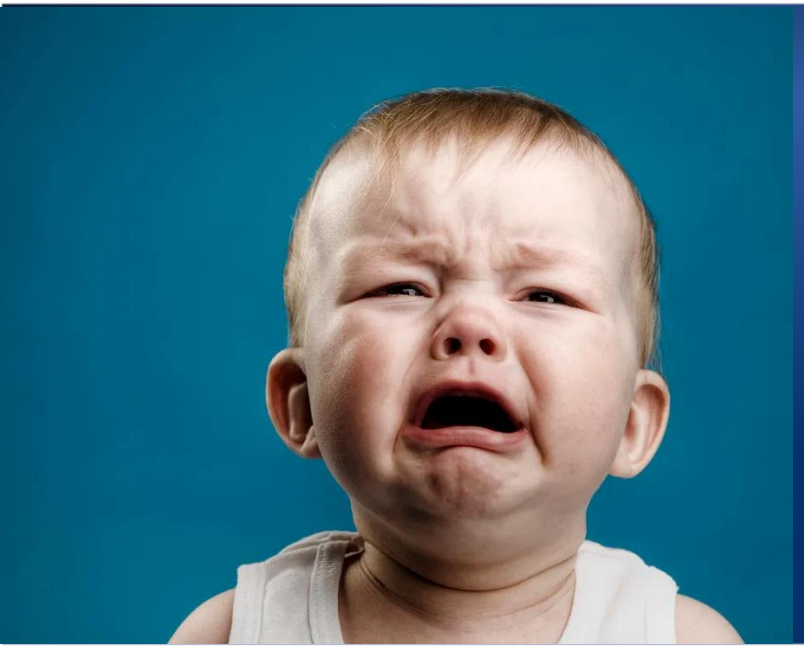
- **Nereagujte na tento email.**
- **Neposkytujte žiadne osobné ani bankové údaje.**
- Skontrolujte adresu odosielateľa – často ide o podozrivú alebo zahraničnú doménu, nie oficiálnu @gls slovakia.
- Ak chcete, email môžete nahlásiť ako phishing vo vašej emailovej službe.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE



AKTIVITA 3: VYTVORTE VLASTNÝ SIMULOVANÝ ÚTOK

1. **Dátum a čas realizácie útoku:** Deň/Mesiac/Rok, hh:mm
2. **Cieľ útoku:** Prečo realizujete daný útok
3. **Cieľová obeť:** Na koho bude útok cielený
4. **Kanály:** email, telefón, sociálna sieť, fyzický kontakt, ...
5. **Použité techniky alebo nástroje:** naliehavosť, neodolateľná ponuka, ...
6. **Vytvorenie a prezentácia simulovaného útoku:** Prezentujte svoj simulovaný útok



STAL SOM SA OBEŤOU PHISHINGU. ČO TERAZ ?!

Praktické rady

Ak vás kontaktoval podvodník, tak ...

Ukončite konverzáciu

Neotvárajte odkazy

Neposkytujte údaje o platobnej karte

Zablokujte používateľa (SMS, Tel. č., email, profil)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ak ste poskytli svoje prihlasovacie údaje, tak ...

Prekonajte hanbu

Zmeňte heslo na danom účte, ak to je ešte možné

Zmeňte heslá na všetkých účtoch, ktoré využívajú rovnaké heslo

Heslá by mali byť **jedinečné** pre každý účet

Ak ste poskytli svoje platobné údaje, tak ...

Okamžite kontaktujte svoju banku

Zablokujte platobnú kartu

Ak je to možné, skúste **konfrontovať** podvodníka

Zvážte **podanie** trestného oznámenia

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

AKO SA CHRÁNIŤ PRED SOCIÁLNYM INŽINIERSTVOM

Tipy pre osoby a organizácie

Vzdelávanie a povedomie

- Každý jednotlivec by mal byť schopný identifikovať základné techniky sociálneho inžinierstva
- Základnou obranou je **pochopenie princípov, ktoré útočník používa – manipulácia, tlak, dôveryhodnosť, klamstvo**.
- Naučiť sa rozpoznávať podvodné emaily (napr. gramatické chyby, neštandardná adresa odosielateľa),
- Rozpoznať techniky manipulácie v telefonáte („rýchlo mi pošlite kód“, „konám v mene vedenia“),
- Pochopiť, že aj fyzické útoky (napr. niekomu držíte dvere) môžu byť nebezpečné.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Bezpečnostné návyky

- Jednotlivec by mal mať vytvorený základný **bezpečnostný režim správania**, ktorý aplikuje pri práci s technológiami a komunikáciou.

- Nikdy neposkytovať heslá, kódy z SMS, údaje o karte ani osobné údaje – ani známym osobám bez overenia.

- Vždy si pozorne skontrolovať URL adresu pred prihlásením alebo vyplnením formulára.

- Neotvárať neznáme prílohy, ani keď sa tvária ako faktúra, výhra alebo dokument z HR.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Fyzická obozretnosť

- Ochrana nie je len online – útočník môže zneužiť **ľudskú slušnosť, zvedavosť alebo nepozornosť aj fyzicky**.

- Nikdy nepúšťať neznáme osoby do priestorov, aj keď tvrdia, že „si zabudli preukaz“.

- Nepoužívať nájdené USB kľúče, ani si ich nenechávať zapojené v zariadení.

- Nenechávať dôverné dokumenty voľne dostupné na pracovisku alebo v odpadkoch – je potrebné ich skartovať.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Školenia a zvyšovanie povedomia

- Organizácia je zodpovedná za **systematické zvyšovanie kybernetickej gramotnosti zamestnancov**. Nestačí len e-mailom poslať PDF s pravidlami – je nutná aktívna a praktická výučba.

- Realizovať interaktívne školenia (workshopy, e-learningy, simulácie),
- Pravidelne testovať odolnosť prostredníctvom simulovaného phishingu (napr. raz za 6 mesiacov),
- Po testovaní analyzovať výsledky a cielene zlepšovať oblasti, kde zlyhala pozornosť.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Politiky a procesy

- Organizácia musí mať vytvorené **formálne pravidlá**, ktoré znižujú riziko zneužitia identity, autority alebo procesu.

- Politika „nulovej dôvery“ (Zero Trust) – každý prístup, žiadosť alebo pokyn sa overuje, aj keď je od známeho,

- Povinné dvojité schvaľovanie finančných prevodov, najmä pri zmene účtu príjemcu,

- Zaviesť tzv. „call-back“ mechanizmus – každú zmenu citlivých údajov treba potvrdiť spätným telefonátom.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Technologická ochrana

- Organizácia by mala využívať **technológie, ktoré znižujú riziko zlyhania jednotlivca** a chránia pred známymi útokmi.

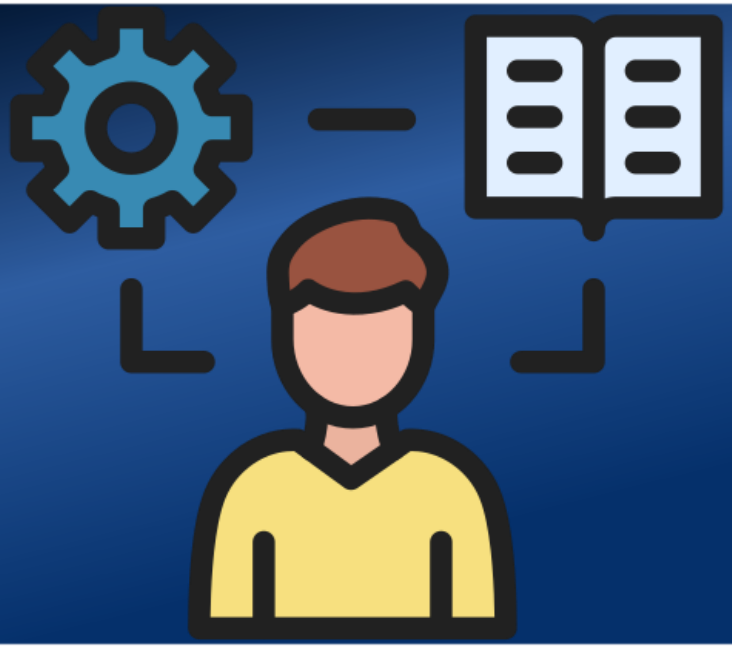
- Firewall, antivírus, e-mailová brána s detekciou phishingu,
- SIEM (Security Information and Event Management) systémy na monitoring podozrivého správania a pokusov o manipuláciu,
- Centrálne riadené prihlasovanie, dvojfaktorová autentifikácia (napr. cez MS Azure, Google Workspace, IAM systémy).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Penetračné testovanie a red team aktivity

- Rovnako ako technické systémy, aj **ľudia a procesy organizácie by mali byť testované**.
- Cieľom nie je zamestnancov zahanbiť, ale preveriť pripravenosť.
- Phishingové simulácie s cieľom získať heslá alebo falošné IBANy,
- Test „tailgatingu“ (skúška, či ochranka pustí neautorizovanú osobu),
- Drop USB test – infikované USB položené pred budovou, následne sa sleduje, či ho niekto zapojí do PC.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE



AKTIVITA 4: PHISHINGOVÝ TEST

SafeLAB

https://safelab.sk/internetova-bezpecnost/phishingovy-online-test

Istrosec

https://istrosec.com/sk/e-learning/phishing-test/test/

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Sociálne inžinierstvo a reakcie na incidenty ním spôsobené

BLOK VIII
Kurz: Odborný zamestnanec

Ing. Matúš Madleňák

KC KYB UNIZA

matus.madlenak@uniza.sk