



Kybernetická a Informačná bezpečnosť



CSIRT.SK

• Činnosti

- proaktívne
- reaktívne

• Aktuálne dve pobočky

- Bratislava
- Košice

• Medzinárodná a národná spolupráca

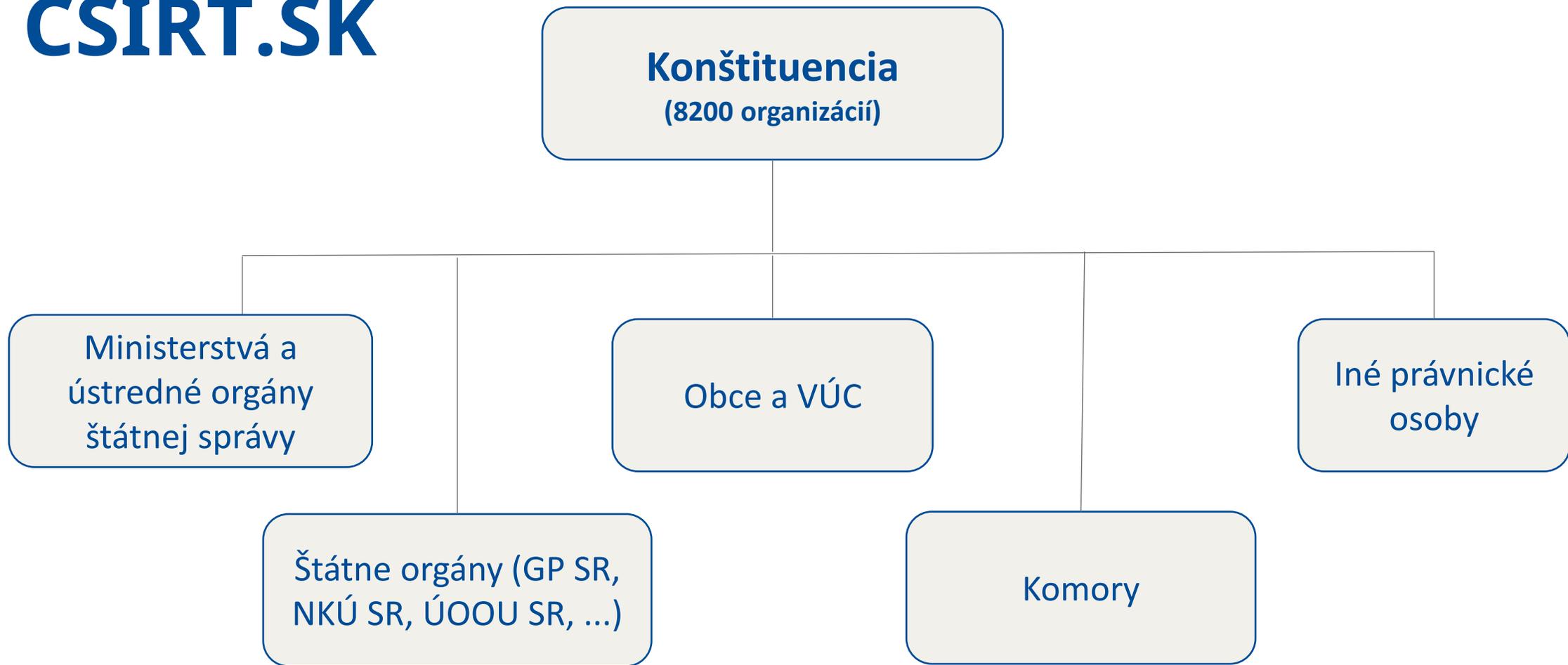
- FIRST (USA), TF CSIRT / Trusted Introducer, ENISA – CSIRTs Network (EÚ)
- iné CSIRT tímy
- akademický sektor



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



CSIRT.SK



Bezpečnostné hrozby



iROZHLAS



DOMOV SVĚT EKONOMIKA SPORT KULTURA VĚDA KOMENTÁŘE ŽIVOTNÍ STYL VOLBY POČASÍ

ONLINE: Koronavirus ve světě a v Česku - čtěte aktuální zprávy →

Kde se nacházíte: iROZHLAS.cz / Zprávy ze světa | Související témata: New Orleans USA kybernetický útok počítačová síť FBI

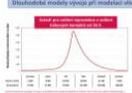
New Orleans čelí kybernetickému útoku. Starostka vyhlásila stav ohrožení a nechala vypnout servery

Americké město New Orleans vyhlásilo stav ohrožení kvůli kybernetickému útoku proti počítačovým systémům městské správy. Oznámila to televize CNN. Starostka LaToya Cantrellová nařídila preventivně vypnout všechny počítačové servery, které městské úřady používají. Na některých z nich se objevily útočné viry požadující výkupné.

New Orleans (USA) 12:31 14. prosince 2019     



ZPRÁVY, KTERÉ JSTE NEČETLI

 Modely šíření koronaviru v Česku. Nejhorší bude na přelomu září a října, odhadují statistici

 Hasiči dostali rozsáhlý požár opuštěného domu v Plzni pod kontrolu. Trať na Klatovy byla zavřená

 Lukašenko: Bělorusko uzavírá hranice s Polskem a Litvou. Na ukrajinských hranicích posílí kontrola

 Rousky jsme si možná měli nechat celé léto, připustil Babiš během interpelací před poslanci

Bezpečnosť z pohľadu používateľa



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

- je potrebné myslieť na súkromie a bezpečnosť
- povedali by ste cudziemu človeku vaše telefónne číslo, adresu kde bývate, aké máte auto alebo čo všetko sa nachádza vo vašom byte?
- venujte pár minút nastaveniu súkromia vášho profilu
- to čo raz zverejníte už ostane verejné
- v stávke je vaša reputácia a bezpečnosť
- všetky informácie o vás môžu byť použité pri útokoch sociálnym inžinierstvom

Cibulková ukázala doklady svojho priateľa. Neuvedomila si následky

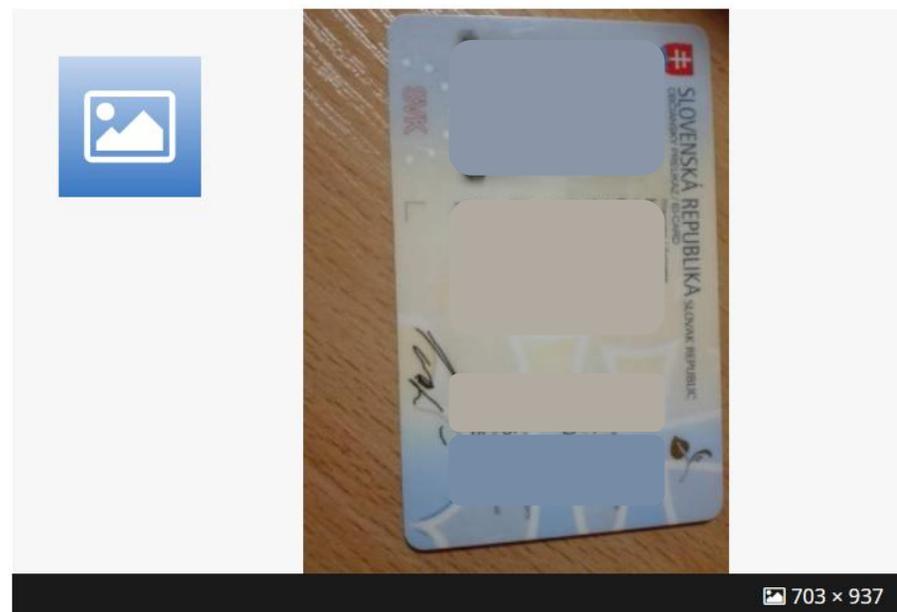
Odborník odporúča oba preukazy vymeniť.



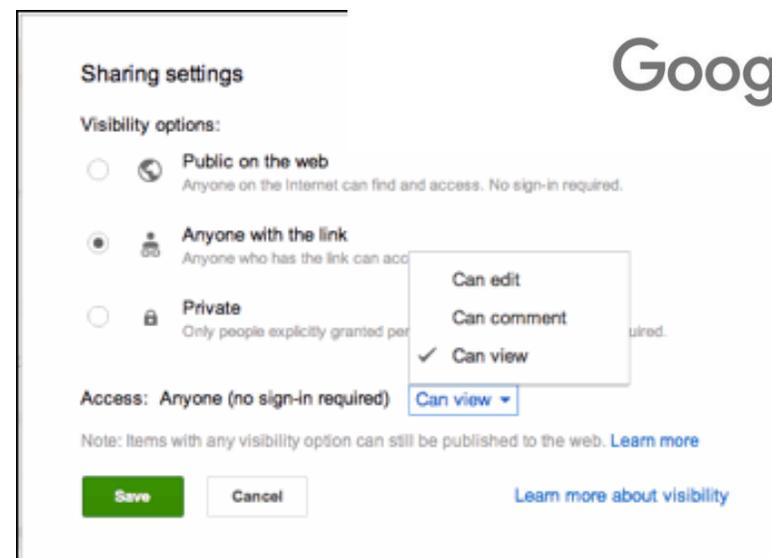
Bezpečnosť z pohľadu používateľa



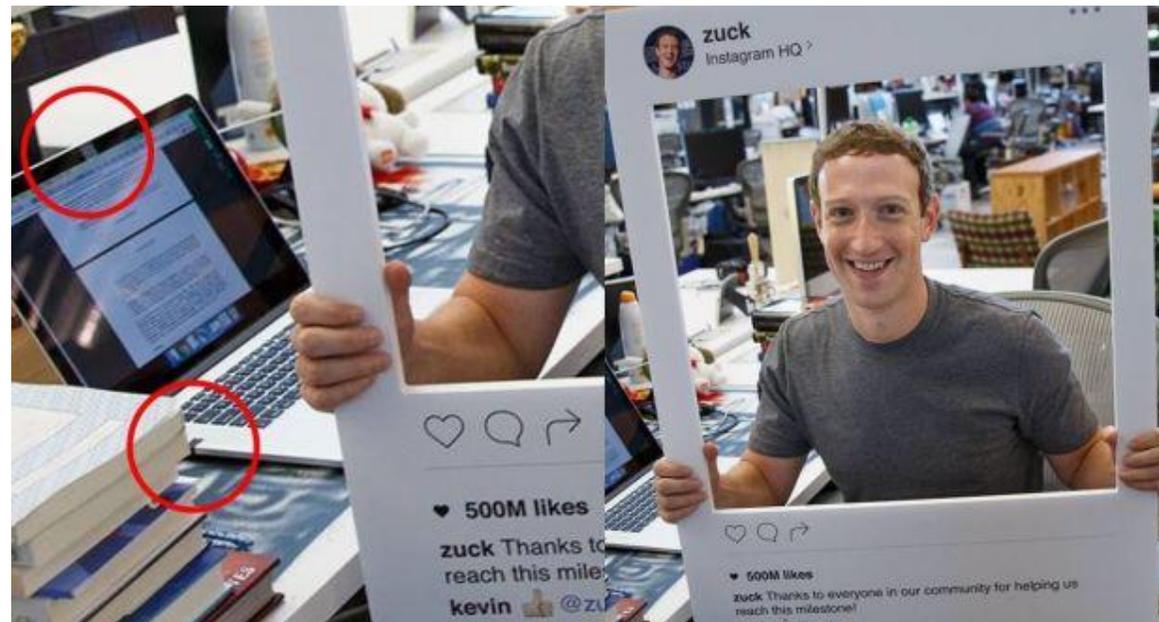
OP.jpg



Google Drive



Bezpečnosť z pohľadu používateľa



Bezpečne na sociálnych sieťach

- To čo raz zverejníte už ostane verejné
- Identita ľudí, s ktorými komunikujete online, môže byť falošná (podvodník, hacknutý účet kamaráta ...)
- Zábava, nie spoľahlivý zdroj informácií (algoritmy, emotívny obsah)
- Falošné účty, trollovia

The Social Dilemma
(dokumentárny film)





MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

SOCIÁLNE INŽINIERSTVO

Úvod k sociálnemu inžinierstvu

- Sociálne inžinierstvo - umenie manipulácie ľudí za účelom vykonania akcie alebo vyzradenia dôverných informácií.

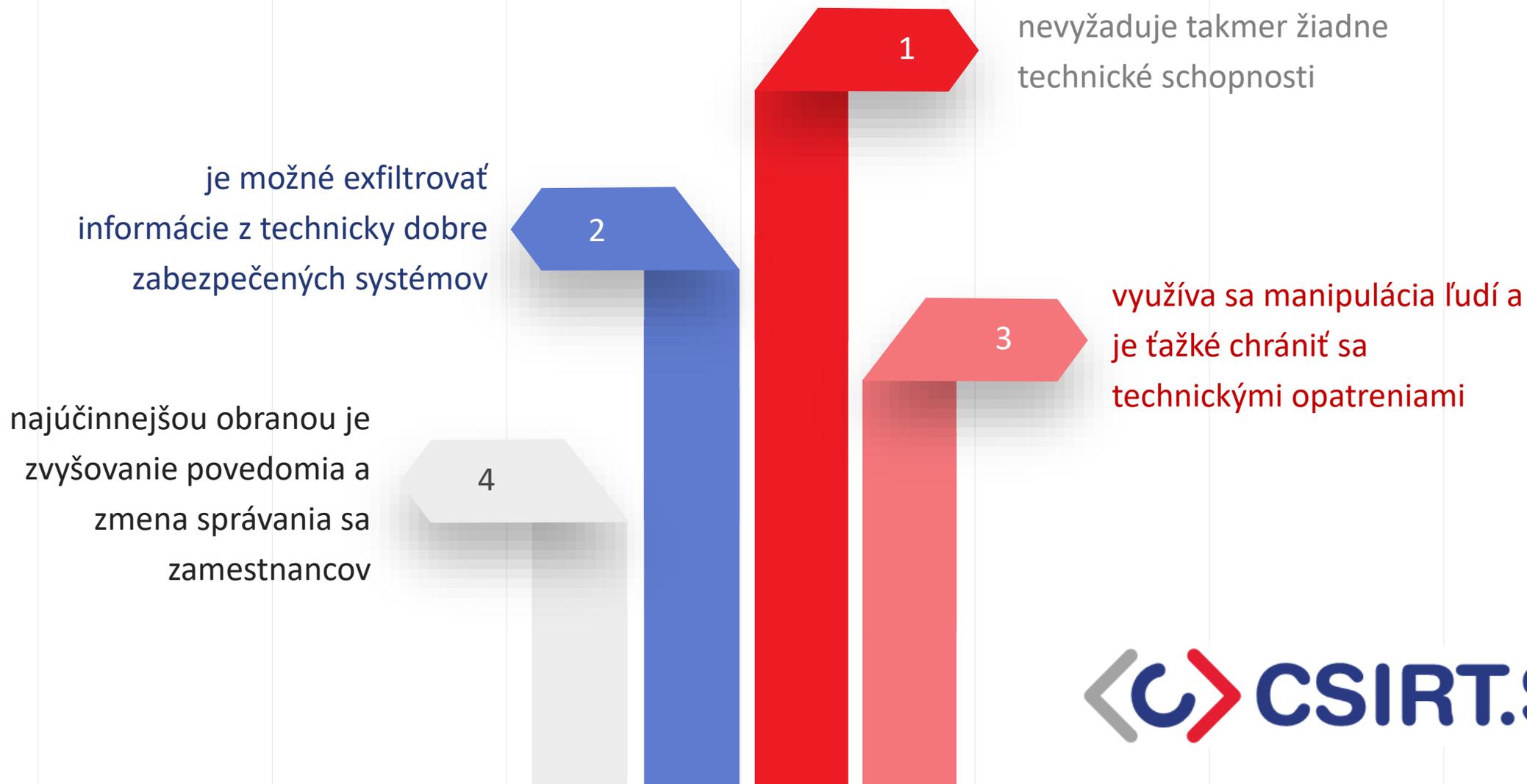
"Sociálne inžinierstvo používa vplyv a presvedčanie k oklamaniu ľudí tým, že ich presvedčí, že sociálny inžinier je niekto, kto nie je. V dôsledku toho môže sociálny inžinier využiť ľudí s cieľom získať informácie buď s použitím alebo bez použitia technológií."

Kevin Mitnick





Úvod k sociálnemu inžinierstvu





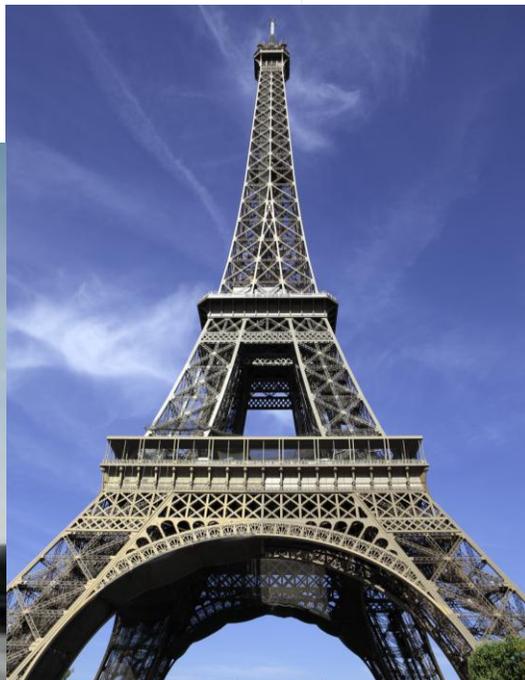
MINISTERSTVO

INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Úvod k sociálnemu inžinierstvu

„Všetko závisí od toho, ako sa pozeráme na veci, a nie od toho, aké sú.“

Carl Gustav Jung



Zdroj: https://www.freepik.com/free-photo/eiffel-tower_1064924.htm, <https://www.pexels.com/photo/people-walking-near-eiffel-tower-3305370/>

**Princípy
sociálneho
inžinierstva (I.)**

The diagram features a central light blue ring containing the title. Six speech bubble-shaped callouts point towards this center, each containing a principle. The callouts are arranged in two columns of three. The left column callouts are dark blue, grey, and dark blue. The right column callouts are red, blue, and red. The background has vertical light blue lines.

reciprocita

záväzok a
konzistencia

sociálne
preukázanie
správnosti/
sociálny vplyv

autorita

príťažlivosť

nedostatok



MINISTERSTVO

INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Ciele sociálneho inžinierstva

01

**získať citlivé osobné
informácie**

(adresa, dátum narodenia,
rodné číslo, údaje
o platobnej karte)

02

**získať prihlasovacie
údaje**

do informačných
systémov obete

03

**nainštalovať podvodné
aplikácie**

do počítača, tabletu,
alebo mobilného
telefónu,

04

spustiť škodlivý kód

z prílohy alebo
návštevou falošnej
webovej stránky

Typy útokov



SMISHING



PHISHING



SPEAR
PHISHING



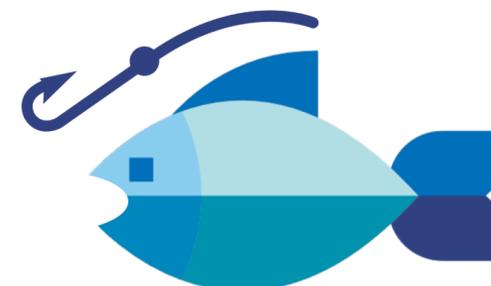
WHALING



VISHING



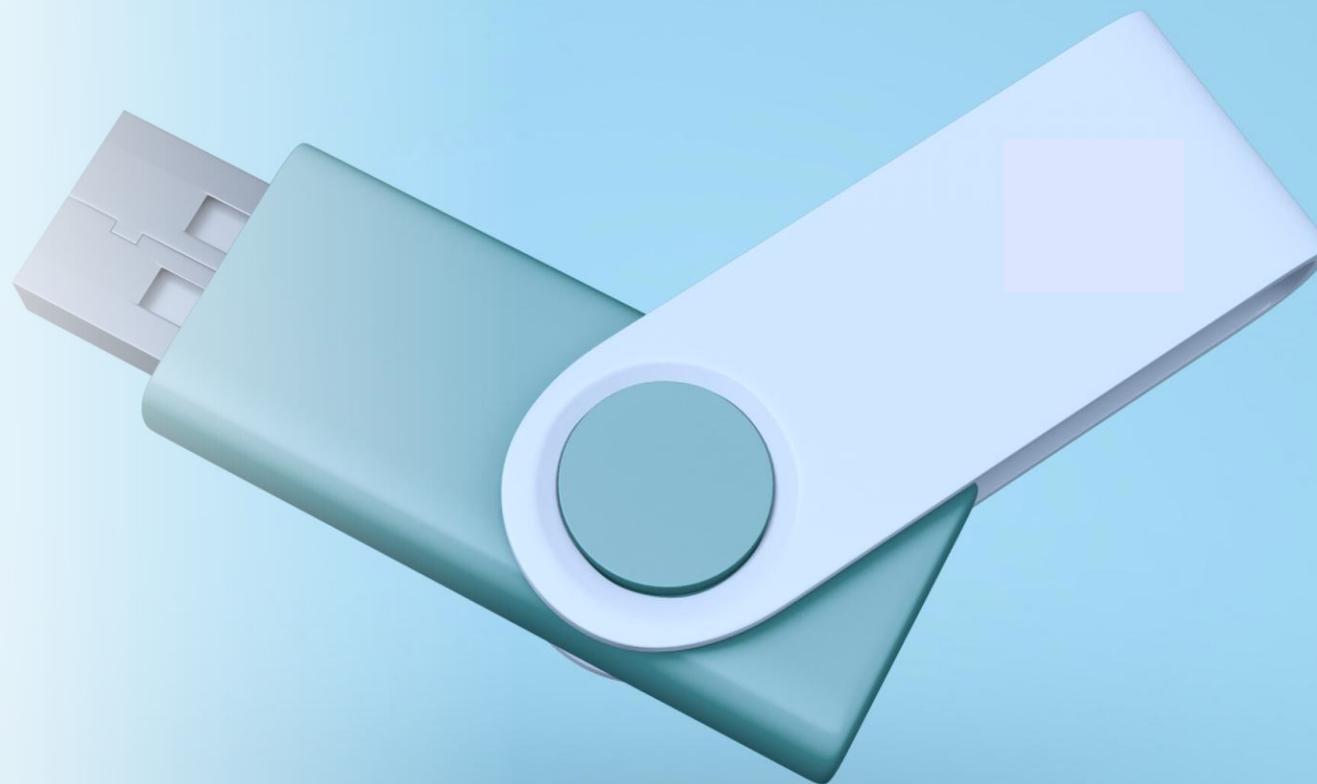
PIGGYBACKING



BAITING

Baiting

- nastraženie infikovaných dátových médií (USB kľúč, DVD)
- verejné miesta, kde pascu niekto určite nájde (výťah, toaleta, kuchynka)
- atraktívne označenie (napr. “návrh miezd na rok 2024”)
- poskytnutie nového digitálneho obsahu (napr. filmov, hudby)





MINISTERSTVO

INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Podvodné správy (scam)

- podvod páchaný na používateľoch za účelom finančného zisku, alebo zneužitia identity
- napr. list z Nigérie alebo inej západoafrickej krajiny
- vyžaduje sa od cieľovej osoby poplatok, pokuta a pod.
- Psychologicky prepracovaný postup, zneužívanie kognitívnych skreslení (sunk-cost fallacy/skreslenie utopených nákladov)

Týždne som si písala s romantickým podvodníkom. Ráno ma miloval, večer mi vulgárne vynadal



Romantický podvodník mi počiатku posielal množstvo zamilovaných správ. Keď zistil, že o ňom pripravujem článok, vynadal mi.

Zdroj: Aktuality.sk / iStockphoto

<https://www.aktuality.sk/clanok/zp12gsc/tyzdne-som-si-pisala-s-romantickym-podvodnikom-rano-ma-miloval-vecer-mi-vulgarne-vynadal/>

Phishing



Vážený zákazník,
Váš balík je na ceste:
STAV: Čaká sa na distribučné centrum.
Spracovanie prebieha na termináli
Platba: 59.95 SKK

Na potvrdenie

Dôležité: v prípade neodpovedania vám
serta pošle váš balík späť, situáciu prosím
vyriešte do 24.09.2020



Vážený príjemca balíka

Dovoľujeme si Vás informovať, že sme obdržali informácie
balíka a zajtra bude doručený do skladu Slovenskej pošty
vnútroštátnu prepravu.

* Číslo zásielky: SK#490171401

Váš balík bude uložený v našom sklade, kým nebudete m

* **Potvrdenie o doručení**

Upozorňujeme, že získate iba 3 dni bezplatného úložiska
účtovaný príplatok 2,84 EUR za každý deň uloženia.

© 2022 Slovenská-Pošta

PayPal

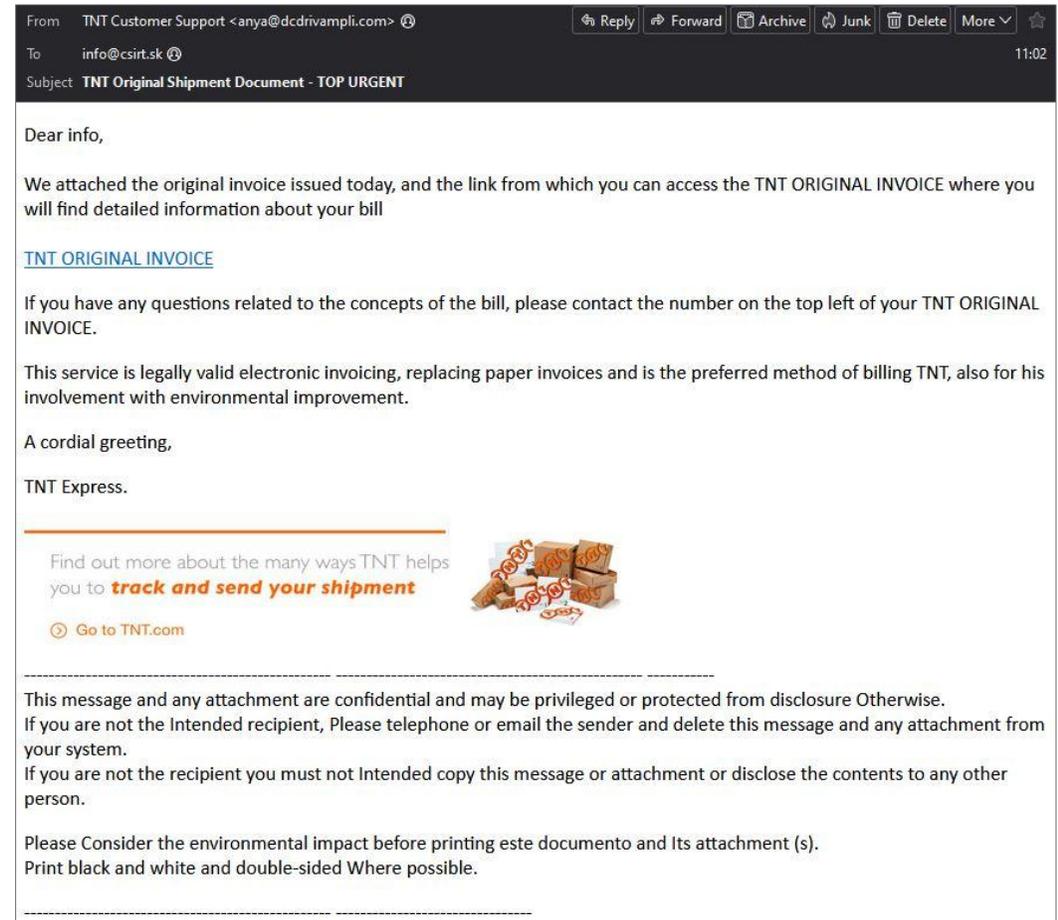
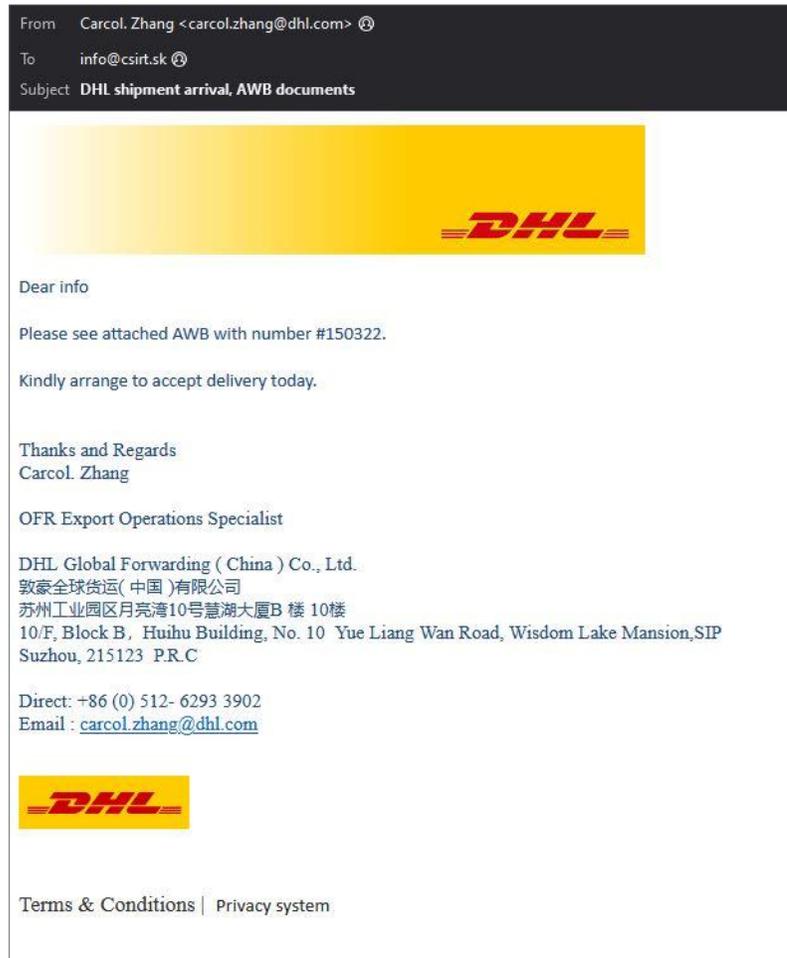
We are constantly working to make safer PayPal, easier and more convenient for our customers.
This means that from time to time we have to make changes to the terms of our User Agreement.
To ensure that you are always aware we posted the latest updates on our website . compte.

What I need to do ?

[Update your information](#)

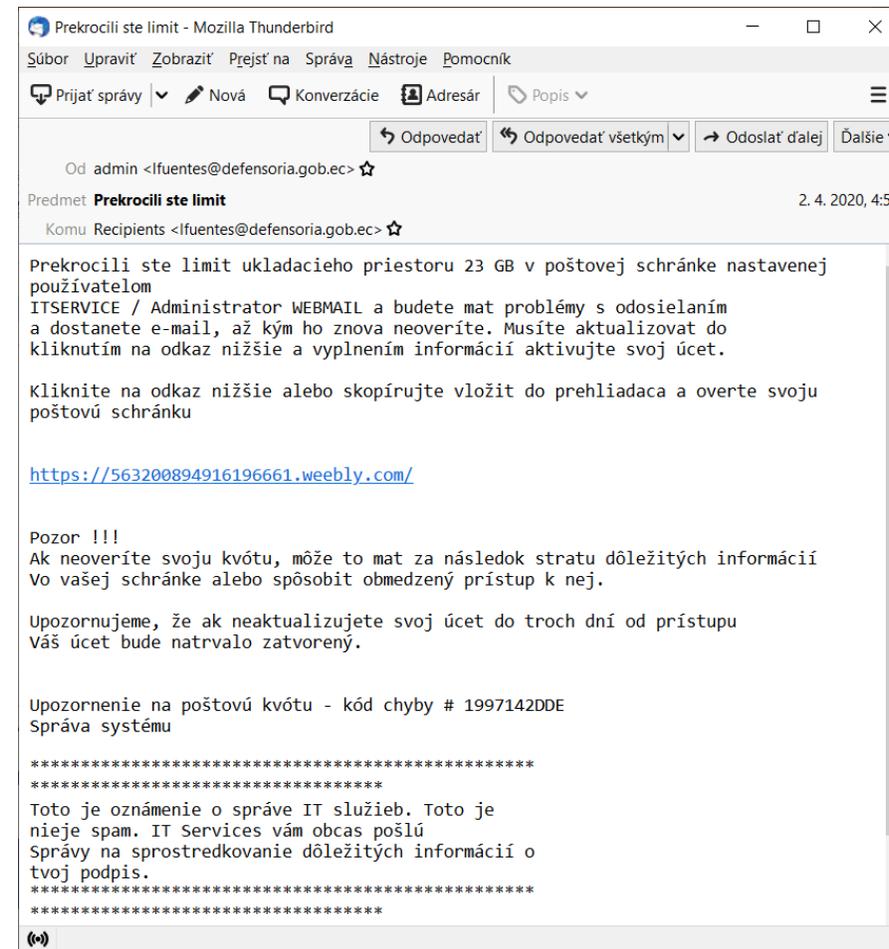
Sincerely,
PayPal Support

Phishing

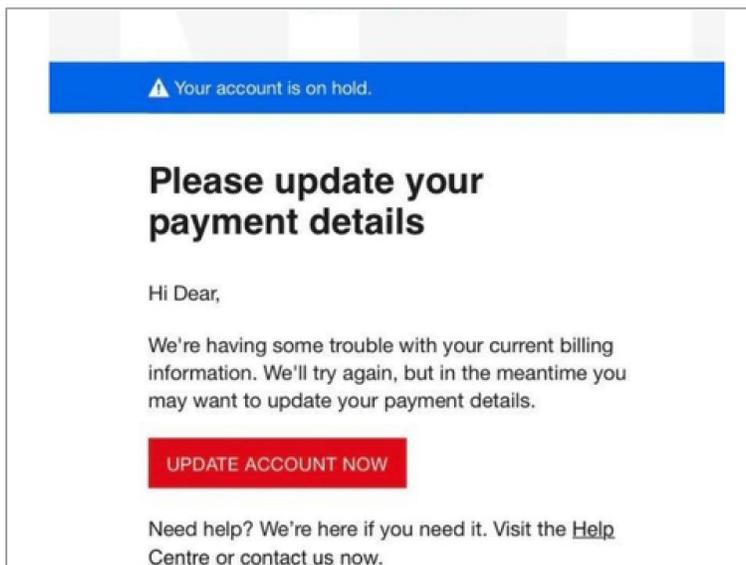


Phishing

- 90% útokov začína phishingom
- patrí k najčastejším spôsobom získavania osobných údajov
- legitímne vyzerajúci email využíva rôzne zámienky, ako napríklad:
 - doručenie výhry, alebo možnosť získania finančných prostriedkov,
 - informácia o ukončení platnosti účtu, alebo nutnosti rozšírenia úložného priestoru,
 - žiadosť banky o overenie totožnosti a iných údajov (napr. čísla kreditnej karty či prístupových kódov k internet bankingu),
 - doručenie oskenovaného dokumentu,



Phishing



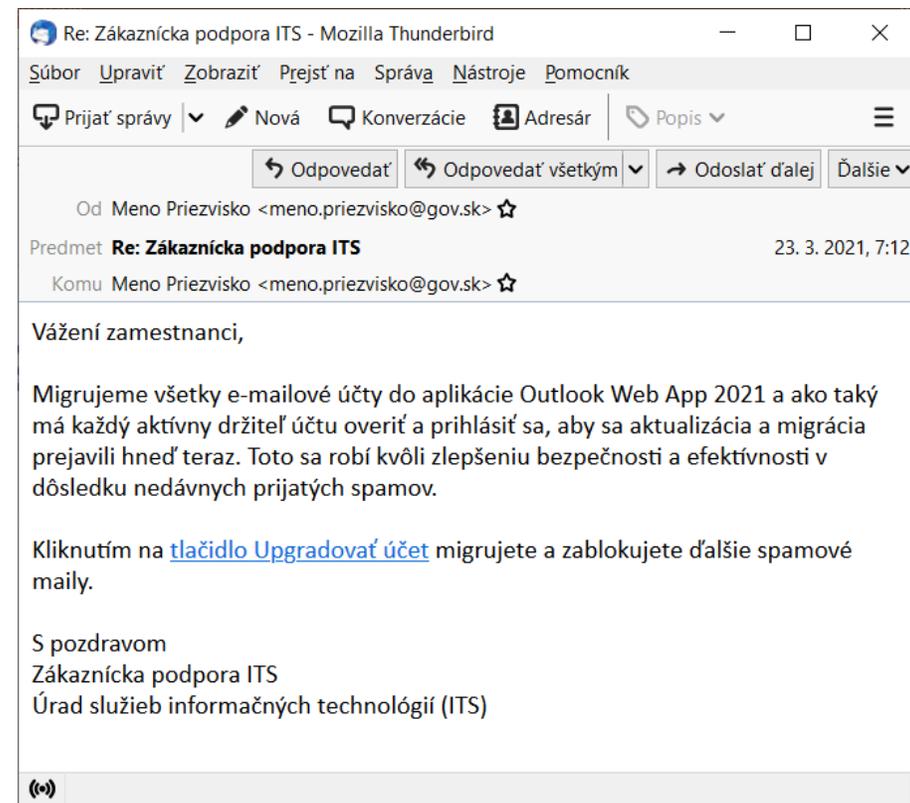
Od: [redacted]@fno.cz>

Odoslané: štvrtok, 19. októbra 2023 10:13

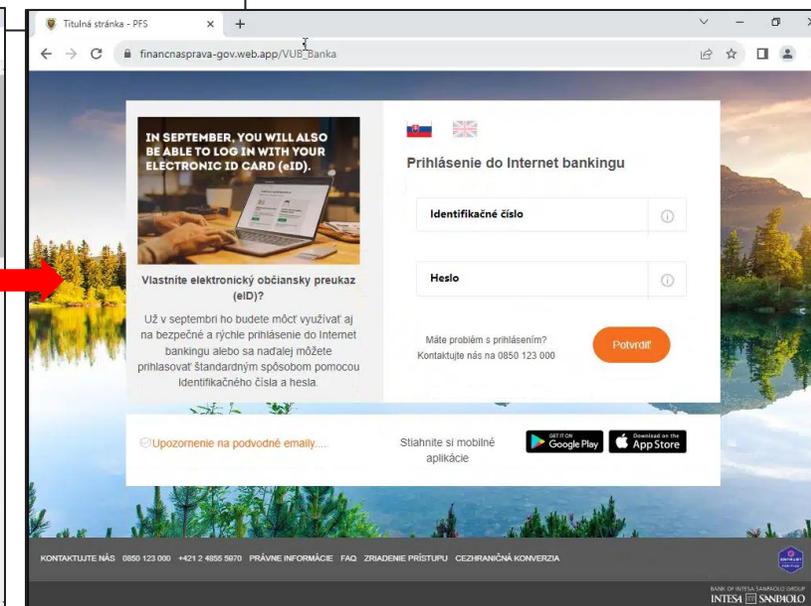
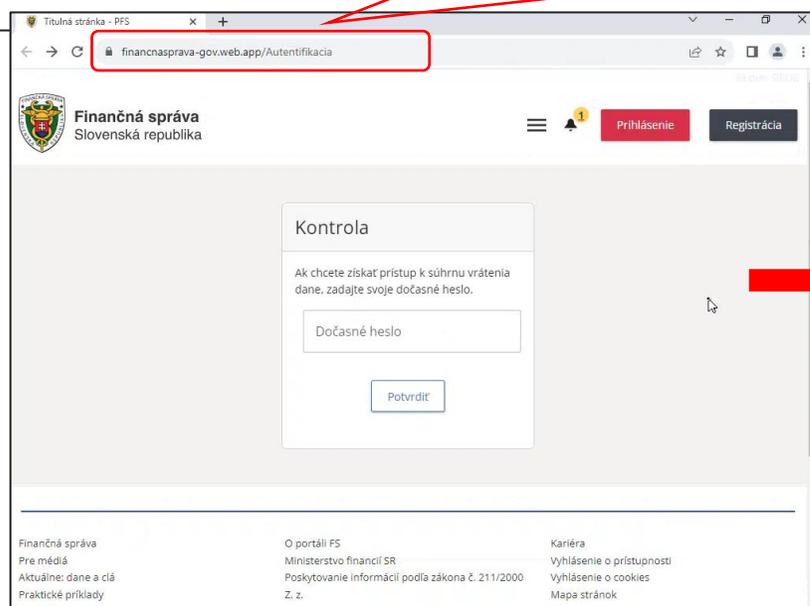
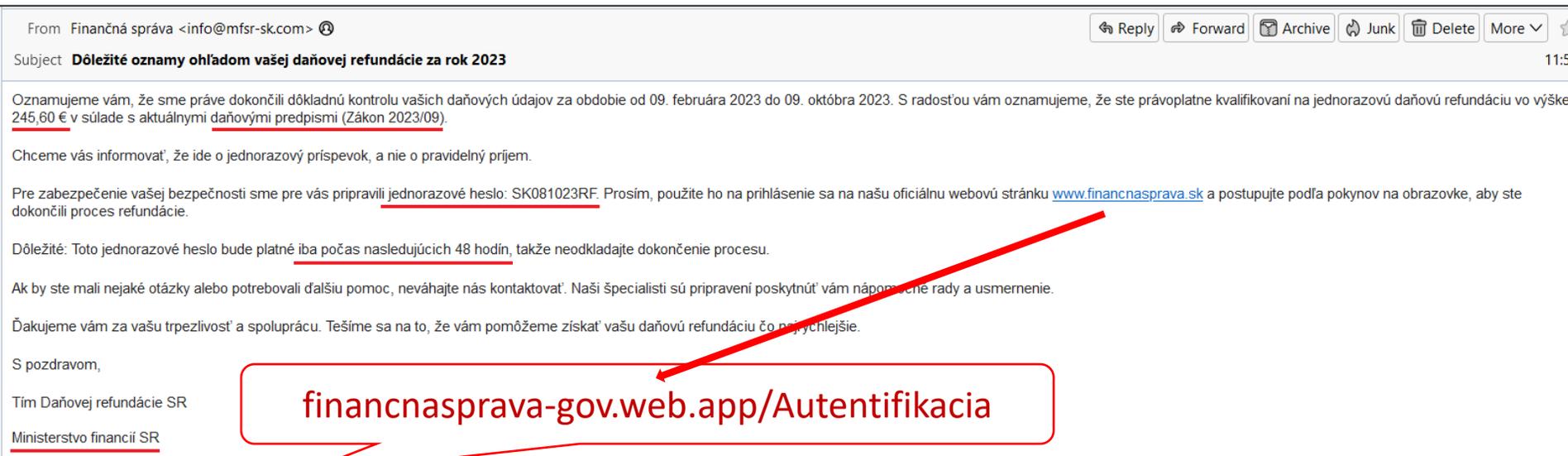
Predmet: IT-SERVICE

UPOZORNENIE: Tento e-mail pochádza od odosielateľa mimo organizácie a obsahuje podozrivé kľúčové slová. Zvýšte prosím pozornosť na obsah, odosielateľa, odkazy a prílohy. V prípade podozrenia na škodlivý obsah zašlite podozrivý e-mail na spam@nsud.sk.

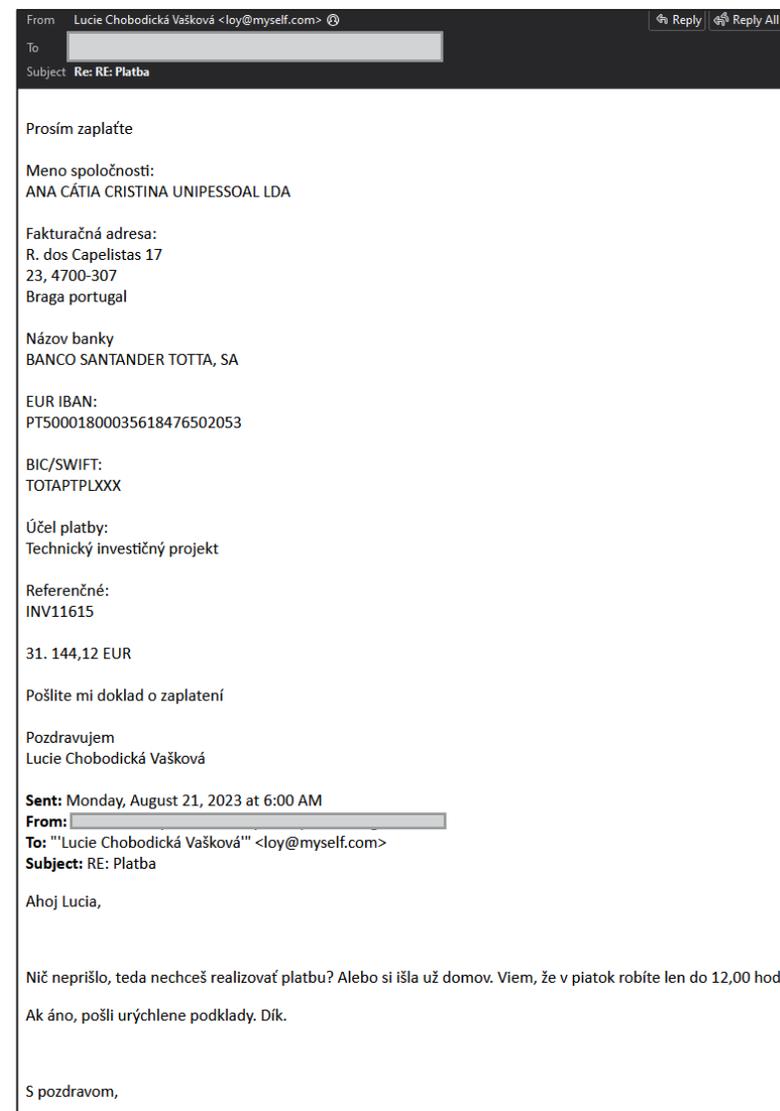
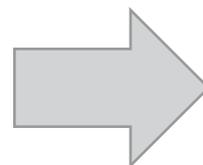
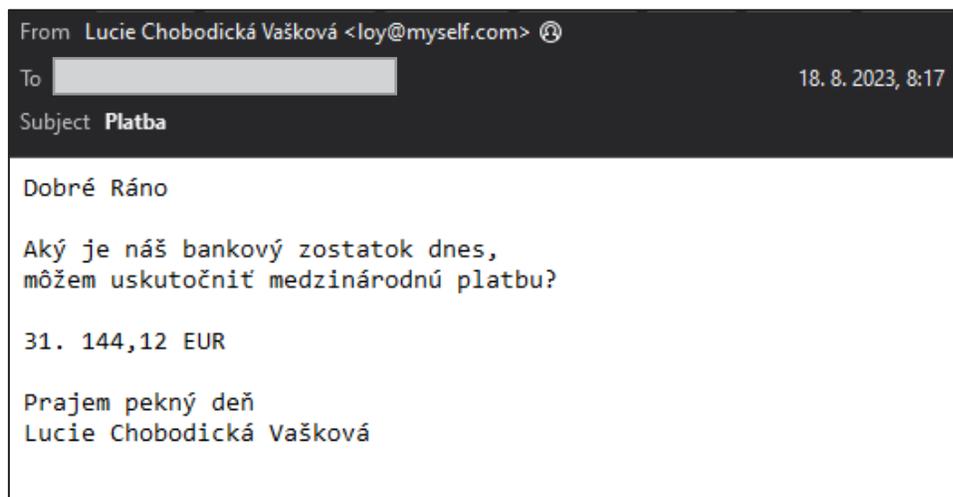
Heslo poštovej schránky vyprší po jednom dni. pre uloženie hesla. [KLIKNITE SEM](#) pre aktualizáciu a okamžité odoslanie.



Phishing



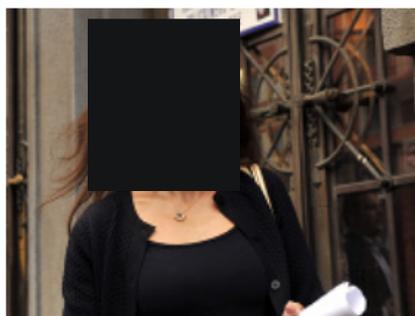
Spear-phishing



Spear-phishing

Podvodník obral neuveriteľným trikom štát o peniaze: Úradník mu poslal pol milióna za toalet'áky

Pošlite nám tip



██████████ podala trestné oznámenie.

24.08.2015 11:05

BRATISLAVA - Metodicko-pedagogické centrum (MPC) v Bratislave, ktoré je priamo riadenou organizáciou ministerstva školstva, dostalo koncom júna od jedného zo svojich dodávateľ informáciu o zmene bankového účtu. Organizácia na nový účet poslala vyše 459.555 eur. Neskôr sa však podľa riaditeľky MPC ██████████

ukázalo, že email od dodávateľa bol fiktívny. MPC preto podalo trestné oznámenie na neznámeho páchatel'a a vyvodilo dôsledky.



Slovákovi volá falošná technická podpora Microsoftu. Podvodníci chcú prístup do počítača



NOVINKY

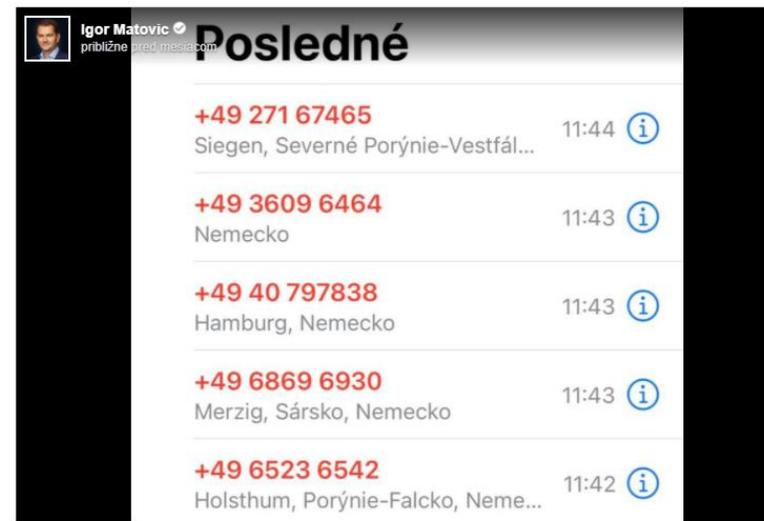
Falošná technická podpora Microsoftu už zneužíva aj predvoľbu +421



Vishing

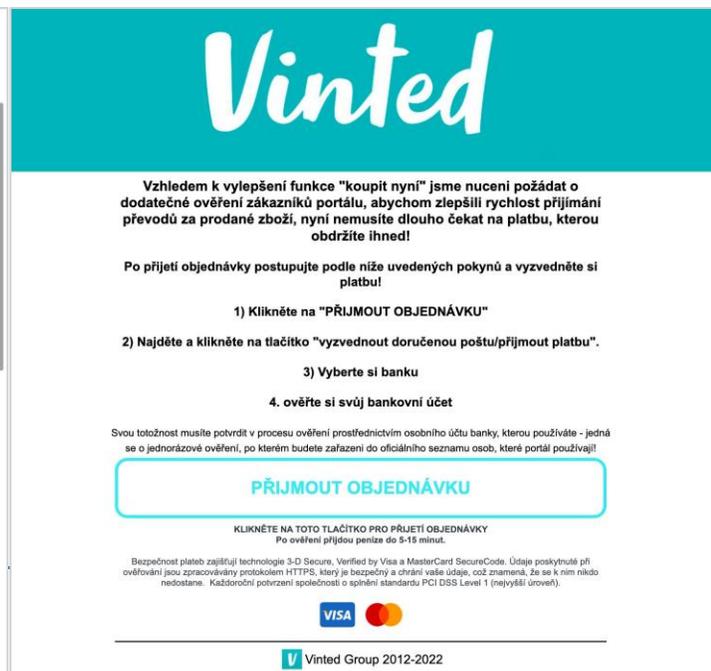
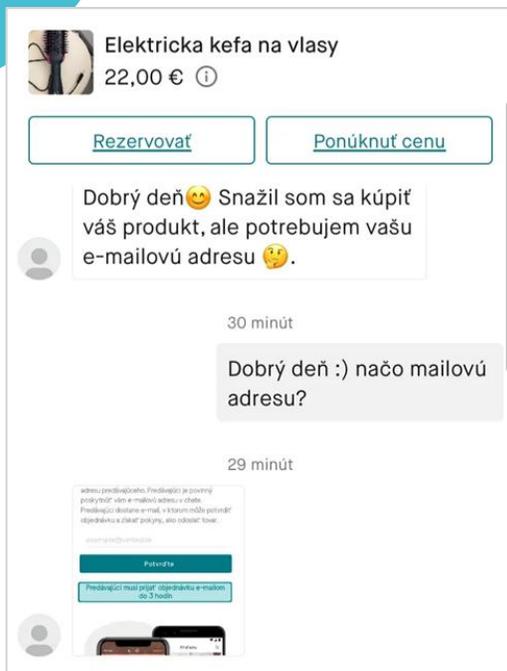
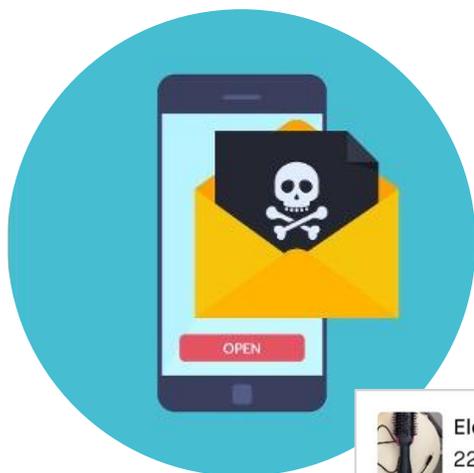
17.12.2020 18:50 | Správy

Falošná podpora Microsoftu chcela muža pripraviť o 17 000 eur, upozornila polícia



Zdroj: <https://support.microsoft.com/sk-sk/windows/ochrana-pred-falo%C5%A1nou-technickou-podporou-2ebf91bd-f94c-2a8a-e541-f5c800d18435>

SMiShing



Od: Slovenská pošta <support@asc925.com>
Predmet: Vaše balenie N: 2938456 čaká na vás !
Dátum: 06.február 2021 06:48:05 CET
Pre: [REDACTED]

Otvoriť | Odpovedať | Odpovedať všetkým | Preposlať
| Vymazať | Uložiť do šablón

E-mail sa zobrazuje bez obrázkov. [Zobraziť celý email.](#)



Vážený ##email##,

Váš balík N: 2938456 čaká na spracovanie z dôvodu nezaplatených nákladov na dopravu (2,99 EUR), balík sme nechali čakať na vašu platbu

Sledovacie číslo: [9405511699000070018991](#)

Poznámka: Ak nedostaneme vašu platbu, vaša objednávka bude vrátená odosielateľovi do 48 hodín.

Pošlite môj balík

Navštívte stránku [SkTracking®](#)? a skontrolujte najaktuálnejší stav vášho balíka. Zaregistrujte sa do služby Informed Delivery®, aby ste si mohli digitálne zobrazit ukážku adresy prichádzajúcej pošty vo veľkosti listu a spravovať svoje balíky s plánovaným príchodom coskoro! Ak chcete aktualizovať, ako často budete dostávať e-maily z USPS, prihláste sa do svojho účtu SKpost.com.

ZNAKY PHISHINGU

Urgencia a hrozba

Zdroj: <https://www.posta.sk/informacie/pozor-na-podvody>

Musíte dokončiť platbu vo výške (2,99 EUR). - Mozilla Thunderbird

Ľubor Upraviť Zobrazit' Prejsť na Správa Nástroje Pomocník

Prijat' správy Nová Konverzácie Adresár Popis

Odpovedať Odpovedať všetkým Odoslať ďalej Ďalšie

Od Slovenská Pošta <support@sbosportclub.com>

Predmet **Musíte dokončiť platbu vo výške (2,99 EUR).** 27. 1. 2021, 16:45

Komu meno.priezvisko@gov.sk



Vážený zákazník,

ďakujeme, že používate Slovenská pošta, váš balík na vás čaká.

Musíte dokončiť platbu vo výške (2,99 EUR).

Čo by som mal robiť?

Kliknutím na nižšie uvedený bezpečný odkaz dokončíte platbu svojich prepravných poplatkov

S pozdravom.

Starostlivosť o zákazníkov Slovenská pošta.

[zaplat' teraz](#)

Gramatika a štylistika

- Emailová správa obsahuje **gramatické alebo štylistické chyby**, resp. preklepy
- Vážený pani
- Aktuálne – **dobrá slovenčina v phishingu**
- Podvodné správy sú stále viac "medzinárodné" ale **zlepšuje sa v národných jazykoch**

| Pozor na podvodné emaily: Útočníci zlepšili slovenčinu, klamú, že vás nahrali pri sledovaní porna

8

AUTOR: ROMAN KADLEC PUBLIKOVANÉ: 14. JANUÁRA 2020

NOVINKY

Na novú vlnu podvodov upozornil ESET.

Podvodníci zameriavajúci sa na digitálne vydieranie svojich obetí **opäť vylepšili svoju taktiku**. Bezpečnostná spoločnosť ESET **varuje používateľov pred nepravdivými podvodnými emailovými správami**, ktoré sa pokúšajú vylákať výpalné od ľudí sledujúcich pornografický obsah na svojich digitálnych zariadeniach.



BY SYNCED
2019-10-31

COMMENT 1



MINISTERSTVO

INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Príliš dobrý text

Text je príliš dobrý na to, aby sme mu verili

- výhra v lotérii, do ktorej sme sa nezapojili
- kupón na 90% zľavu v eshope

Odpovedať Odpovedať všetkým Preposlať



po 03.09.2018 19:39

DRA.SANTA MARIA JOSE BOSCH. <aganex_consult@libero.it>

OZNÁMENIE O CENENÍ: ZÍSKALA Coca-Cola PLC PROMOTION (2018), BERÚCENIE!

Komu

OZNÁMENIE O CENENÍ: ZÍSKALA Coca-Cola PLC PROMOTION (2018), BERÚCENIE!

Používateľ / príjemca účtu !,

Chceli by sme Vás informovať, že váš účet používateľov online vyhral (750 000,00 €) v našej výročnej propagačnej kampani sponzorovaný spoločnosťou Coca-Cola Plc Global v spolupráci s Microsoft.Používajúci aktívne používateľa E-mailový účet od spoločnosti poskytovateľov služieb.

Ako firemnú politiku vyberáme každoročne (9) kandidátov ako našich víťazov prostredníctvom E-mailového hlasovania (EBS)

E-mail Ballot (EBS) žiadosť od kandidátov.Zameraná na našu spoločenskú zodpovednosť, aktivácia predaja ako

ako aj na zníženie chudoby na svete. Môžete sa obrátiť na svojho akreditovaného dôveryhodného bankového poradcu

osobné údaje pre náležitú remitentance výhier losovania

Sr. Alexander Cruz Hernando Santo.

Globanet Finance & Claims Services.

E-mail: info_globanetapex@consultant.com

Kancelária Telefón: (+ 34) 604-261-425.





MINISTERSTVO

INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

<https://download.moja-stranka.com/obsah?v=3zdg>



Vážený používateľ účtu,

Platnosť Vášho hesla vyprší za dva dni, aby ste udržali svoj účet, prosím,
[KLIKNITE SEM](#) a postupujte podľa inštrukcií, aby ste si udržali Váš e-mailový
účet **ALEBO KLIKNITE TENTO LINK:**

<http://updates.ponggok.com/>

Neaktualizácia vášho e-mailového účtu spôsobí jeho deaktiváciu, buďte
upozornení!

IT-Help Desk,
PA 19104

IT Help Desk © 2018 VŠETKY PRÁVA REZERVOVANÉ

Odkazy

- Odkazy v phishingovej emailovej správe smerujú na falošnú stránku.
- Legitímny názov –
 - banka.sk, banka.sl, banka.com, banka.uk, banka.super.sk, banla.sk, barka.sk
 - support.sk a suqqort.sk
 - kia.sk a kla.sk
 - super.sk/banka.sk
- Cambridge University - Typoglycemia





MINISTERSTVO

INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Odkaz v obrázkoch

Phishingové emailové
správy s **obrázkom**,
ktorý obsahuje odkaz.

PayPal

We are constantly working to make safer PayPal, easier and more convenient for our customers.

This means that from time to time we have to make changes to the terms of our User Agreement.

To ensure that you are always aware we posted the latest updates on our website, complete.

What I need to do ?

[Update your information](#)

Sincerely,

PayPal Support

"Kia Motors Slovakia" <info@kmss.sk> Mon, Dec 29, 2014 at 9:02 AM

Reply-To: info@kmss.sk

To: "\"Chuck Norris\"" <chucknorris@gmail.sk>

Želáme Vám vyladený motor
po celý rok



The Power to Surprise

www.kia.com/sk/campaigns-and-redirects/pf-2015/presentation/

Podozrivá príloha

From Maersk Shipping <sales02@inbox.org> 
To info@csirt.sk 
Subject Invoice copy 22. 12. 2023, 15:57

Following are the list of Invoices we made payment for.

5480394988

5480394682

Please do not reply directly to this automated message. This e-mail was sent from a notification-only address that cannot accept incoming e-mail.

Legal

The information contained in this message is privileged and intended only for the recipients named. If the reader is not a representative of the intended recipient, any review, dissemination or copying of this message or the information it contains is prohibited. If you have received this message in error, please immediately notify the sender, and delete the original message and attachments.

Maersk will as part of our communication and interaction with you collect and process your personal data. You can read more about Maersk's collection and processing of your personal data and your rights as a data subject in our [privacy policy](#).

Please consider the environment before printing this email.

>  1 attachment: invoice #65328975.pdf.html 67,5 KB  Save

UNCHECKED ŽIADOSŤ O CENOVÚ PONUKU (Univerzita Komenského v Bratislave) EUI894/SK4633 - Mo...
Súbor Upraviť Zobrazit' Prejsť na Správa Nástroje Pomocník
Prijat' správy Nová Konverzácie Adresár Popis
Odpovedať Odpovedať všetkým Odoslať ďalej Ďalšie
Od Univerzita Komenského v Bratislave <admin@uniba.sk>
Predmet ***UNCHECKED*** ŽIADOSŤ O CENOVÚ PONUKU (Univerzita Komenského v Bratislave) EUI894/SK4633 7. 12. 2020, 12:43
Komu undisclosed-recipients;

 UNIVERZITA KOMENSKÉHO
V BRATISLAVE
100

Zdravím vás z univerzity v Barcelone
(Dúfam, že ste vy a vaša rodina v bezpečí tejto doby)
Do ruk:
Na základe dobrých odporúčaní vašej spoločnosti sme Univerzita Komenského v Bratislave pod vedením Dr. Mgr. Róbert Zembera.
Potrebujeme vašu ponuku pre náš rozpočet na rok 2020 (priložené).
Odošlite svoju ponuku 10. decembra 2020 alebo skôr.
Ďakujeme a ostávame s pozdravom.

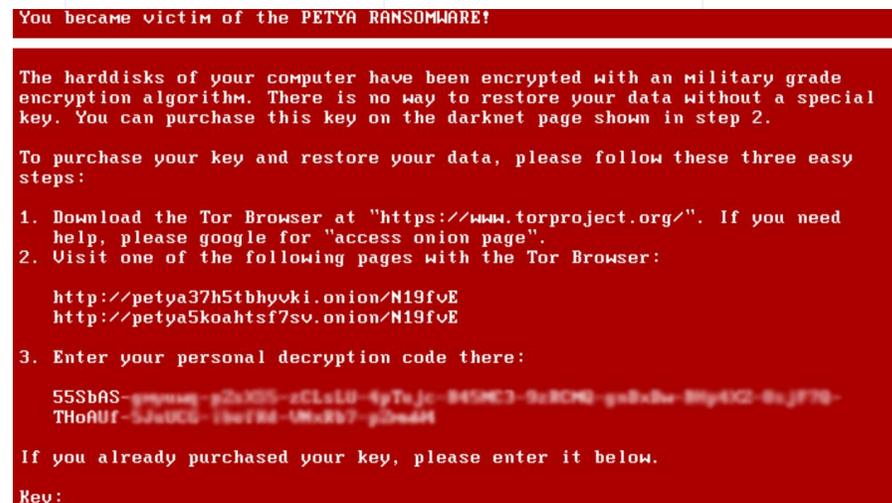
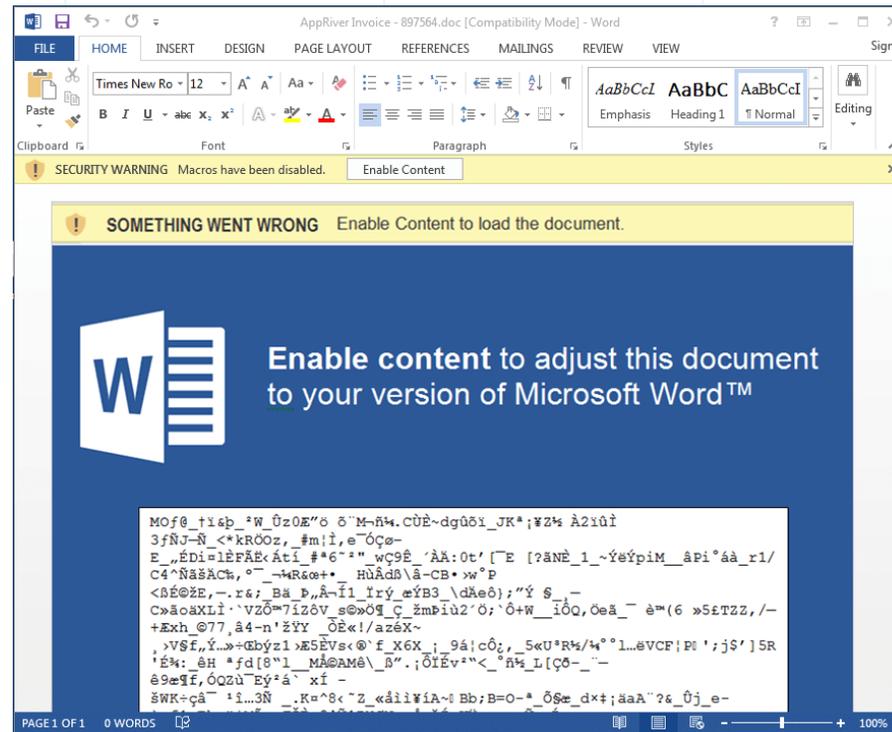
>  1 príloha: ŽIADOSŤ O CENOVÚ PONUKU 07-12-2020-pdf.zip 152 kB  Uložiť



Škodlivý kód

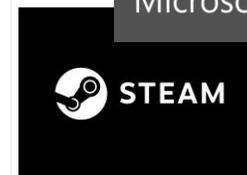
Malware = Malicious Software

- **Adware** – zobrazovanie reklám
- **Trójsky kôň / zadné vrátka** – prístup do počítača
- **Spyware** – špionáž, únik údajov
- **Keylogger** – krádež stlačení kláves / heslá
- **Cryptominer** – ťaženie kryptomien
- **Botnet**
- **Downloader** – stiahnutie ďalšieho škodlivého kódu
- **Ransomware** – šifrovanie a výkupné
- **Deštrukčný malvér** – zničenie dát alebo hardvéru



Ochrana voči škodlivému kódu

- Obozretnosť používateľa
- Inštalovať len softvér z overených zdrojov
- Antivírusový program a firewall
- Automatické aktualizácie
- Odinštalovanie nepoužívaných aplikácií
- Nastavenia operačného systému (nepotrebné služby, autoplay, ...)
- Používateľský účet s obmedzenými oprávneniami



Zhodný odosielateľ a príjemca

Od: janko.hrasko@gov.sk <janko.hrasko@gov.sk>

Komu: janko.hrasko@gov.sk <janko.hrasko@gov.sk>

Predmet: Security Notice. janko.hrasko@gov.sk was hacked! Change your password now!

Dear user of gov.sk

I am a spyware software developer.
Your account has been hacked by me in the summer of 2018.

I understand that it is hard to believe, but here is my evidence - I sent you this email from your account.

The hacking was carried out using a hardware vulnerability through which you went online (Cisco router, vulnerability CVE-2018-0296).





MINISTERSTVO

INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Odosielať pozná heslo

Hackeri napadli sociálnu sieť LinkedIn.
Ukradli 6,5 milióna hesiel

06.06.2012 / Noviny.sk / Veda a technika

LUCIA HUSÁROVÁ



Od: Jhrasko <....@hoo11.xyz>

Odoslané: sobota, 8. septembra 2018 3:36

Komu: meno.priezvisko@gov.sk

Predmet: Your password is MojeTajneHeslo2021

I am aware **MojeTajneHeslo2021** is your passphrase. Lets get right to purpose. You may not know me and you are most likely thinking why you are getting this e mail? None has compensated me to investigate about you.

...

You get just two solutions. Why dont we look at these types of options in particulars:

1st solution is to skip this e mail. In this situation, I most certainly will send your very own recorded material to almost all of your contacts and then just think regarding the humiliation you feel. Furthermore if you happen to be in a romantic relationship, exactly how it would affect?

Number 2 alternative would be to give me \$4000. Let us describe it as a donation. Subsequently, I will asap eliminate your video. You could go on with your daily routine like this never happened and you will not hear back again from me.



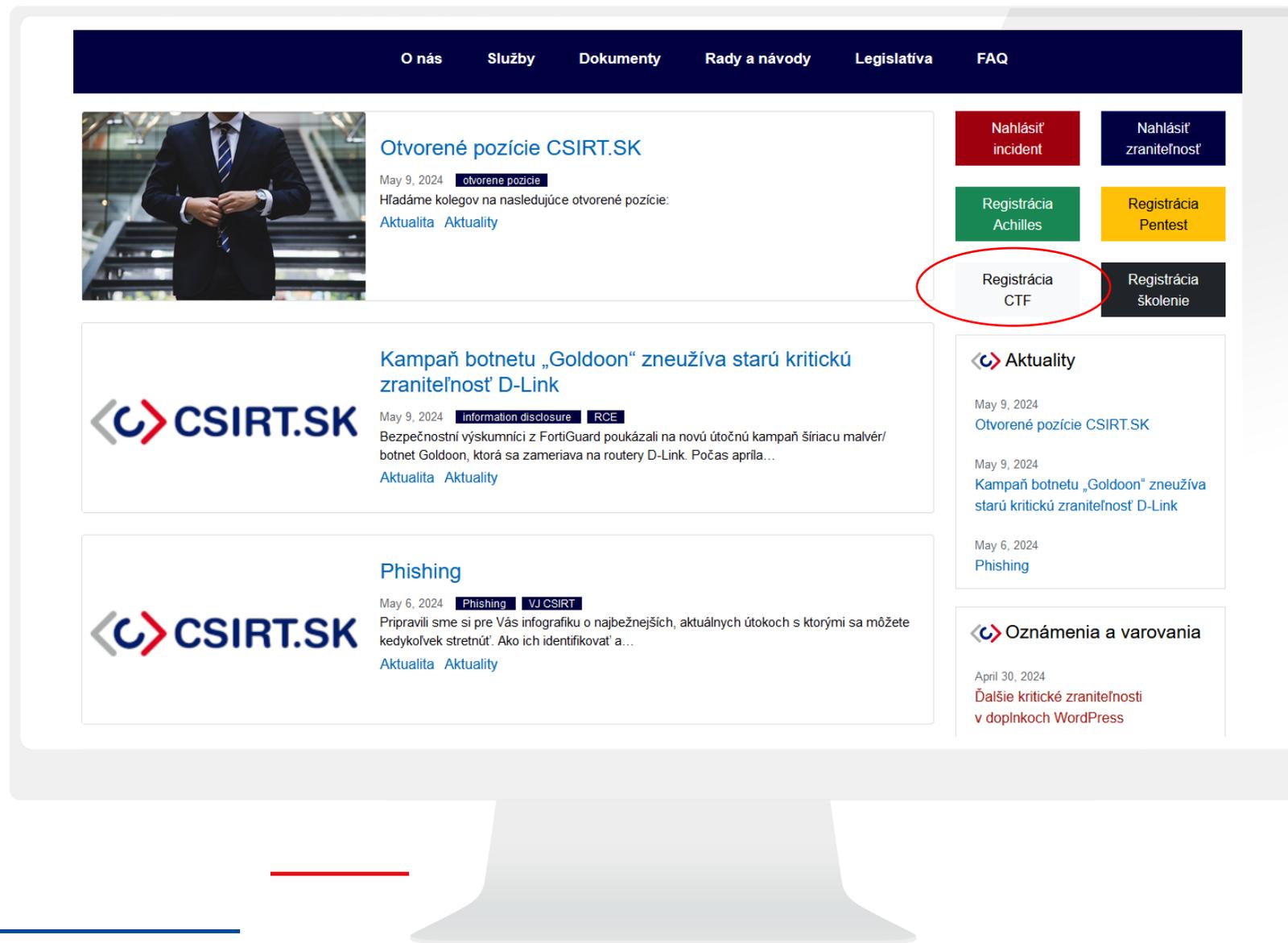
MINISTERSTVO

INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Interaktívny phishingový test

<https://www.csirt.gov.sk>

<https://ctf.kyberakademia.sk/>





MINISTERSTVO

INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Ako na phishing? (I.)

Ukážka zaslaného emailu:



Zmeny v ohodnotení zamestnancov statnej a verejnej spravy
personalne užívateľovi: [REDACTED]

Od: personalne@uradplace.sk

Užívateľovi: [REDACTED]@csirt.gov.sk

Odpovedzte, prosím, užívateľovi personalne@uradplace.sk

11.11.2020 08:42

Vážení kolegovia,

pripravuje sa zmena finančného ohodnotenia zamestnancov v štátnej službe a zamestnancov vo verejnom záujme.

Návrh ohodnotenia zamestnancov je uvedený na portáli <http://uradprace.sk/platy.php?id=plat&=platSdf23Xs23>

Na tomto portáli bude informácia predbežne umiestnená do 1.12.2020.

Informácia bude pre širokú verejnosť zverejnená v dátume účinnosti novely zákonov č.552/2003 Z.z o výkone práce vo verejnom záujme v znení neskorších predpisov resp. Zákon č. 400/2009 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Pre prihlásenie použite Váš doménový účet (meno/heslo do Vášho počítača).

S pozdravom

Vedúci oddelenia ekonomického zabezpečenia



Ako na phishing? (II.)

- Phishingové emaily ponúkajú niečo lákavé
- Vždy, keď Vám niekto ponúka alebo oznamuje niečo príliš dobré, spozornite!
- Phishing reaguje na aktuálne trendy a snaží sa tým vzbudiť dôveryhodnosť



Zmeny v ohodnotení zamestnancov štátnej a verejnej spravy

personalne@uradplace.sk

Od: personalne@uradplace.sk

Užívateľovi: @csirt.gov.sk

Odpovedzte, prosím, užívateľovi personalne@uradplace.sk

11.11.2020 08:42

Vážení kolegovia,

pripravuje sa zmena finančného ohodnotenia zamestnancov v štátnej službe a zamestnancov vo verejnom záujme.

Návrh ohodnotenia zamestnancov je uvedený na portáli <http://uradprace.sk/platy.php?id=plat&=platSdf23Xs23>

Na tomto portáli bude informácia predbežne umiestnená do 1.12.2020.

Informácia bude pre širokú verejnosť zverejnená v dátume účinnosti novely zákonov č.552/2003 Z.z o výkone práce vo verejnom záujme v znení neskorších predpisov resp. Zákon č. 400/2009 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Pre prihlásenie použite Váš doménový účet (meno/heslo do Vášho počítača).

S pozdravom

Vedúci oddelenia ekonomického zabezpečenia



MINISTERSTVO

INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Ako na phishing? (III.)

- Obozretný používateľ emailu si všíma nielen meno, ale aj doménu v emailovej adrese
- uradplace.sk nie je doména Úradu práce



Zmeny v ohodnotení zamestnancov statnej a verejnej spravy
personalne užívateľovi: [redacted]

Od: **personalne@uradplace.sk**

Užívateľovi: [redacted]@csirt.gov.sk

Odpovedzte, prosím, užívateľovi personalne@uradplace.sk

11.11.2020 08:42

Vážení kolegovia,

pripravuje sa zmena finančného ohodnotenia zamestnancov v štátnej službe a zamestnancov vo verejnom záujme.

Návrh ohodnotenia zamestnancov je uvedený na portáli <http://uradprace.sk/platy.php?id=plat&=platSdf23Xs23>

Na tomto portáli bude informácia predbežne umiestnená do 1.12.2020.

Informácia bude pre širokú verejnosť zverejnená v dátume účinnosti novely zákonov č.552/2003 Z.z o výkone práce vo verejnom záujme v znení neskorších predpisov resp. Zákon č. 400/2009 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Pre prihlásenie použite Váš doménový účet (meno/heslo do Vášho počítača).

S pozdravom

Vedúci oddelenia ekonomického zabezpečenia



MINISTERSTVO

INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Ako na phishing? (IV.)

- Informácia mala byť zverejnená len pár týždňov



Zmeny v ohodnotení zamestnancov statnej a verejnej spravy
personalne užívateľovi: [REDACTED]

Od: personalne@uradplace.sk

Užívateľovi: [REDACTED]@csirt.gov.sk

Odpovedzte, prosím, užívateľovi personalne@uradplace.sk

11.11.2020 08:42

Vážení kolegovia,

pripravuje sa zmena finančného ohodnotenia zamestnancov v štátnej službe a zamestnancov vo verejnom záujme.

Návrh ohodnotenia zamestnancov je uvedený na portáli <http://uradprace.sk/platy.php?id=plat&=platSdf23Xs23>

Na tomto portáli bude informácia predbežne umiestnená do 1.12.2020.

Informácia bude pre širokú verejnosť zverejnená v dátume účinnosti novely zákonov č.552/2003 Z.z o výkone práce vo verejnom záujme v znení neskorších predpisov resp. Zákon č. 400/2009 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Pre prihlásenie použite Váš doménový účet (meno/heslo do Vášho počítača).

S pozdravom

Vedúci oddelenia ekonomického zabezpečenia



MINISTERSTVO

INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Ako na phishing? (V.)

- Phishing sa môže odvolávať na authority ako je vláda SR
- Tiež sa môže odvolávať na zákony a nariadenia aby vzbudil dôveryhodnosť



Zmeny v ohodnotení zamestnancov statnej a verejnej spravy
personalne užívateľovi: [REDACTED]

Od: personalne@uradplace.sk

Užívateľovi: [REDACTED]@csirt.gov.sk

Odpovedzte, prosím, užívateľovi personalne@uradplace.sk

11.11.2020 08:42

Vážení kolegovia,

pripravuje sa zmena finančného ohodnotenia zamestnancov v štátnej službe a zamestnancov vo verejnom záujme.

Návrh ohodnotenia zamestnancov je uvedený na portáli <http://uradprace.sk/platy.php?id=plat&=platSdf23Xs23>

Na tomto portáli bude informácia predbežne umiestnená do 1.12.2020

Informácia bude pre širokú verejnosť zverejnená v dátume účinnosti **novely zákonov č.552/2003 Z.z** o výkone práce vo verejnom záujme v znení neskorších predpisov resp. **Zákon č. 400/2009 Z. z.** o štátnej službe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Pre prihlásenie použite Váš doménový účet (meno/heslo do Vášho počítača).

S pozdravom

Vedúci oddelenia ekonomického zabezpečenia



Ako na phishing? (VI.)

- URL odkaz, ktorý napriek tomu, že zobrazuje odkaz na stránku uradprace.sk v skutočnosti smeruje na podvrhnutú stránku uradplace.sk
- Obozretný používateľ pred kliknutím na odkaz skontroluje, kam v skutočnosti smeruje priložením kurzoru na tento odkaz
- V spodnej lište emailového klienta sa zobrazí skutočná adresa odkazu



Zmeny v ohodnotení zamestnancov statnej a verejnej spravy
personalne užívateľovi: [redacted]

Od: personalne@uradplace.sk

Užívateľovi: [redacted]@csirt.gov.sk

Odpovedzte, prosím, užívateľovi personalne@uradplace.sk

11.11.2020 08:42

Vážení kolegovia,

pripravuje sa zmena finančného ohodnotenia zamestnancov v štátnej službe a zamestnancov vo verejnom záujme.

Návrh ohodnotenia zamestnancov je uvedený na portáli <http://uradprace.sk/platy.php?id=plat&=platSdf23Xs23>

Na tomto portáli bude informácia predbežne umiestnená do 1.12.2020.

Informácia bude pre širokú verejnosť zverejnená v dátume účinnosti novely zákonov č. 52/2003 Z.z o výkone práce vo verejnom záujme v znení neskorších predpisov resp. Zákon č. 400/2009 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Pre prihlásenie použite Váš doménový účet (meno/heslo do vášho počítača).

S pozdravom

Vedúci oddelenia ekonomického zabezpečenia

<http://www.uradplace.sk/>



MINISTERSTVO

INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Ako na phishing? (VII.)

- Phishingové emaily od Vás budú žiadať zadanie prihlasovacích údajov, resp. ich overenie alebo Vás budú varovať pred ich vypršaním



Zmeny v ohodnotení zamestnancov statnej a verejnej spravy
personalne užívateľovi: [redacted]

Od: personalne@uradplace.sk

Užívateľovi: [redacted]@csirt.gov.sk

Odpovedzte, prosím, užívateľovi personalne@uradplace.sk

11.11.2020 08:42

Vážení kolegovia,

pripravuje sa zmena finančného ohodnotenia zamestnancov v štátnej službe a zamestnancov vo verejnom záujme.

Návrh ohodnotenia zamestnancov je uvedený na portáli <http://uradprace.sk/platy.php?id=plat&=platSdf23Xs23>

Na tomto portáli bude informácia predbežne umiestnená do 1.12.2020.

Informácia bude pre širokú verejnosť zverejnená v dátume účinnosti novely zákonov č.552/2003 Z.z o výkone práce vo verejnom záujme v znení neskorších predpisov resp. Zákon č. 400/2009 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Pre prihlásenie použite Váš doménový účet (meno/heslo do Vášho počítača).

S pozdravom

Vedúci oddelenia ekonomického zabezpečenia

<http://www.uradplace.sk/>

Online



MINISTERSTVO

INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Ako na phishing? (VIII.)

- Na zvýšenie dôveryhodnosti útočníci použijú podpis dôveryhodného pracovníka s autoritou
- Tieto údaje je možné získať z otvorených zdrojov, alebo pomocou sociálneho inžinierstva (Výročná správa, telefonát, starý interný telefónny zoznam, ktorý nebol skartovaný a našiel sa v koši)



Zmeny v ohodnotení zamestnancov statnej a verejnej spravy
personalne užívateľovi: [redacted]

Od: personalne@uradplace.sk

Užívateľovi: [redacted]@csirt.gov.sk

Odpovedzte, prosím, užívateľovi personalne@uradplace.sk

11.11.2020 08:42

Vážení kolegovia,

pripravuje sa zmena finančného ohodnotenia zamestnancov v štátnej službe a zamestnancov vo verejnom záujme.

Návrh ohodnotenia zamestnancov je uvedený na portáli <http://uradprace.sk/platy.php?id=plat&=platSdf23Xs23>

Na tomto portáli bude informácia predbežne umiestnená do 1.12.2020.

Informácia bude pre širokú verejnosť zverejnená v dátume účinnosti novely zákonov č.552/2003 Z.z o výkone práce vo verejnom záujme v znení neskorších predpisov resp. Zákon č. 400/2009 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Pre prihlásenie použite Váš doménový účet (meno/heslo do Vášho počítača).

S pozdravom
Vedúci oddelenia ekonomického zabezpečenia

<http://www.uradplace.sk/>

Online



IDENTIFIKÁCIA A AUTENTIFIKÁCIA (HESLÁ)

Časté chyby: Rovnaké heslá na viacerých účtoch



Časté chyby: Používanie služobných prostriedkov na súkromné účely



Zdroj: www.freepik.com



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

www.mirri.gov.sk

 **CSIRT.SK**

Identifikácia a autentifikácia

Útoky na heslá:

- známe a frekventované slová > útok pomocou slovníkov
- generovanie krátkych hesiel > útok hrubou silou
- sociálne inžinierstvo



Zdroj: www.freepik.com

Identifikácia a autentifikácia

<https://haveibeenpwned.com/>

The screenshot shows the homepage of the 'Have I Been Pwned' website. At the top, there is a navigation menu with links for Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main heading is a large white box containing the text ';--have i been pwned?'. Below this, a sub-heading reads 'Check if your email or phone is in a data breach'. A search input field is provided with the placeholder text 'email or phone (international format)' and a 'pwned?' button. Below the search field, there is a section for 'Generate secure, unique passwords for every account' with a link to 'Learn more at 1Password.com'. At the bottom, statistics are displayed: 538 pwned websites, 11,288,428,986 pwned accounts, 114,106 pastes, and 200,545,326 paste accounts. Two columns of 'Largest breaches' and 'Recently added breaches' are also visible, listing various data breaches with their respective account counts.

This screenshot shows a detailed view of the 'Largest breaches' and 'Recently added breaches' section. It features two columns of data. The 'Largest breaches' column lists major data breaches such as 'Collection #1 accounts' (772,904,991 accounts), 'Verifications.io accounts' (763,117,241 accounts), and 'Onliner Spambot accounts' (711,477,622 accounts). The 'Recently added breaches' column lists more recent breaches like 'CityBee accounts' (110,156 accounts), 'Ge.tt accounts' (2,481,121 accounts), and 'StoryBird accounts' (1,047,200 accounts). Each entry includes a small icon representing the breach and the total number of accounts affected.

This screenshot shows the 'Pwned Passwords' section of the website. It features a search input field with a 'pwned?' button. Below the search field, a message reads: 'Oh no — pwned! This password has been seen 22 269 times before. This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!'. The background of this section is a dark red color.

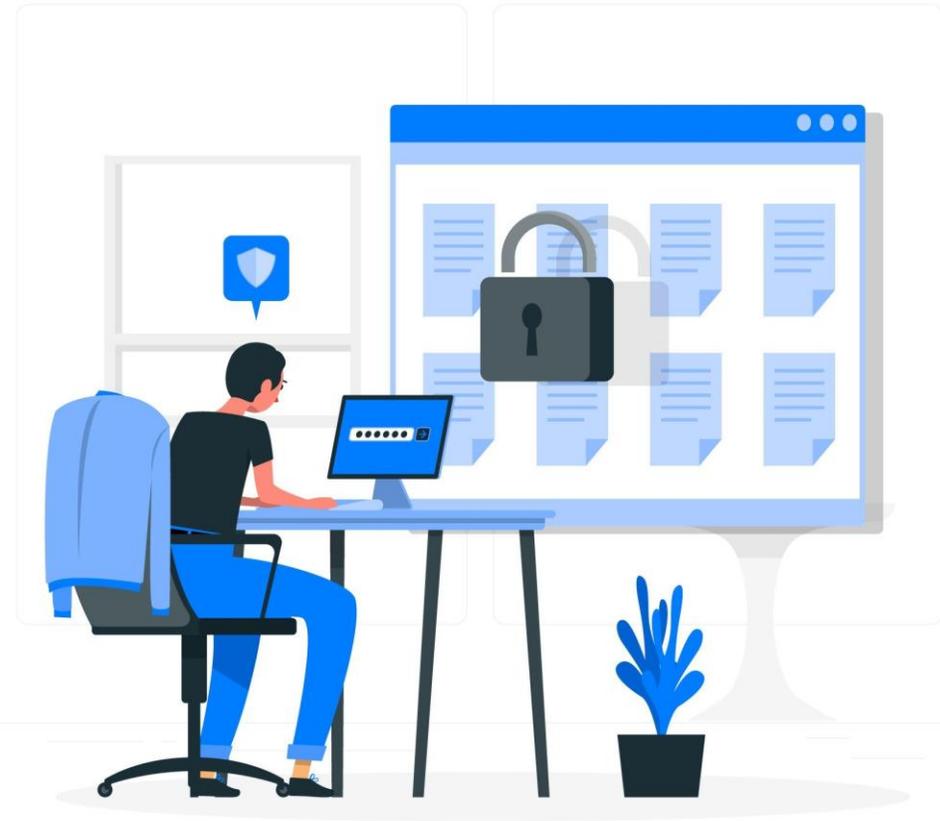
Uchovanie prístupových údajov

heslá sú tajné

- správca hesiel

nevhodné:

- obrazovka monitora
- klávesnica
- kalendár
- kontakty v mobile



Zdroj: www.freepik.com

Uchovanie prístupových údajov

- aplikácie na správu hesiel ponúkajú možnosť prístupí k svojim heslám z akéhokoľvek zariadenia
- umožňujú vygenerovanie náhodného hesla a jeho následné automatické zapamätanie

 **bitwarden**

1Password 

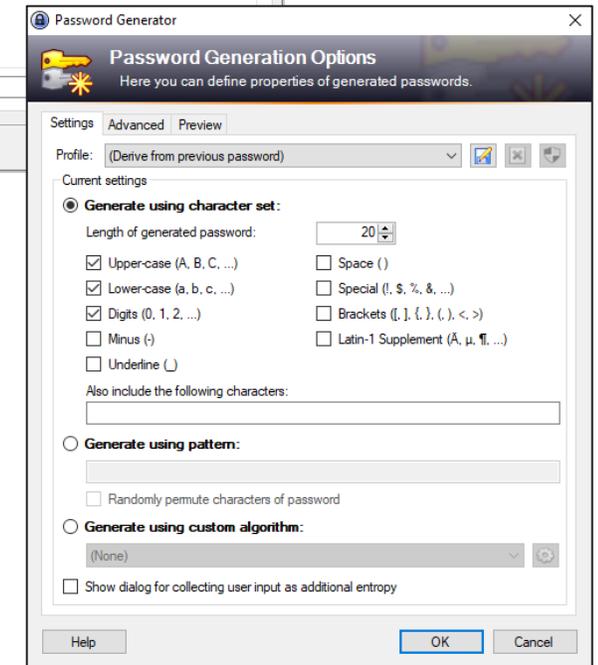
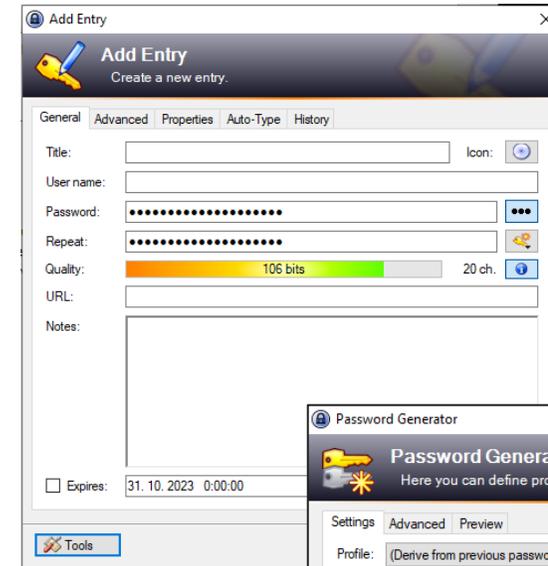
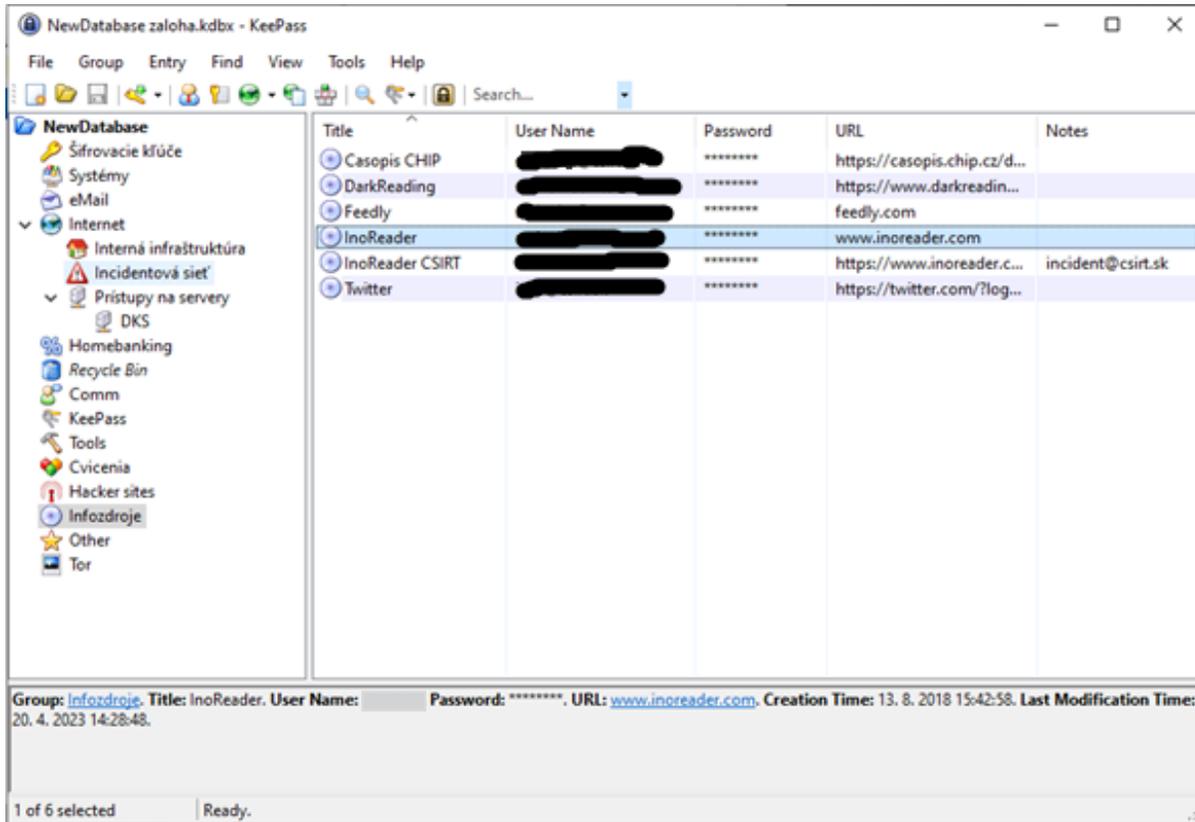
 dashlane



KeePass

Uchovanie prístupových údajov

KeepPass



Krádež prístupových údajov

1. Strata Kontroly nad svojim účtom

- nastavenia, posielanie správ a zverejňovanie obsahu vo vašom mene, zneužitie účtu/identity

2. Súkromie

- ohrozenie vašich osobných informácií, zneužitie na vašu manipuláciu

3. Kybernetická Bezpečnosť

- krádež identity aj v iných službách, kam heslo funguje, resp. kam sa prihlasujete danou službou (Facebook, Gmail)

4. Dôveryhodnosť

- ak niekto vytvorí nevhodný obsah alebo správy pod vaším menom, môže to mať negatívny vplyv na váš vzťah s priateľmi, rodinou alebo v zamestnaní

5. Zneužitie

- šírenie nepravdivých informácií, vydieranie alebo iné nebezpečné správanie, prihlásenie sa alebo registrácia na iné služby



MINISTERSTVO

INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Viacfaktorová autentifikácia



+ PIN

Dvojfaktorová – 2 faktory - znalosť a vlastníctvo

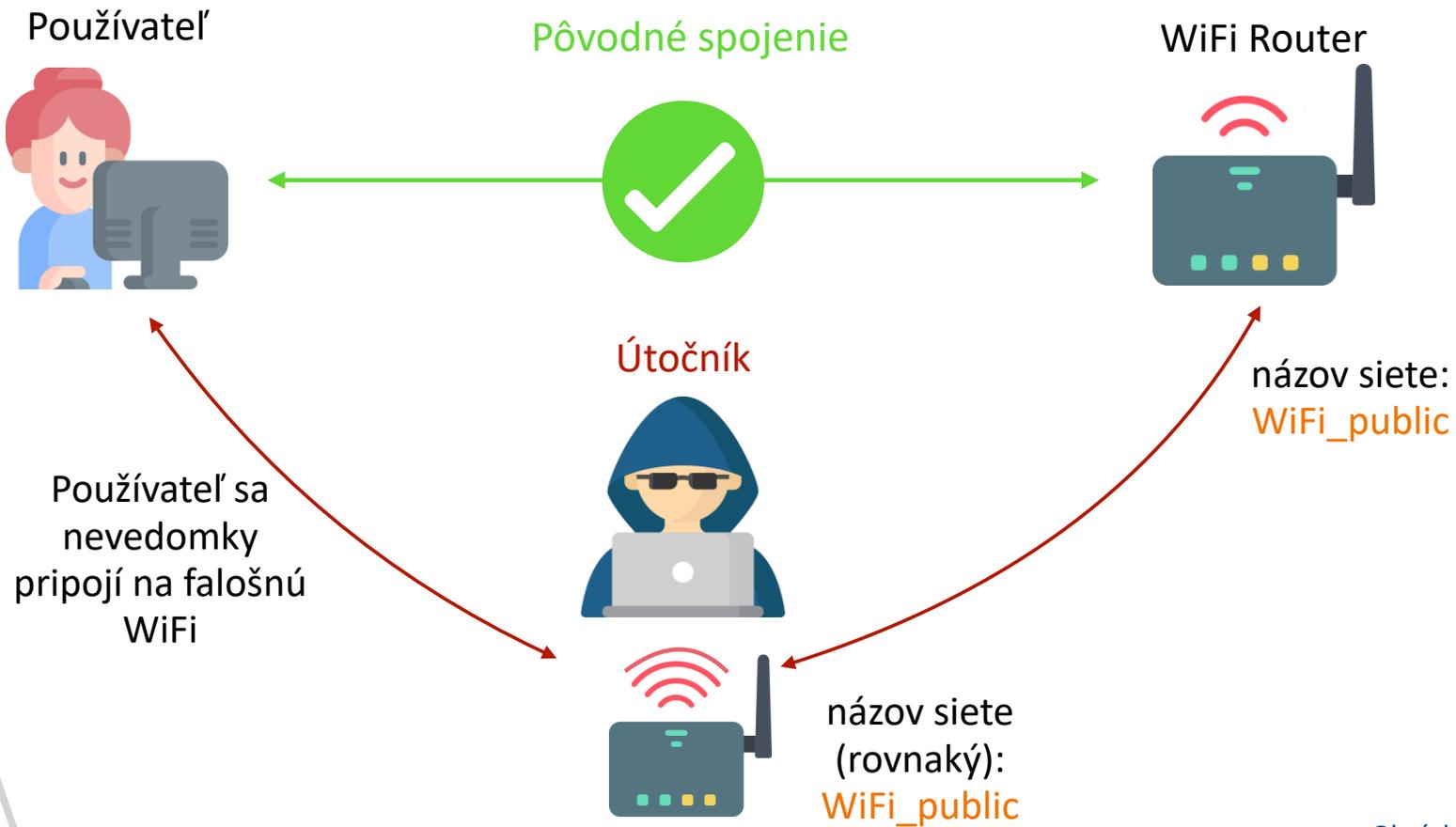
Faktor autentifikácie - faktor, pri ktorom sa potvrdilo, že je spojený s osobou

- na základe **držby** - je faktor, ktorého držbu je osoba povinná preukázať („niečo mám“)
- na základe **poznania** - je faktor, ktorého poznanie je osoba povinná preukázať („niečo viem“)
- **inherentný** faktor autentifikácie - je založený na fyzickej vlastnosti fyzickej osoby, pričom osoba je povinná preukázať, že má túto fyzickú vlastnosť („niečo som“)

- internet banking
- výber hotovosti



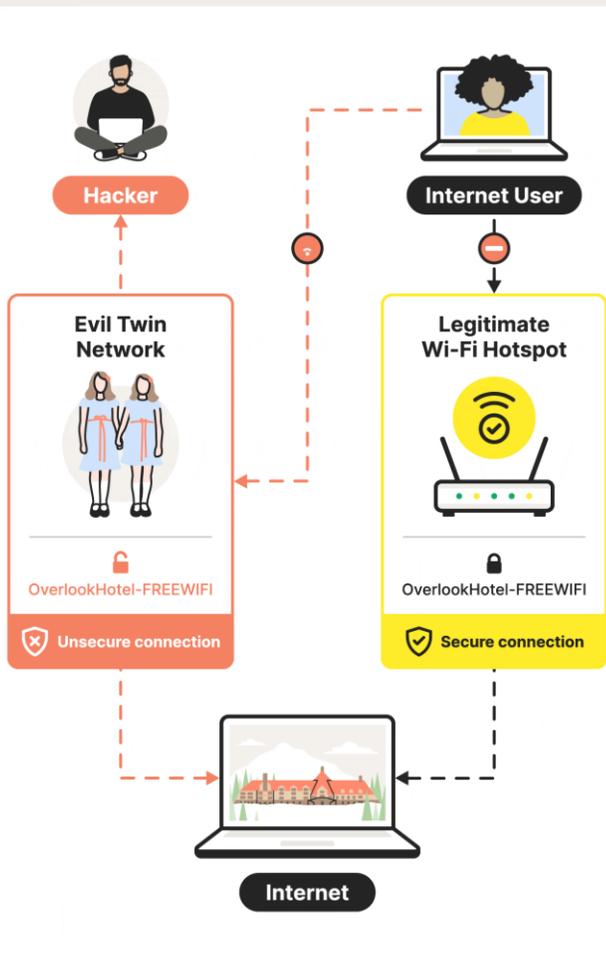
Verejné WiFi siete



Obrázky: Flaticon.com

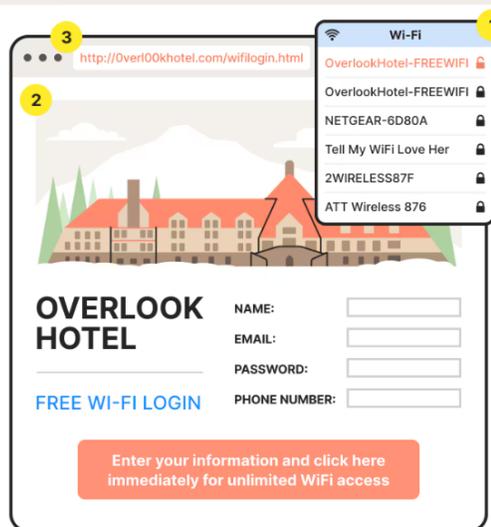
Evil Twin Attacks Explained

All internet and no security can make surfing the web a risky experience.



WiFi - Evil Twin

Warning Signs of an Evil Twin Attack



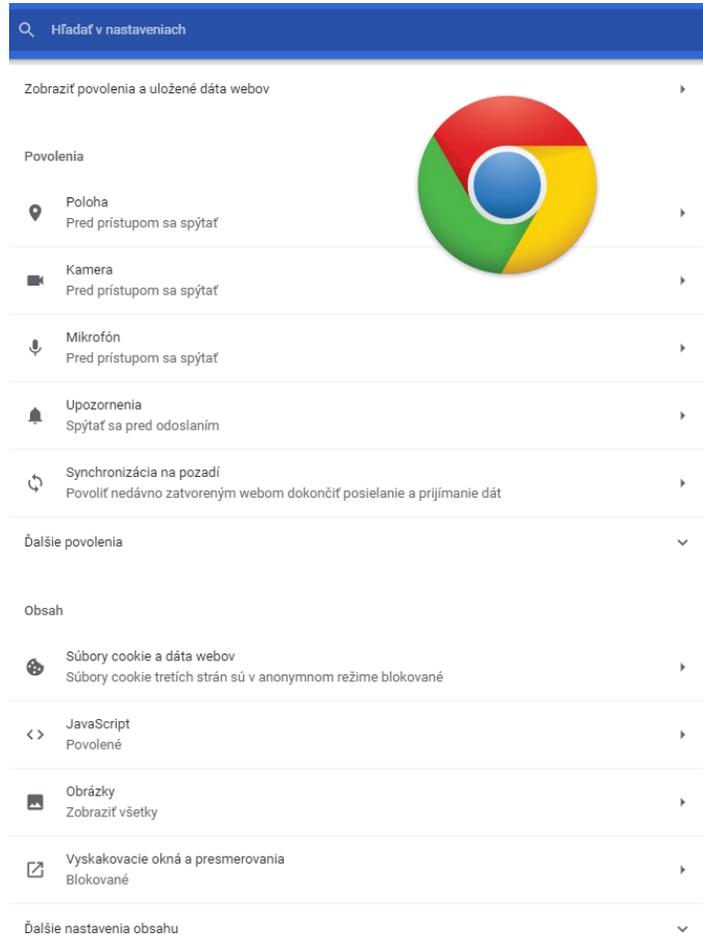
- 1 Duplicate network names
- 2 Suspicious captive portal pages
- 3 Lack of security

Evil Twin Attack Protection Tips

Follow these tips to keep any evil twins from ruining your internet experience.

- Avoid unsecured Wi-Fi networks
- Use a VPN
- Stick to "HTTPS" websites
- Use two-factor authentication
- Avoid using private accounts on public Wi-Fi
- Turn off auto-connect
- Use your own personal hotspot

Bezpečnosť webových prehliadačov



<https://github.com/gorhill/uBlock>



<https://www.eff.org/https-everywhere>



<https://privacybadger.org/>

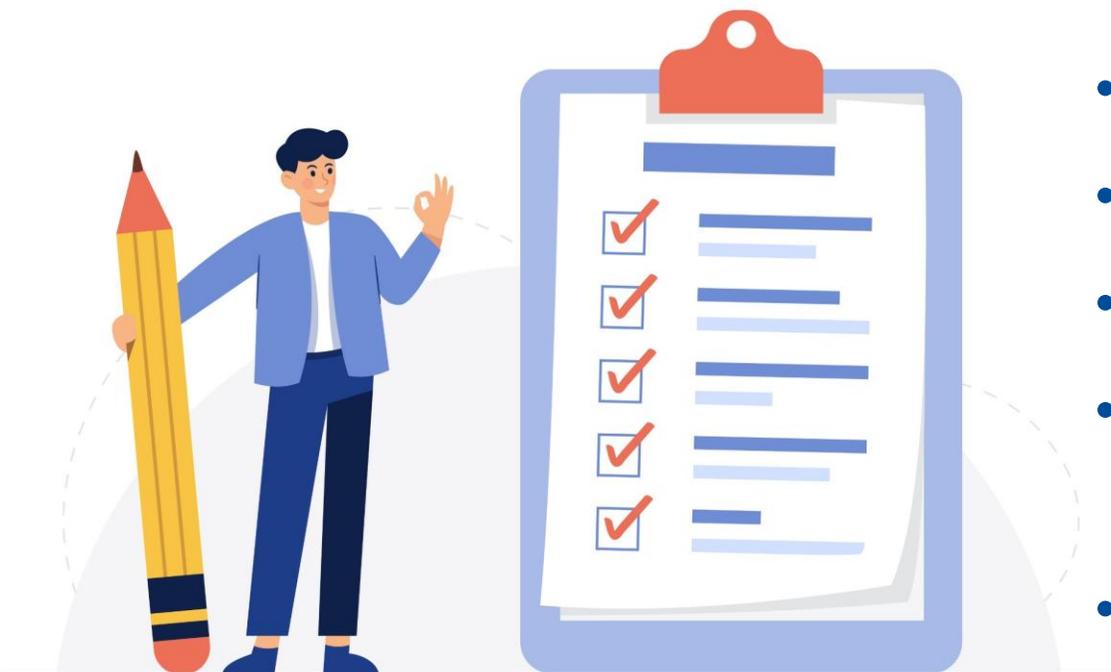


MINISTERSTVO

INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Odporúčania na záver

- Vyhodnocujte podozrivé emailové správy
- Aktualizujte operačný systém a aplikácie
- Používajte silné heslá a bezpečne ich ukladajte
- Používajte antivírusový program
- Šifrujte údaje pri ich ukladaní a prenose
- Používajte bezpečnostné nastavenia webových prehliadačov
- Identifikujte a hláste bezpečnostné incidenty



Zdroj: www.freepik.com



ĎAKUJEME!

www.mirri.gov.sk