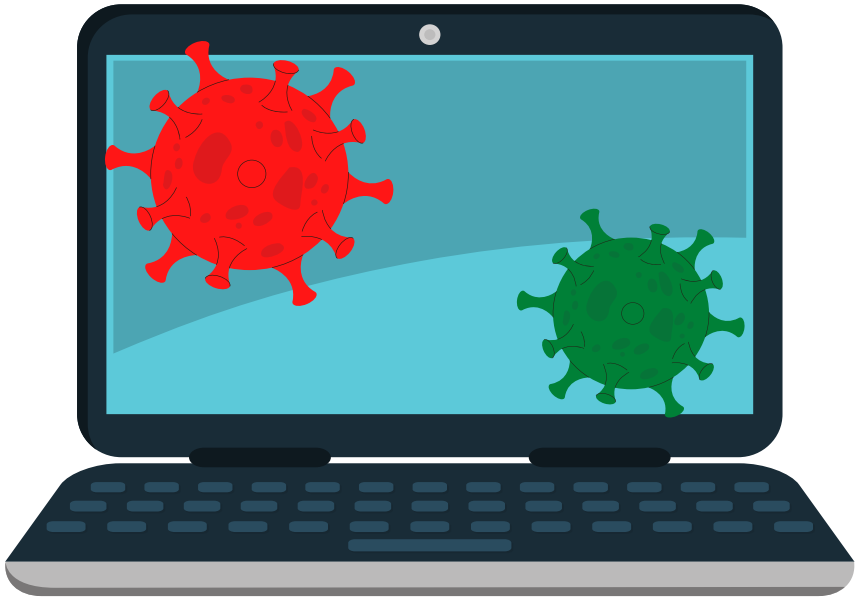
Informačná bezpečnosť

Kybernetický bezpečnostný tím GKMKE



Gymnázium sv. Košických mučeníkov

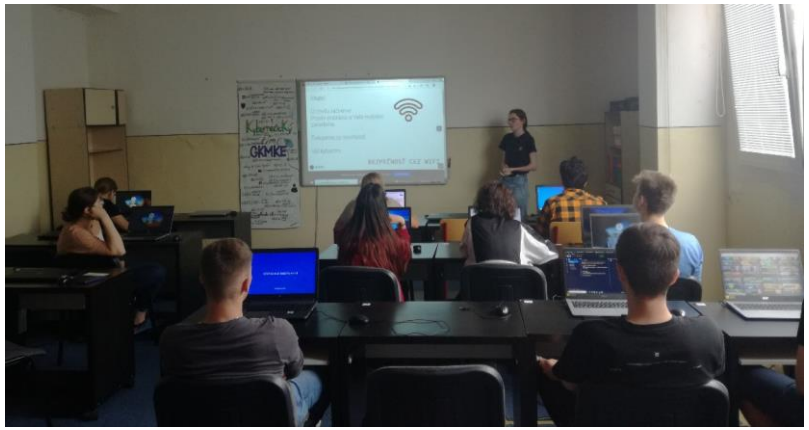
Čordákova 50, Košice - KVP

Zdroj: https://www.kosicekmk.sk/index.php/content

KyberTím GKMKE

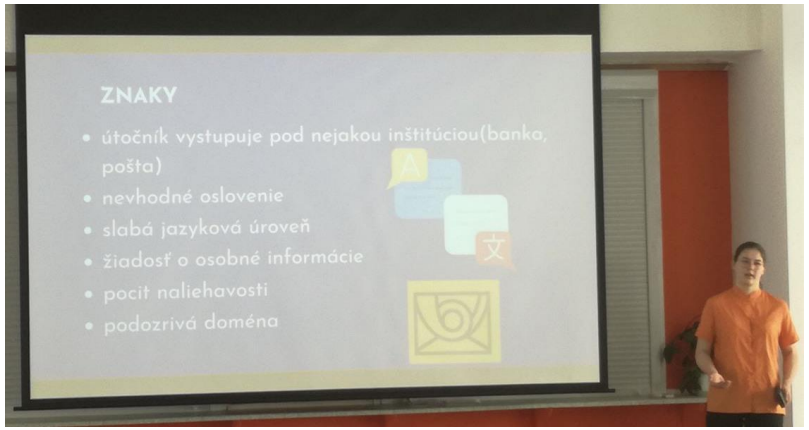
- od šk. roka 2021/2022
- projekt CSIRT UPJŠ: **Nauč sa základy informačnej bezpečnosti a vzdelávaj svoje okolie** - vzdelávanie (https://csirt.upjs.sk/#/projekty/zvysovanie-bezpecnostneho-povedomia-na-SS)
- aktivity: https://gym.gkmke.sk/it-aktivity/kyberneticka-bezpecnost/
- projekt **Výnimočné školy 2022/2023**

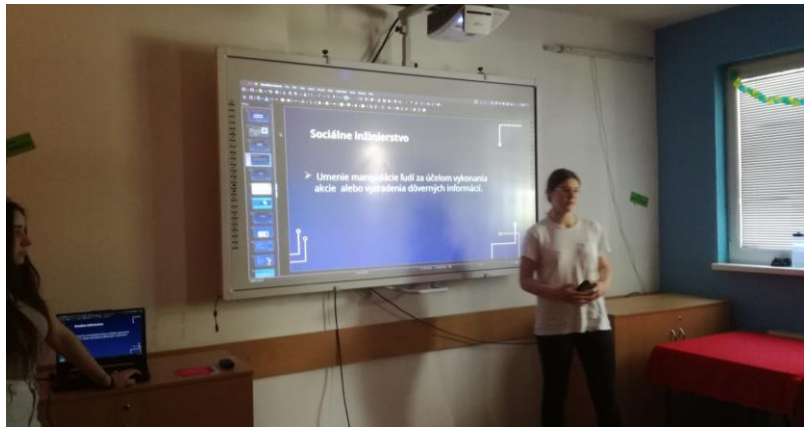
Zdroj: https://sk-nic.sk/pt/fond-sk-nic/
https://m.facebook.com/profile.php?id=100064622697239&_rdr

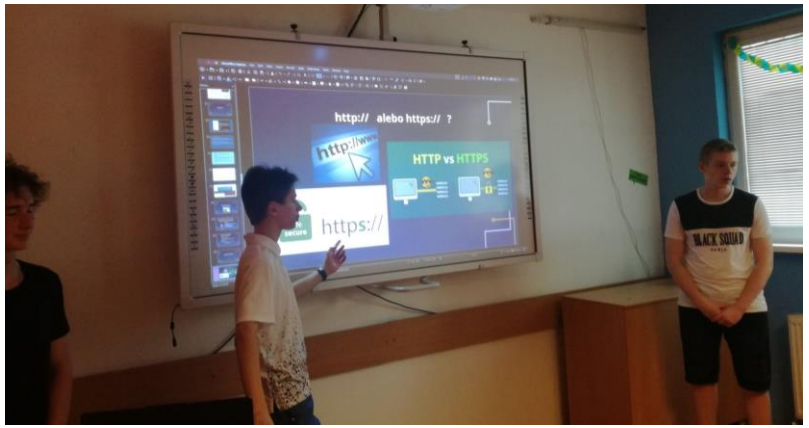


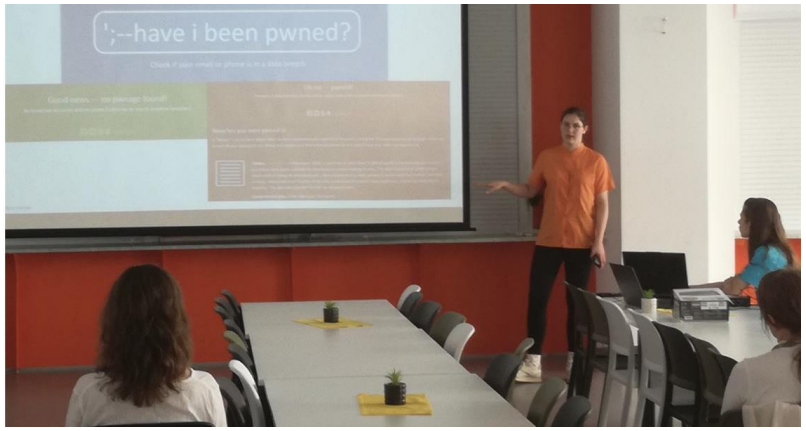
Vzdelávacie aktivity pre žiakov našej školy

2021/2022



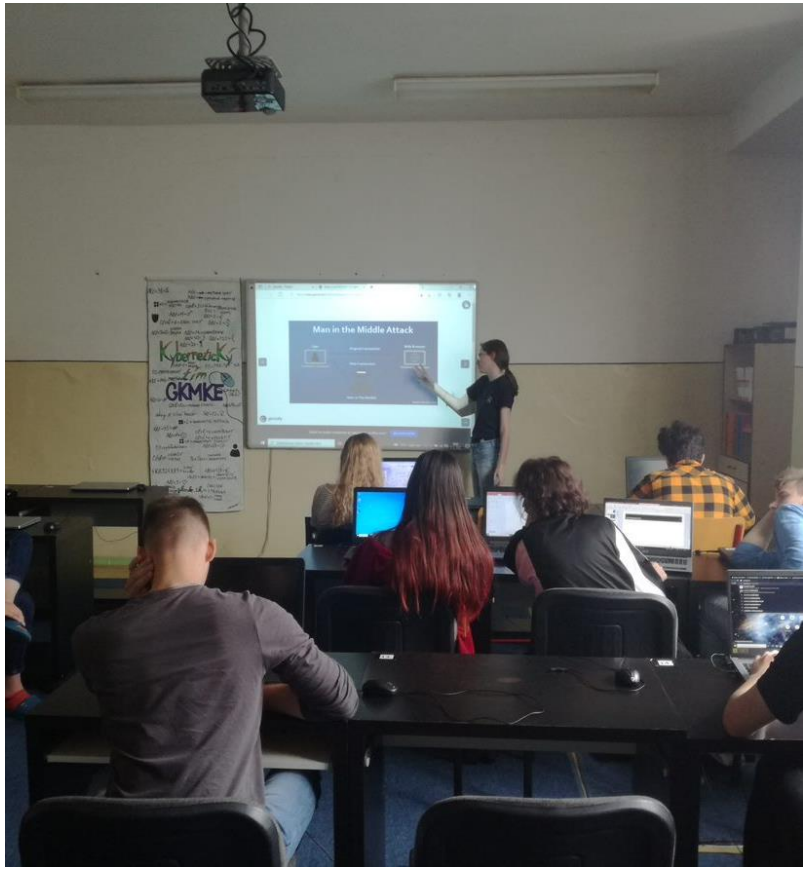






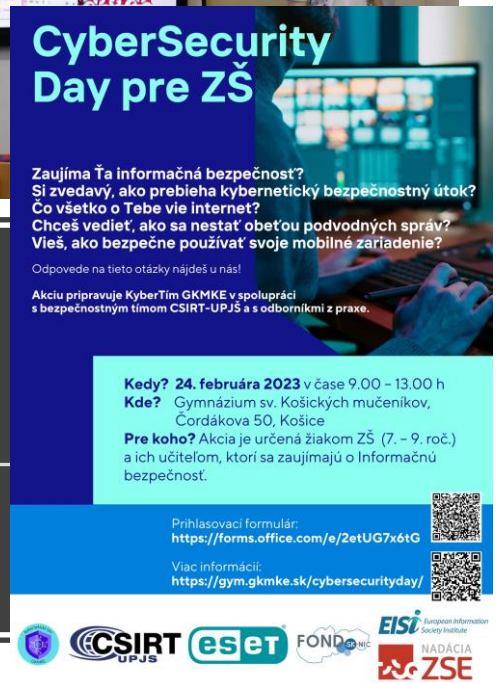
Workshopy pre rodičov, Centrum Dorka

2021/2022



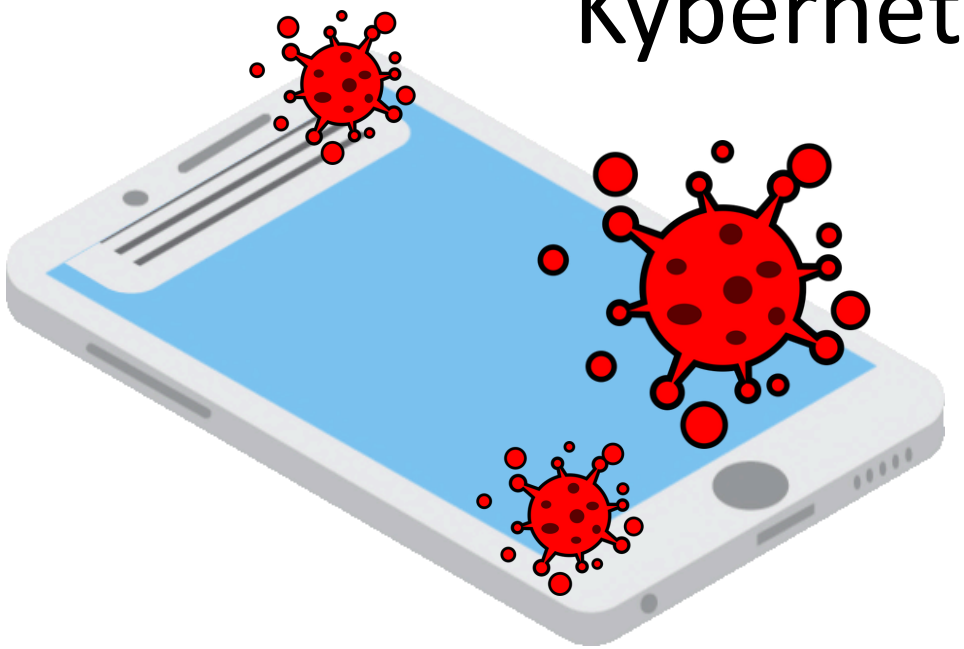
Workshopy pre žiakov, ZPP Radosť

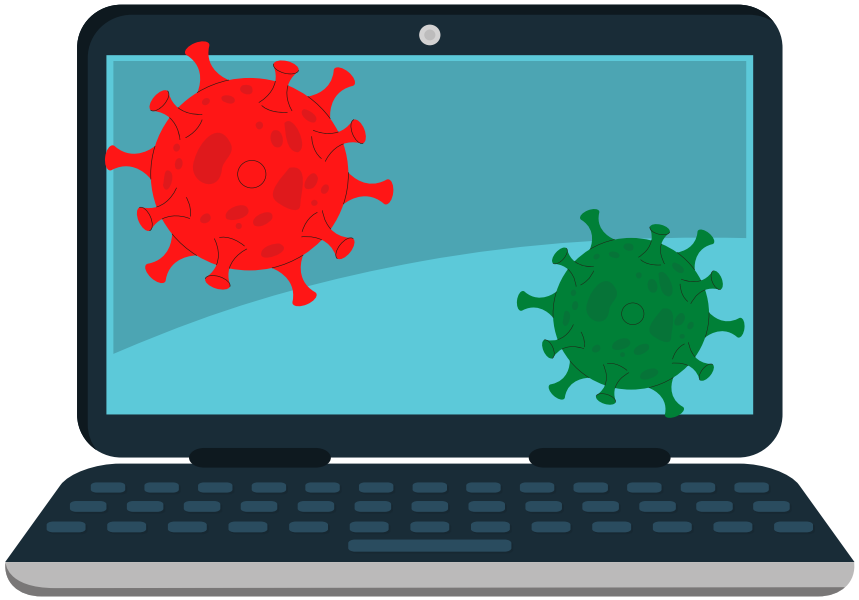
seniorov, 2022/2023

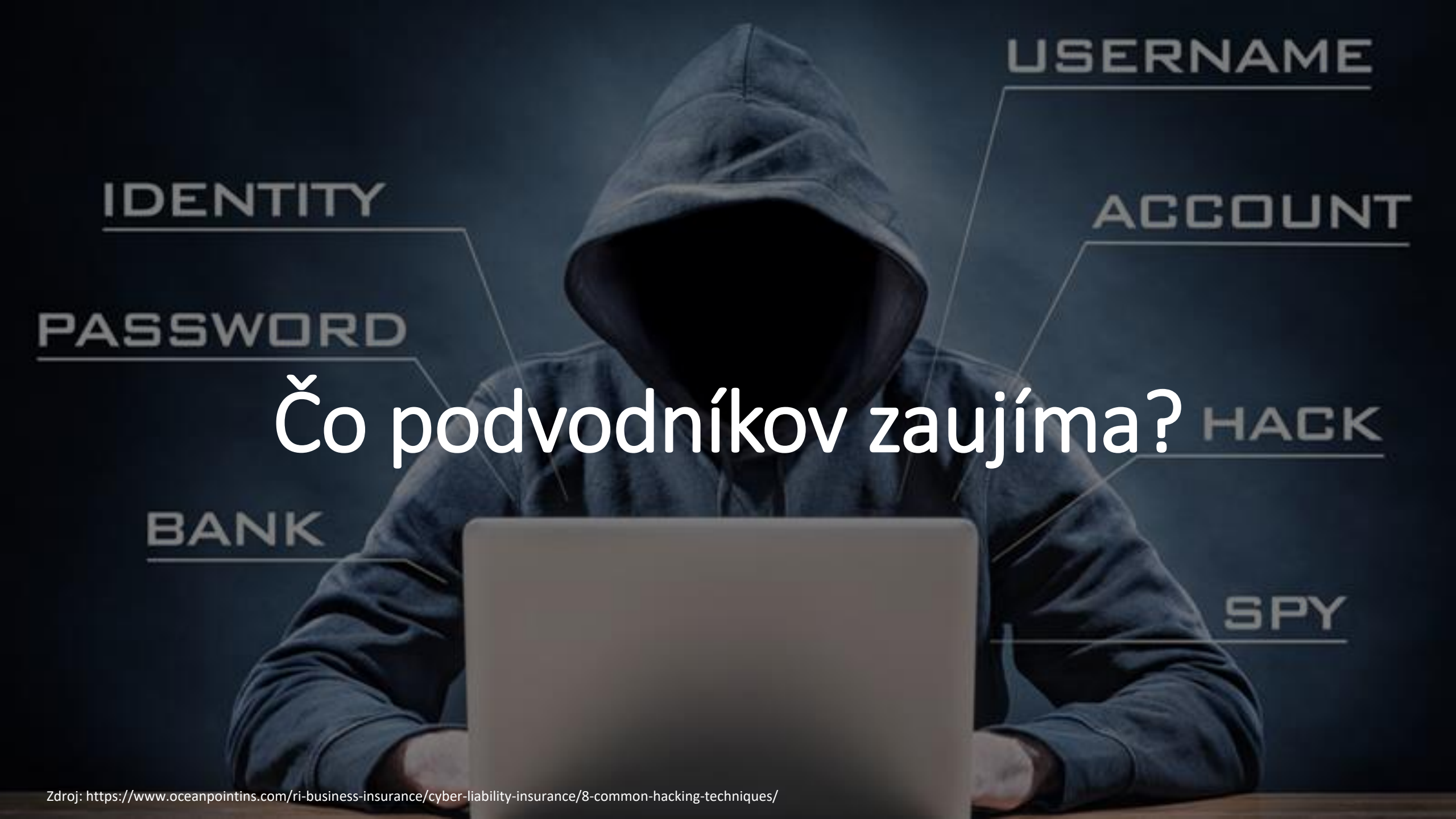


Ako sa nestať obeťou podvodných správ

Kybernetický tím GKMKE







Čo podvodníkov zaujíma?

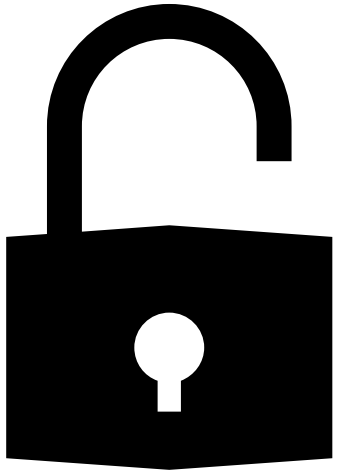
Zdroj: https://www.oceanpointins.com/ri-business-insurance/cyber-liability-insurance/8-common-hacking-techniques/

ZAUJÍMAVÉ INFORMÁCIE

- používateľské meno a heslo (najmä do internetbankingu)
- rodné číslo
- čísla bankových účtov
- PIN kód (osobné identifikačné číslo)
- čísla platobných kariet a ich CVC kódy

Bezpečnosť z pohľadu používateľa

- čo raz zverejníte na internete, ostane už navždy verejné!
- všetky informácie o Vás môžu byť použité pri útokoch sociálnym inžinierstvom,
- zverejňujete cudzím ľuďom vašu adresu, telefónne číslo, rodné číslo, čo máte doma, kedy ste na dovolenke a pod.???
- myslite na súkromie a bezpečnosť!



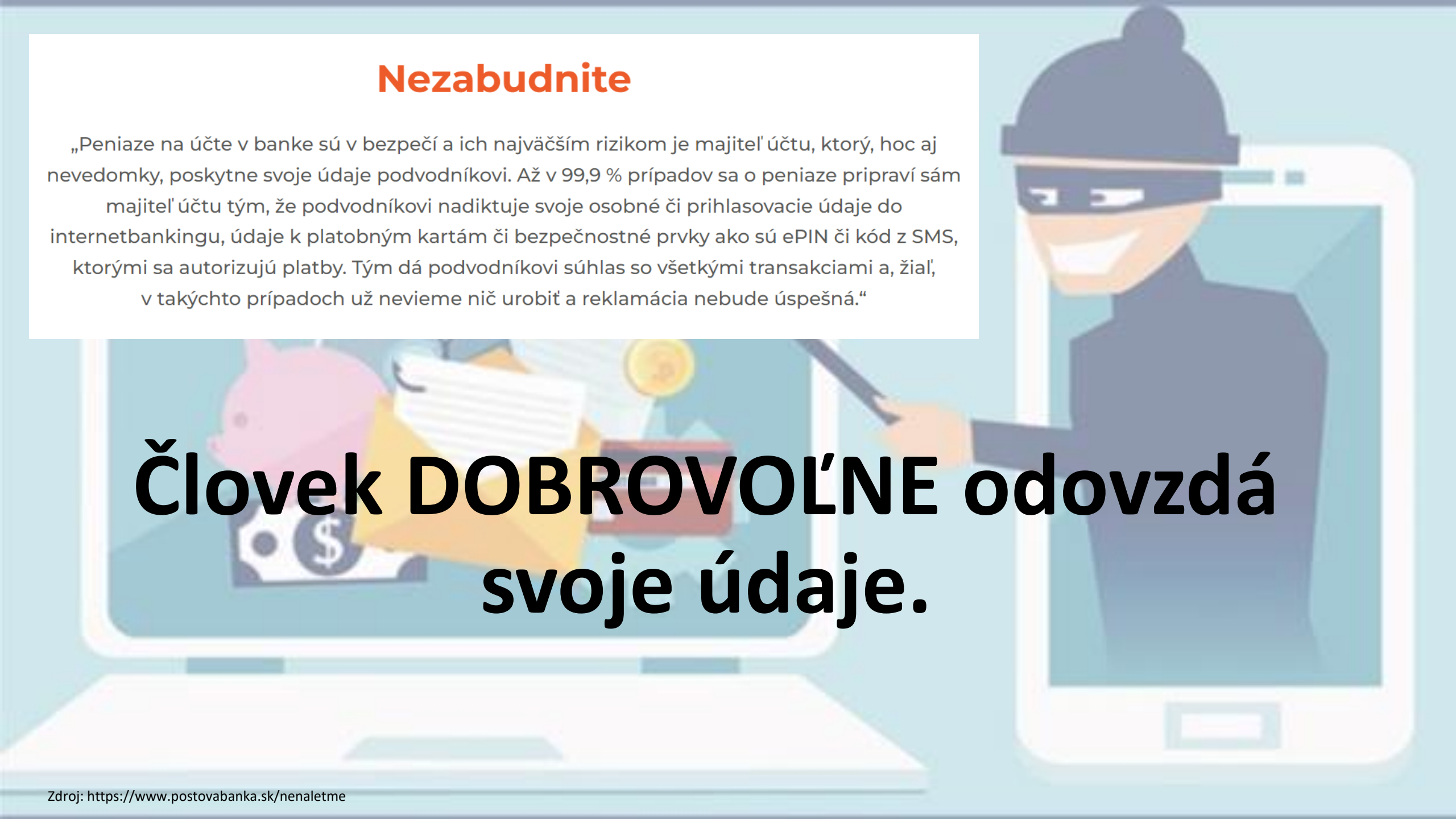
Podvodné správy

Zdroj: https://www.onlinesicherheit.gv.at/Services/News/Vorsicht-vor-Phishing-im-Home-Office.html

36 miliárd phishingových správ ročne!

Nezabudnite

„Peniaze na účte v banke sú v bezpečí a ich najväčším rizikom je majiteľ účtu, ktorý, hoc aj nevedomky, poskytne svoje údaje podvodníkovi. Až v 99,9 % prípadov sa o peniaze pripraví sám majiteľ účtu tým, že podvodníkovi nadiktuje svoje osobné či prihlasovacie údaje do internetbankingu, údaje k platobným kartám či bezpečnostné prvky ako sú ePIN či kód z SMS, ktorými sa autorizujú platby. Tým dá podvodníkovi súhlas so všetkými transakciami a, žiaľ, v takýchto prípadoch už nevieme nič urobiť a reklamácia nebude úspešná.“

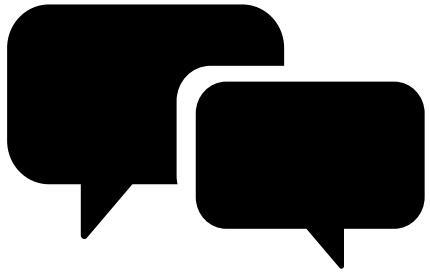


Človek DOBROVOĽNE odovzdá svoje údaje.

Zdroj: https://www.postovabanka.sk/nenaletme

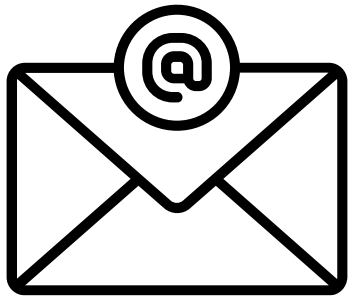
Možnosti útokov

CEZ SMS



CEZ TELEFÓN

CEZ E-MAIL

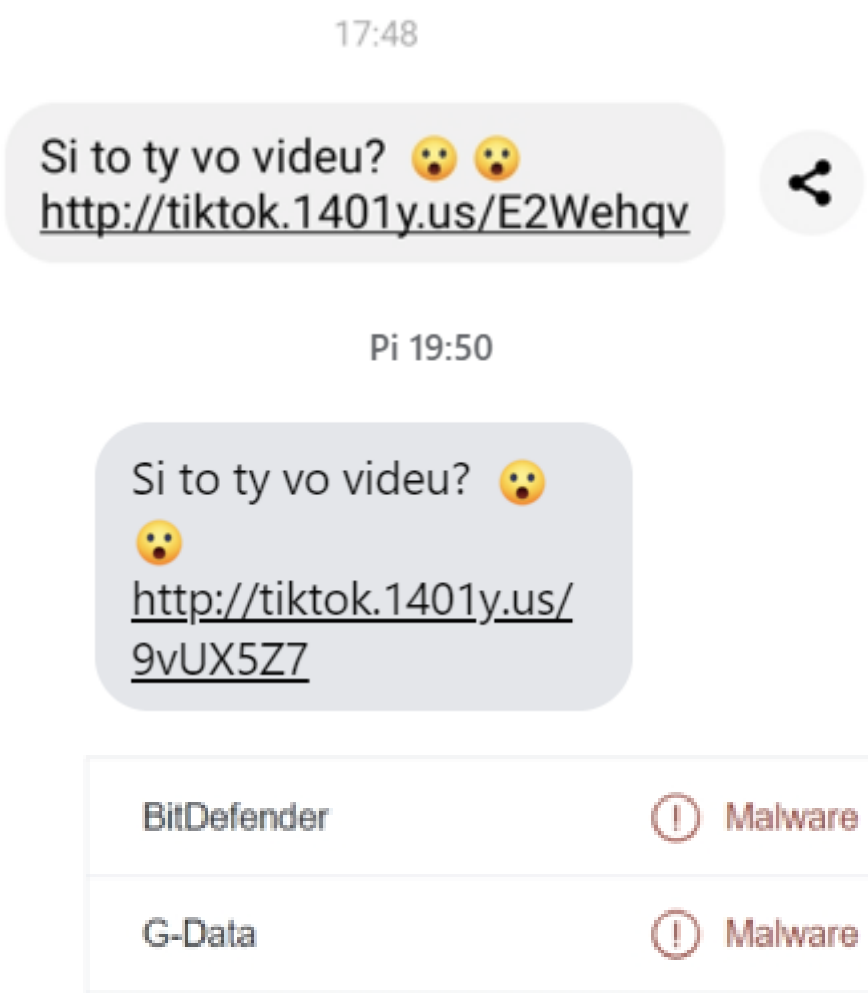


CEZ SOCIÁLNE SIETE

Podvodné správy

CEZ SOCIÁLNE SIETE

Podvodné správy



„Si to ty vo videu“: Pozor na falošné správy od priateľov na Messengeri. Kradnú FB kontá

Nachytali ma, čo teraz?

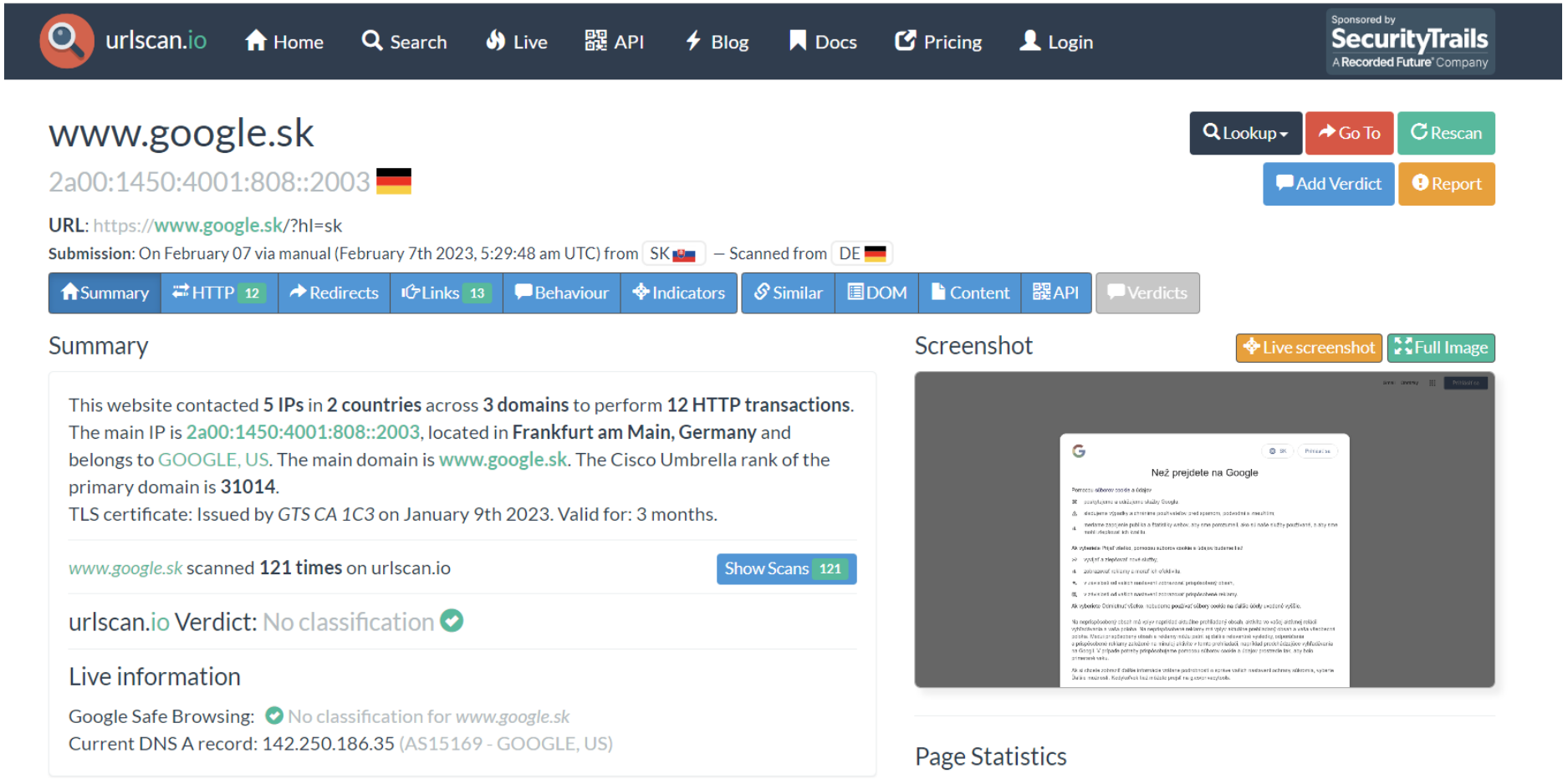
S priateľom, ktorý vám falošné správy posiela, sa odporúčame spojiť mimo sociálnej siete, napríklad telefonicky alebo osobne. Presvedčte sa, či má ku svojmu kontu stále prístup.

V oboch prípadoch – teda i vtedy, ak už hackeri obeť z jej vlastného účtu „vymkli“ zmenou hesla – môžete použiť **náš návod pre zabezpečenie facebookového konta >>>**

Sociálnej sieti viete napríklad nahlásiť, že vaše konto bolo hacknuté. Facebook ho dokáže obnoviť aj v prípade, že hackeri už zmenili e-mailovú adresu prepojenú s účtom. Treba však počítať s tým, že Facebook od vás bude chcieť v rámci preukázania totožnosti napríklad zaslanie skenu občianskeho preukazu.

Zdroj: https://zive.aktuality.sk/clanok/vyQMmui/si-to-ty-vo-videu-pozor-na-falosne-spravy-od-priatelov-na-messengeri-kradnu-fb-konta/

Otestujte odkaz



Otestujte URL adresu: https://urlscan.io/

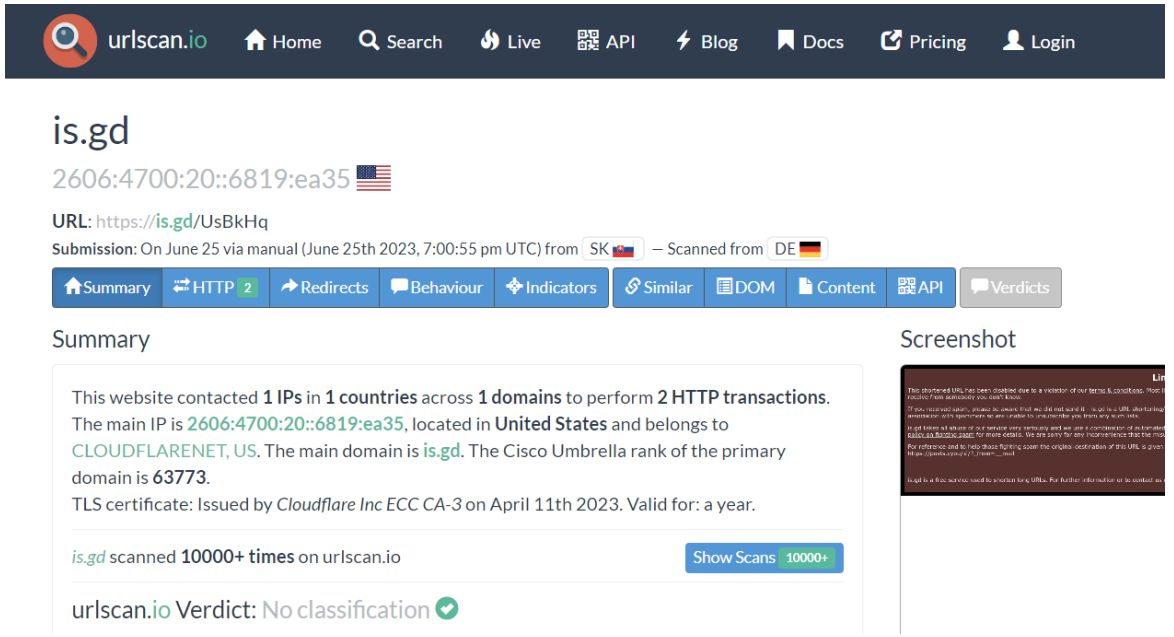
Zdroj: https://urlscan.io/

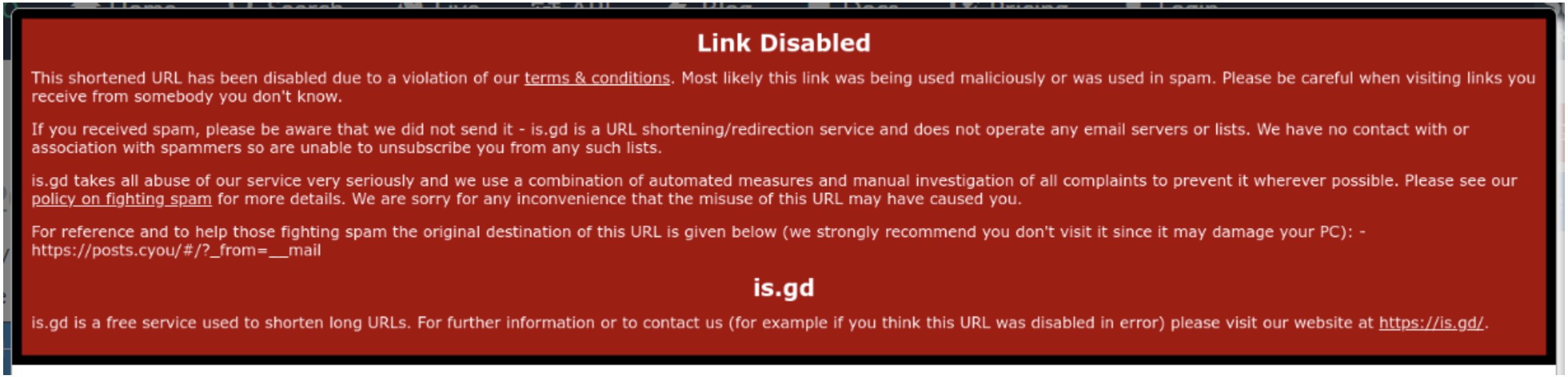
Podvodný odkaz

- P. tlačidlom myši skopírovať, NEKLIKAŤ!!!

https://is.gd/UsBkHq

- Nakopírovať do: https://urlscan.io/

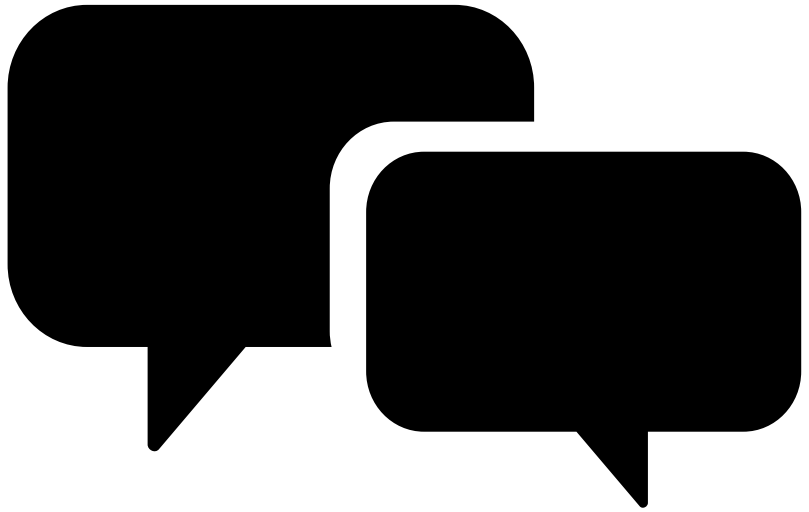




Zdroj: https://urlscan.io/

Podvodné sms správy

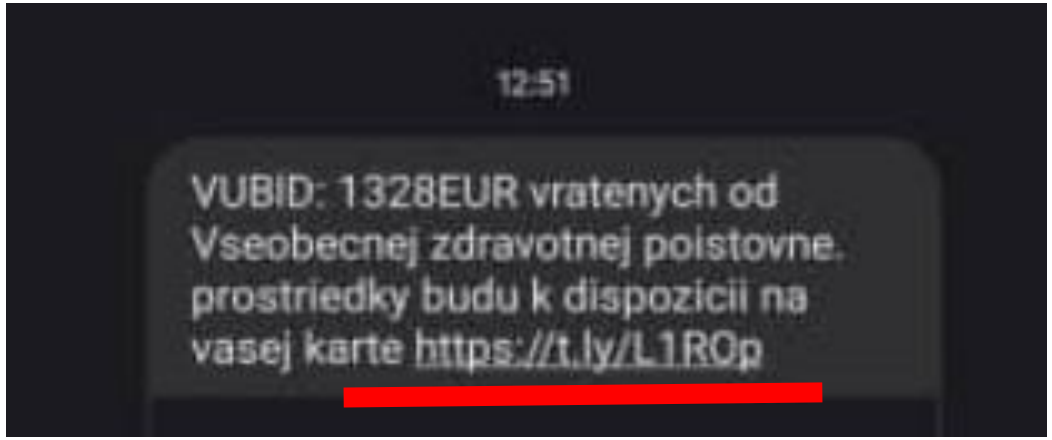
SMISHING



Podvodné sms správy

AKTUÁLNE!

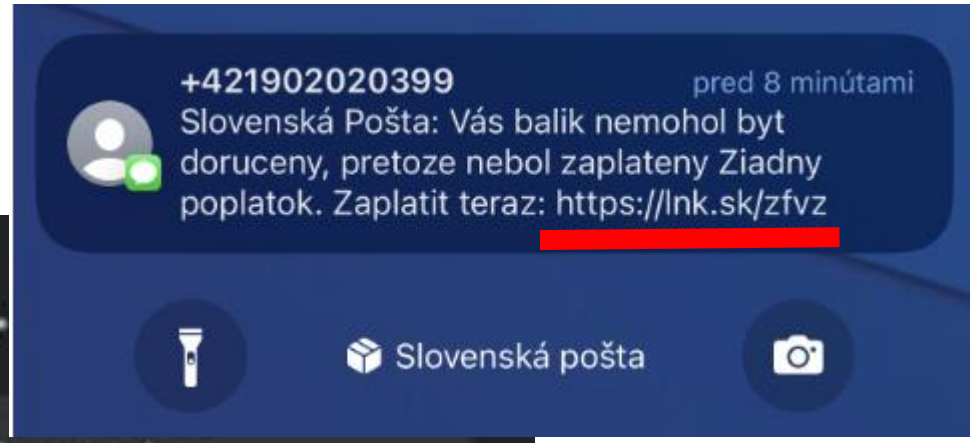
- od Všeobecnej zdravotnej poisťovne
- vrátenie peňazí na platobnú kartu
- podvodný link !
- **poisťovňa nevracia finančné prostriedky takouto formou!!!**

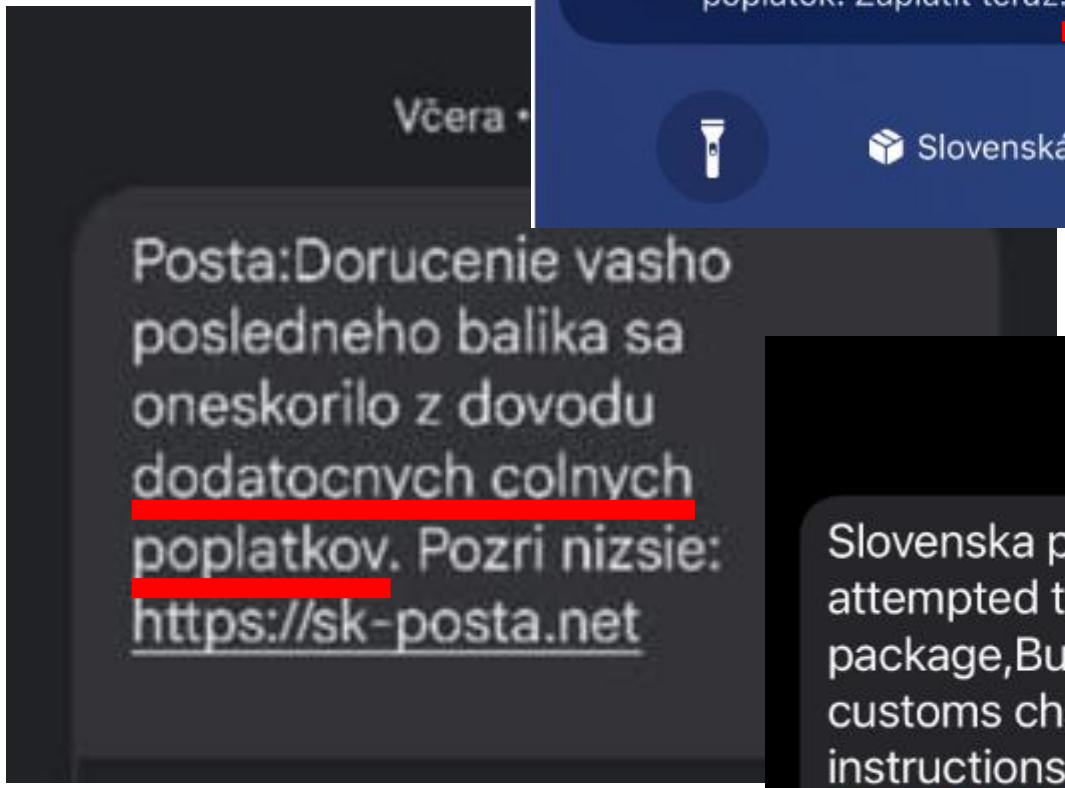


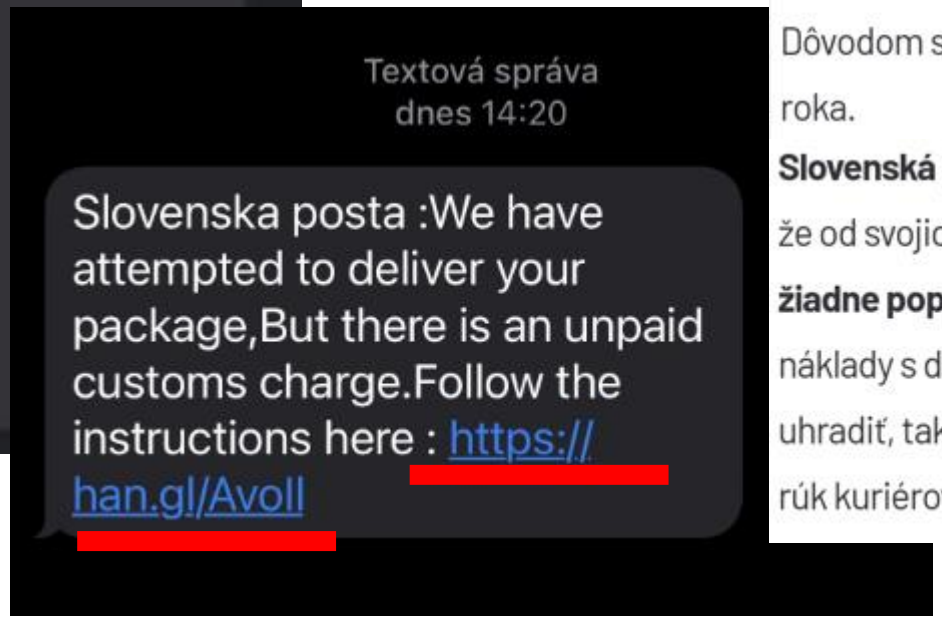
Zdroj: https://vosveteit.zoznam.sk/dalsi-zakerny-sms-podvod-zaplavuje-telefony-slovakov-ak-vam-pride-tato-sprava-vymazte-ju-a-nereagujte-na-nu/

Podvodné sms správy

- od pošty







Pozor, podvodníci spustili masívnu kampaň!

Dnes tu máme podobnú kampaň, ktorej cieľom je oklamať ľudí a získať na ich úkor peniaze. Tentokrát podvodníci ale posielajú vo veľkej miere **SMS správy, v ktorých sa píše, že máte uhradiť drobný poplatok, aby vám mohol byť doručený balík**. V skutočnosti ale ide o sofistikovaný podvod, s ktorým sa budeme v nasledujúcich mesiacoch pravdepodobne stretávať čoraz častejšie. Dôvodom sú blížiace sa sviatky súvisiace s koncom roka.

Slovenská po

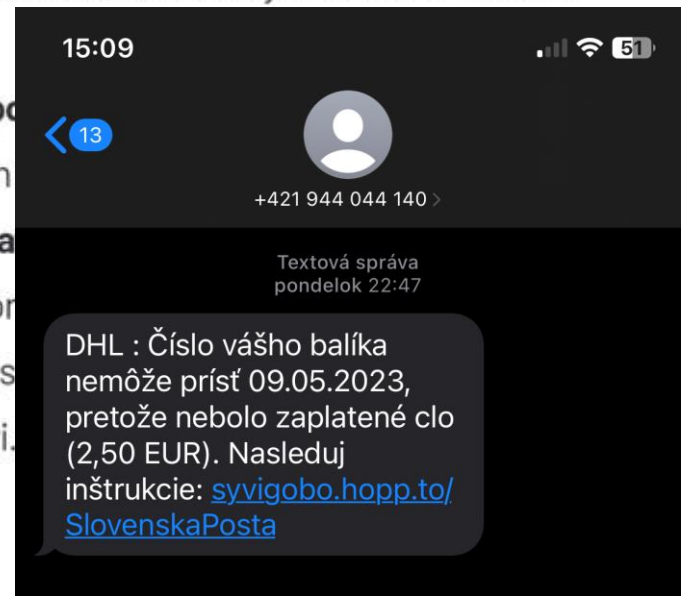
že od svojich

žiadne popla

náklady s dor

uhradiť, tak s

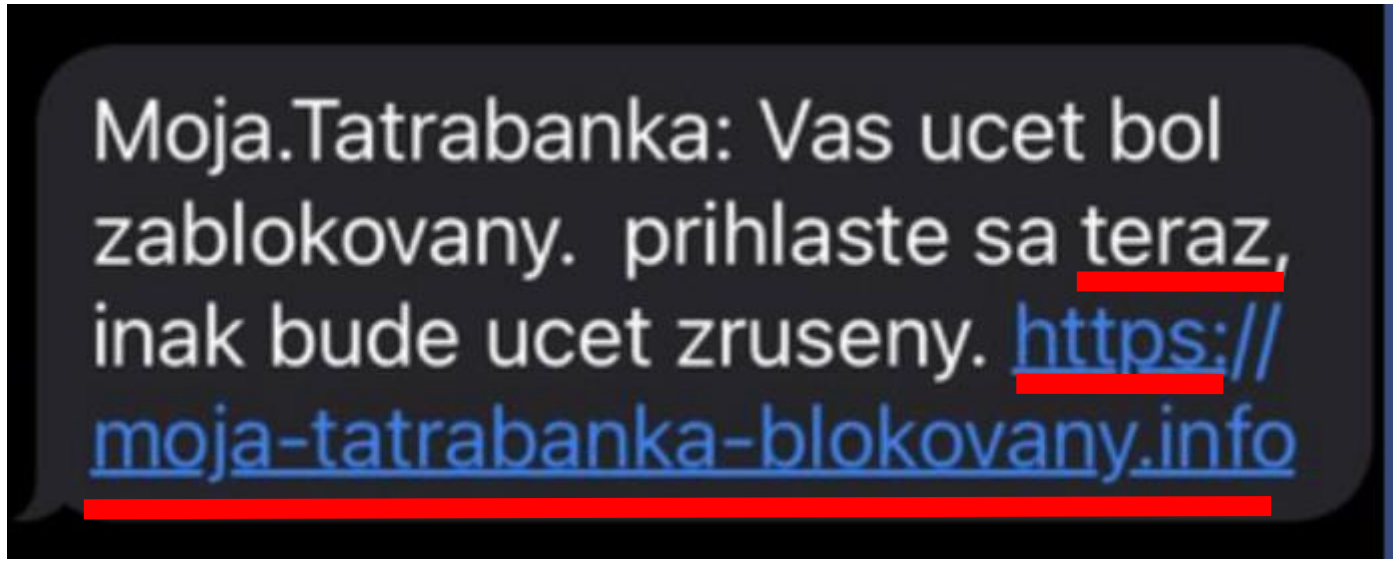
rúk kuriérovi.

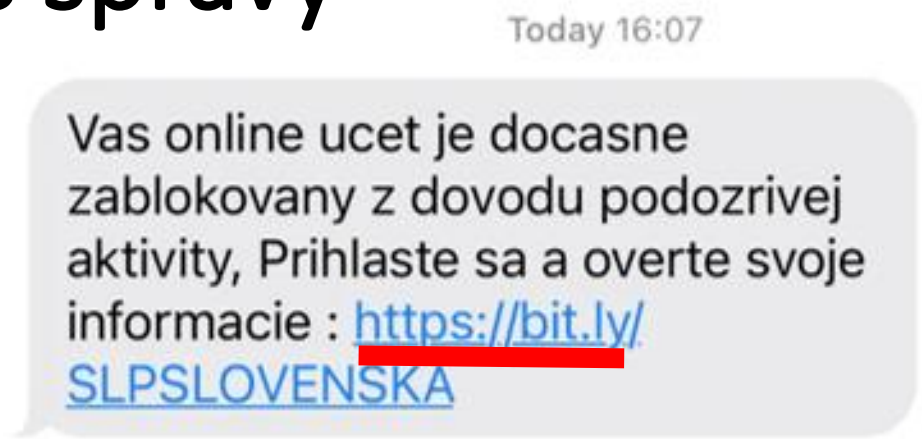


Zdroj: https://www.posta.sk/informacie/pozor-na-podvody

Podvodné sms správy

- od banky





Zdroj: https://ahoj.tv/clanky/clanok/7924/ludia-zacali-dostavat-falosne-smsky-od-bank-policia-upozornuje-na-podvodnikov/
https://www.slsp.sk/sk/aktuality/2021/9/27/slovenska-sporitelna-varuje-internetovi-hackeri-opat-utocia-a-siria-podvodne-e-maily-sms-ky-a-webstranky#/priklady-podvodov/view/2

Podvodné sms správy

- od Finančnej správy SR

- evidujeme dlh,
- pre overenie identity sa prihláste do svojho účtu v banke,
- Link !
- štátne inštitúcie neinformujú občanov o dôležitých informáciách formou SMS správ ani prostredníctvom odkazov, na ktoré je potrebné kliknúť !!!

Zdroj: https://www.info.sk/sprava/229649/dalsi-podvod-cez-smsky-podvodnici-zneuzivaju-meno-uradu-na-taketo-spravy-nereagujte/

Podvodné telefonáty

https://www.youtube.com/watch?v=AzTNrtQ6v_o

VISHING

Zdroj: https://www.youtube.com/watch?v=AzTNrtQ6v_o

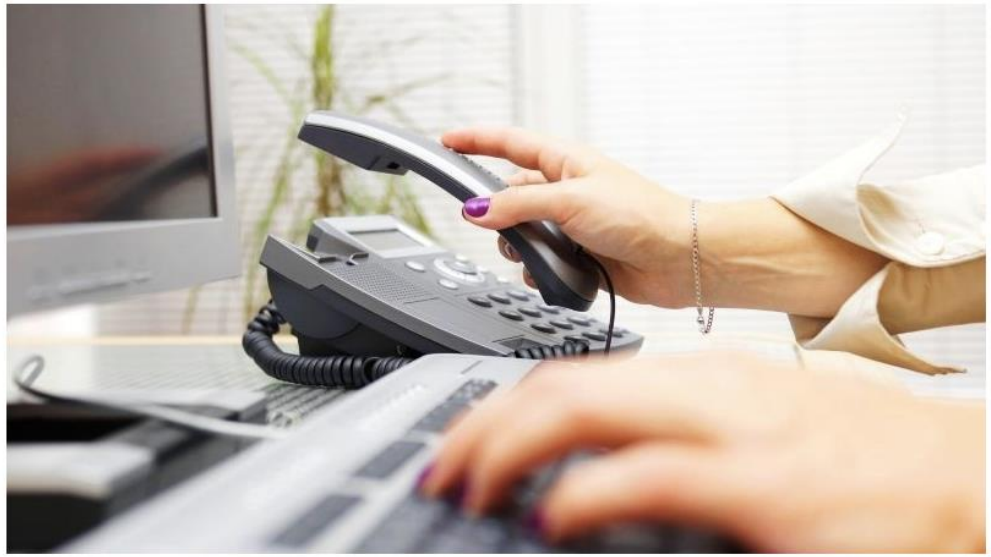
Podvodné telefonáty

- banka
- polícia
- Microsoft

„Dnes nás upozornilo viacero z vás, že podvodníci opäť zodvihli telefóny a kontaktujú vás v mene polície. Anglicky hovoriaci robot sa vydáva za policajtov alebo federálne úrady a tvrdí vám, že vás prídu zatknúť.“, píše

álnej sieti.

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



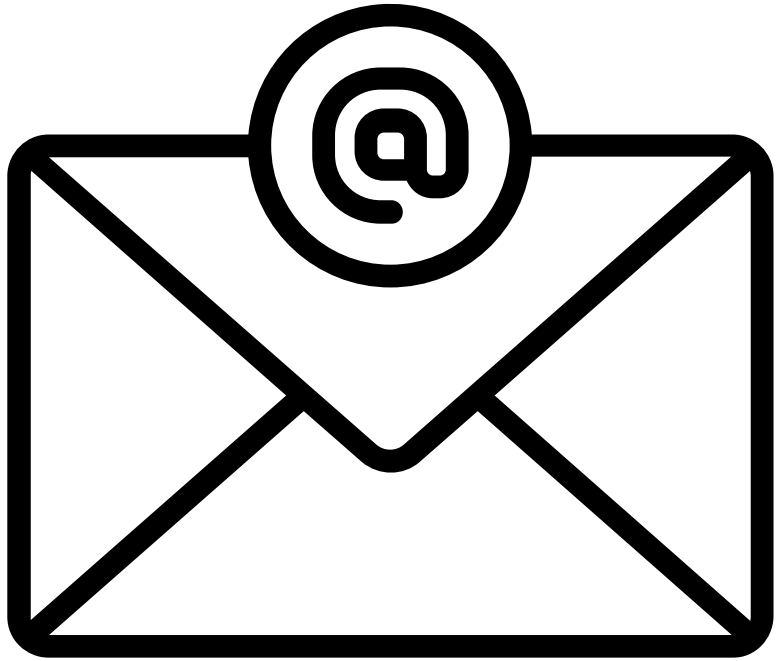
„Polícia s občanmi v žiadnom prípade takýmto spôsobom nekomunikuje. Ak vám zavolá človek alebo robot hovoriaci po anglicky, ktorý sa bude vydávať za políciu, hovor okamžite ukončite a telefónne číslo si zablokujte.“

Zdroj: https://developer.microsoft.com/en-us/games/blog/gdc-and-the-wellbeing-of-our-teams-community/
https://vosveteit.zoznam.sk/aktualne-telefony-slovakov-opat-zaplavuju-stare-zname-podvodne-hovory-ak-vam-niekto-zavola-s-tymto-pribehom-tak-to-rovno-zlozte/
https://zive.aktuality.sk/clanok/150209/falosna-podpora-microsoftu-chcela-muza-pripravit-o-17-000-eur-upozornila-policia/

Podvodné e-maily

https://www.youtube.com/watch?v=2ek-KeYRWdc

PHISHING



Zdroj: https://www.onlinesicherheit.gv.at/Services/News/Vorsicht-vor-Phishing-im-Home-Office.html

Podvodné e-maily  nevhodné oslovenie

A **Allen <lisa@traxtavern.com>**

Komu: Mária Vavrová

Pia 21. 4. 2023 23:59

Dear mariavavrova

We are pleased to inform you that our Company is offering exclusive loans to Individuals and Businesses who are in need of Financial Assistance. Our loan programs are specifically designed to take care of the varied needs of our Clients and offer flexible repayment options.

We understand that obtaining a loan can be a daunting task, but we assure you that the process is simple and transparent. Our team of experienced professionals will guide you through the entire process from application to disbursement of funds.

We offer:

Personal loans
Business loans
Home loans
Educational loans and more.

Our interest rates are competitive, and our loan terms are flexible, allowing you to choose a repayment schedule that suits your financial situation.
To apply for a loan, simply contact me with the details below to provide you with more information.
Thank you for considering us for your financial needs. We look forward to serving you.

Kind Regards:
Allen P. Jones
E-mail: alljonp68@gmail.com
Whatsapp: +1 (418) 669-3356

Podvodné e-maily

výhra

F Facebook <rhuamani@sanpablo.com.pe>

Str 22. 2. 2023 12:54

POZNÁMKA: Ak ste túto správu dostali do priečinka nevyžiadanej pošty / hromadného obsahu, je to z dôvodu obmedzení implementovaných vaším poskytovateľom internetových služieb, preto vás (Facebook Lottery Team) vyzývame, aby ste s ňou zaobchádzali skutočne.
****

Blahoželáme:
Váš E-MAILOVÝ ÚČET vyhral sumu 1 milión libier šterlingov (1 000 000,00 GBP) v prebiehajúcom promo ocenení online na Facebooku a Coronavirus (COVID-19) finančné prostriedky od generálneho riaditeľa Facebooku Inc. Zuckerberg. Vaše číslo lístka je 00545 188 564756. Všetci účastníci boli vybraní prostredníctvom počítačového randomizovaného systému vyžrebovaného z 27 miliónov e-mailových adries cez internet a Lucky Winners. TO ZNAMENÁ, ŽE TO NENÍ IBA FACEBOOK UŽÍVATEĽA, KTORÝ MÔŽE Z TEJTO LOTÉRIE ZÍSKAŤ, TOTO LOTÉRIA JE PRE KAŽDÉHO A AK DOSTANETE E-MAIL, ZNAMENÁ TO, ŽE STE JEDENM Z VÝHODNÝCH VÝHERCOV.

Pošlite ďalej svoje všetky podrobnosti, ako napríklad:
1. Celé meno .....
2. Krajina .....
3. Kontaktná adresa .....
4. Telefónne číslo .....
5. Rodinný stav .....
6. Povolanie .....
7. Spoločnosť .....
8. Vek .....

Podrobnosti prosím pošlite:
Kontaktná osoba: pán David M. Wehner, finančný riaditeľ európskeho regiónu UK
* Prostredníctvom e-mailu: claimunit.facebook@hotmail.com

Váš v službe,
Pán Marc Andreessen
Facilitátor lotérie na Facebooku.

********** *******
Nepochybujte o tomto liste alebo ho ignorujte, pretože sme pripravení odovzdať vám vaše neuveriteľné ocenenie od Facebooku.

Podvodné e-maily

výhra

FI **Facebook Inc <rafael.pombo@inocar.mil.ec>**
Uto 26. 4. 2022 11:37

POZNÁMKA: Ak ste túto správu dostali do priečinka nevyžiadanej pošty / hromadného obsahu, je to z dôvodu obmedzení implementovaných vaším poskytovateľom internetových služieb, preto vás (Facebook Lottery Team) vyzývame, aby ste s ňou zaobchádzali skutočne.
****

Blahoželáme:
Váš E-MAILOVÝ ÚČET vyhral sumu 1 milión libier šterlingov (1 000 000,00 GBP) v prebiehajúcom promo ocenení online na Facebooku a Coronavirus (COVID-19) finančné prostriedky od generálneho riaditeľa Facebooku Inc. Zuckerberg. Vaše číslo lístka je 00545 188 564756. Všetci účastníci boli vybraní prostredníctvom počítačového randomizovaného systému vyžrebovaného z 27 miliónov e-mailových adries cez internet a Lucky Winners. TO ZNAMENÁ, ŽE TO NENÍ IBA FACEBOOK UŽÍVATEĽA, KTORÝ MÔŽE Z TEJTO LOTÉRIE ZÍSKAŤ, TOTO LOTÉRIA JE PRE KAŽDÉHO A AK DOSTANETE E-MAIL, ZNAMENÁ TO, ŽE STE JEDENM Z VÝHODNÝCH VÝHERCOV.

Pošlite ďalej svoje všetky podrobnosti, ako napríklad:
1. Celé meno .....
2. Krajina .....
3. Kontaktná adresa .....
4. Telefónne číslo .....
5. Rodinný stav .....
6. Povolanie .....
7. Spoločnosť .....
8. Vek .....

Podrobnosti prosím pošlite:
Kontaktná osoba: pán David M. Wehner, finančný riaditeľ európskeho regiónu UK
* Prostredníctvom e-mailu: facebook.claimunit@outlook.com

Váš e-mail vyhral náš jackpot, ešte raz blahoželáme.

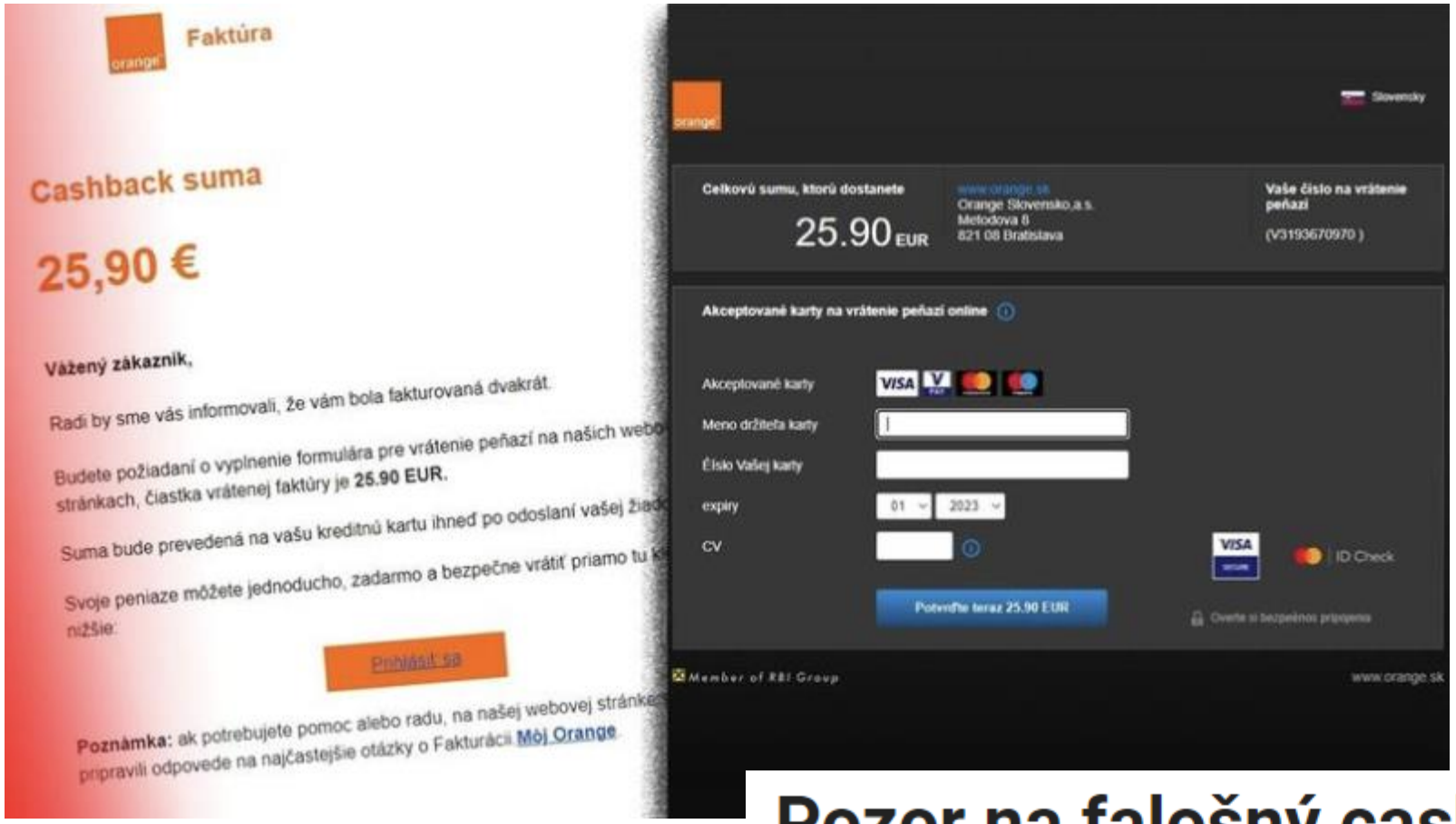
Váš v službe,
Pán Marc Andreessen
Facilitátor lotérie na Facebooku.

********** *******
Nepochybujte o tomto liste alebo ho ignorujte, pretože sme pripravení odovzdať vám vaše neuveriteľné ocenenie od Facebooku

Odpovedať | Odpovedať všetkým | Preposlať

Podvodné e-maily

AKTUÁLNE!



Pozor na falošný cashback od Orangeu. Podvodníci skúšajú nový zákerný trik

Zdroj: https://zive.aktuality.sk/clanok/2ET1GIU/pozor-na-falosny-cashback-od-orangeu-podvodnici-skusaju-novy-zakerny-trik/

Faktúra

Suma, ktorá sa má vrátiť

21,60 €

Fakturačné obdobie
16. 1. 2023 – 15. 2. 2023

Variabilný symbol: 0233316066

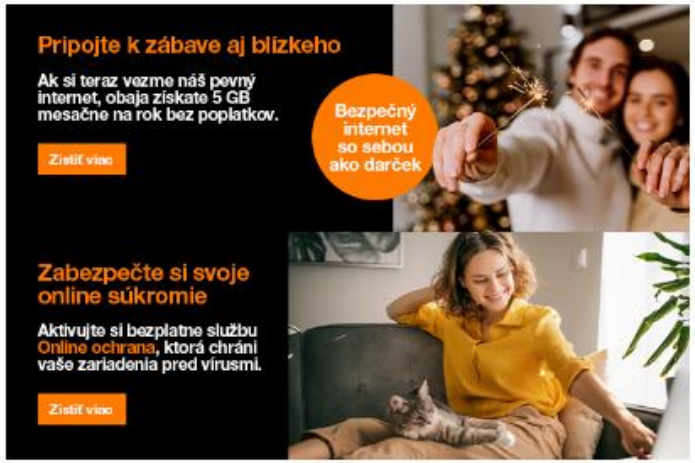
Uvedenie správneho variabilného symbolu je nevyhnutné pre korektné priradenie Vašej platby.

Vážený zákazník,
Chceme vás informovať, že vám bola fakturovaná dvakrát.
Budete požiadaní o vyplnenie formulára na vrátenie peňazí na našej webovej stránke.
Výška vrátenej faktúry je 21,60 €.
Suma bude prevedená na vašu kreditnú kartu do 24 hodín od odoslania vašej žiadosti.
Svoje peniaze môžete vrátiť jednoducho, rýchlo a bezpečne priamo tu kliknutím nižšie.

Prihlásiť sa

Prehľad faktúry

Mesačné poplatky	17,90 €
Zľavy	3,70 €
Celková suma na úhradu	**21,60 €**



Ak si neželáte dostávať spolu s faktúrou aj marketingové informácie, môžete sa po prihlásení a Vašej identifikácii odhlásiť z ich zasielania v Zákazníckej zóne na www.orange.sk v časti Nastavenie personalizovanej komunikácie. Rovnako sa na tomto mieste môžete opätovne na odber prihlásiť. Zmena bude účinná od nasledujúceho fakturačného obdobia.

Právna informácia / Legal notes

Odpovedať | Odp. všetkým | Preposlať | Zmazať | Nahlásiť spam | Ďalšie akcie

Predmet: **Elektronický doklad o vrátení peňazí**

Od: **Orange - faktura**

Komu: Martin Vavra

Dátum: 22.2. 2023 10:08

Orange

Faktúra

Suma, ktorá sa má vrátiť

21,60 €

Fakturačné obdobie
16. 1. 2023 – 15. 2. 2023

Variabilný symbol: 0233316066

Uvedenie správneho variabilného symbolu je nevyhnutné pre korektné priradenie Vašej platby.

Vážený zákazník,
Chceme vás informovať, že vám bola fakturovaná dvakrát.
Budete požiadaní o vyplnenie formulára na vrátenie peňazí na našej webovej stránke.
Výška vrátenej faktúry je 21,60 €.
Suma bude prevedená na vašu kreditnú kartu do 24 hodín od odoslania vašej žiadosti.
Svoje peniaze môžete vrátiť jednoducho, rýchlo a bezpečne priamo tu kliknutím nižšie.

Prihlásiť sa

Prehľad faktúry

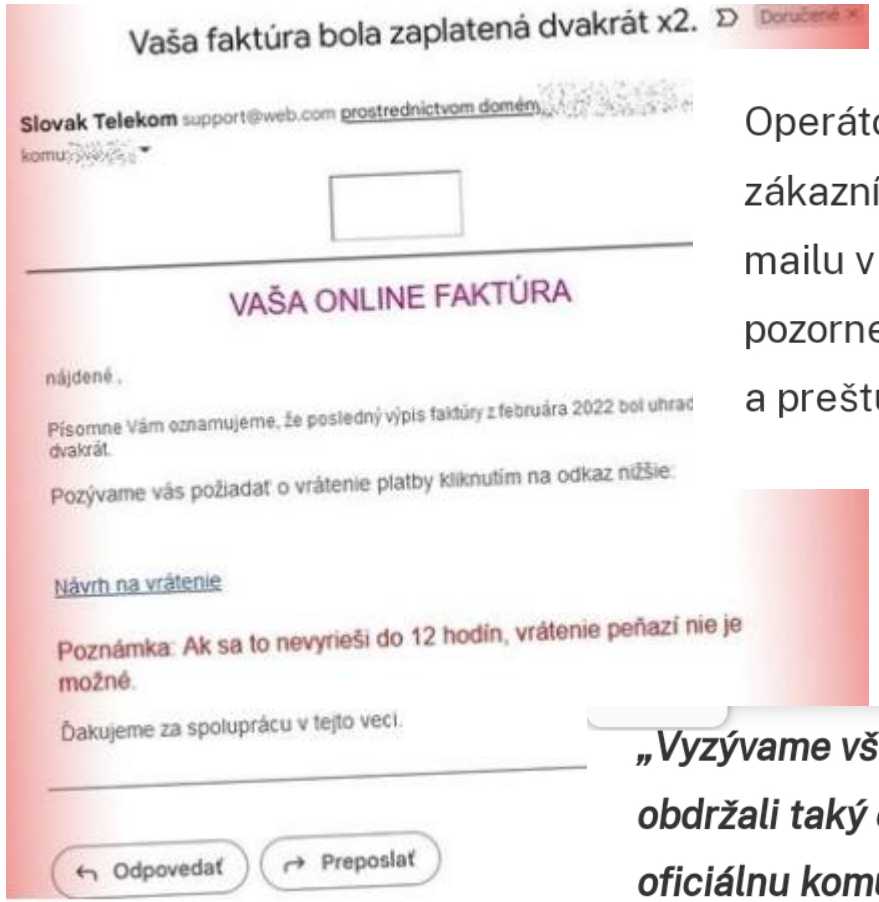
Mesačné poplatky	17,90 €
Zľavy	3,70 €
Celková suma na úhradu	**21,60 €**

Podvodné e-maily

Telekom

Podvodníci svoje obete informujú o dvojitom uhradení faktúry za február 2023. Následne ich vyzývajú ku kliknutiu na priložený link, cez ktorý vraj dostanú svoje peniaze naspäť. ***„Oslovený zákazník je vyzvaný, aby pre navrátenie duplicitnej sumy klikol na uvedený link, ktorý bol súčasťou emailu,“*** uvádza Telekom.

Pochopiteľne, ide o podvod. **Preto za žiadnych okolností na priložený link neklikajte**. Ak si nie ste istí, vždy môžete kontaktovať zákaznícku službu Telekomu, prípadne skontrolovať svoje bankové konto, či skutočne došlo k zaplateniu duplicitnej sumy.



Operátor oznam zakončuje výzvou, aby boli zákazníci v prípade obdržania takéhoto e-mailu v budúcnosti opatrnejší, resp. aby si pozorne prečítali obsah správy a preštudovali informácie od odosielateľa.

„Vyzývame všetkých našich zákazníkov, ktorí obdržali taký e-mail vydávajúci sa za oficiálnu komunikáciu naše firmy, aby neklikali na žiadny URL odkaz, ani nezadávali žiadne svoje osobné identifikačné údaje či údaje o platobnej karte,“ dodáva Telekom.

Zdroj: https://zive.aktuality.sk/clanok/5w50XJU/pozor-na-zlodejov-s-falosnymi-preplatkami-faktur-to-skusaju-aj-na-klientov-telekomu/

Podvodné e-maily banka!

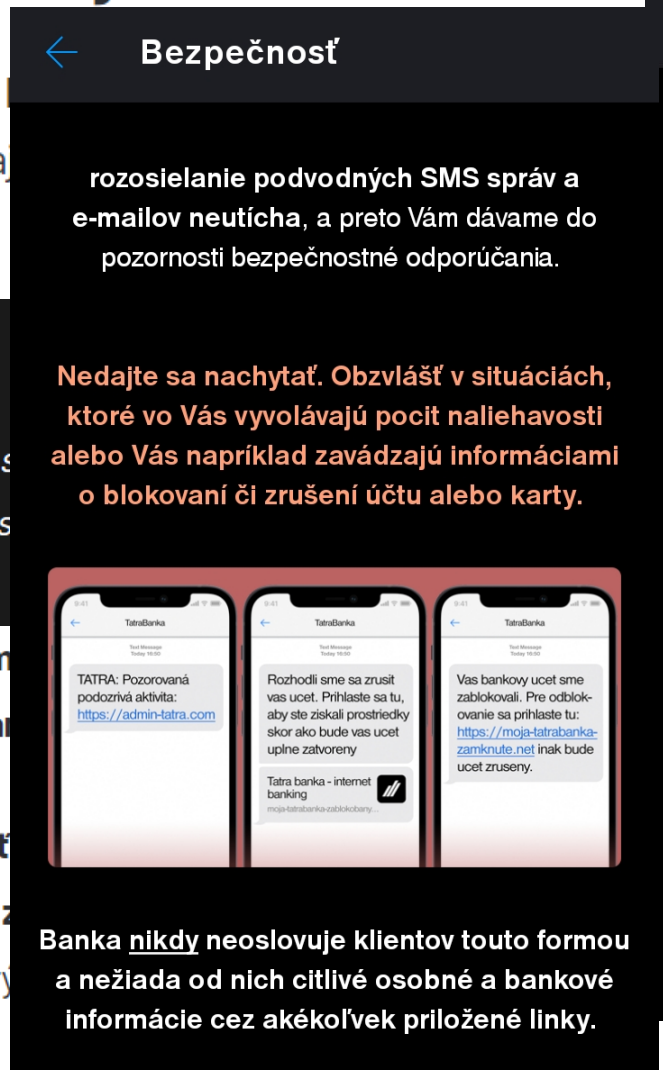
SLSP upozorňuje na množiace sa podvody

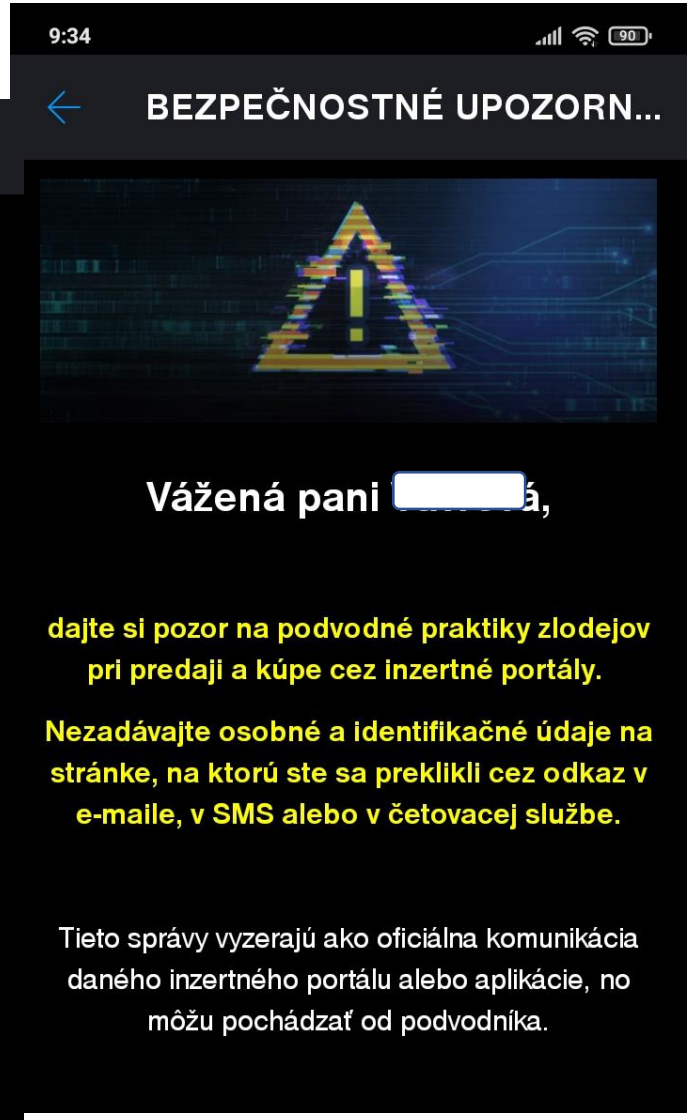
Slovenská sporiteľňa pár dní dozadu informovala, že sa množia
ich značku. Podvodníci sa snažia získať najmä prihlasovacie úda
banky, aby sa dostali k ich peniazom.

> *„Upozorňujeme vás na podvodné e-maily, textové s*
> *ktorými sa podvodníci snažia získať prístupové hes*
> *klientov.“, píše banka v oznámení.*

SLSP vysvetľuje, že **za týmto účelom útočníci posielajú podvodné e-m**
Rovnako upozorňuje aj na to, že sa **množia podvodné SMS správy a kla**

Tieto podvody majú jedného spoločného menovateľa, **snažia sa dostať**
od obete **požadujú vyplnenie prihlasovacích údajov alebo informácie**
používateľ tieto údaje vyplní, tak prakticky ich odovzdá útočníkovi, ktor
pozrieť, ako tieto podvody vyzerajú.





Zdroj: https://vosveteit.zoznam.sk/velka-banka-ukazala-ako-sa-podvodnici-snazia-okradnut-ich-klientov-prosime-vas-o-obozretnost-hlasi-banka/
https://www.tatrabanka.sk/predigitalnubezpecnost/

Podvodné e-maily/sms banka!

Od: Deutsche Kredit Bank <support@udriveaway.com> v mene používateľa info@slsp.sk <info@slsp.sk>
Odoslané: štvrtok 12. januára 2023 6:51
Komu: [redacted]
Predmet: Kontrola osobných údajov - 12/01/2023

Dobrý deň,

Interná administratívna kontrola odhalila, že jeden alebo viacero vašich kontaktných údajov nie je aktuálnych. Prejdite na george.slsp.sk a skontrolujte svoje údaje a v prípade potreby ich upravte. Pri kontrole sa musíte preukázať.

Ďakujeme, že využívate naše služby.

S pozdravom

Andrea [redacted]

Odporúčame Vám navštíviť www.george.sk, kde na jednom mieste nájdete zhrnutie, čo všetko si viete vybaviť cez Georgea, vrátane obľúbených funkcií a videonávodov.

Tel.: +421 25826 8111, 0850 111 888
Mail : info@slsp.sk
web: www.slsp.sk

Slovenská sporiteľňa

SLOVENSKÁ SPORITEĽŇA

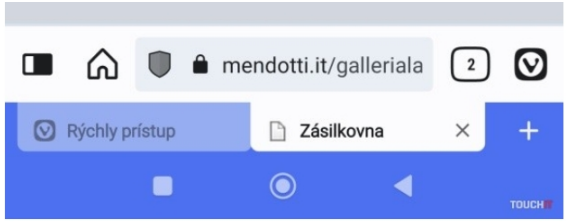
Zdroj: https://vosveteit.zoznam.sk/velka-banka-ukazala-ako-sa-podvodnici-snazia-okradnut-ich-klientov-prosime-vas-o-obozretnost-hlasi-banka/

Zásielkovňa

Zdroj: https://touchit.sk/

Podobnosť so skutočnými mailom je veľmi vysoká správa obsahuje sledovacie číslo ako aj českú lokalizáciu. Argument, že využívate slovenskú Zásielkovňu neobstojí, keďže čeština je nám geograficky a historicky veľmi blízka a tak správu budú mnohí považovať za legitímnu.

Vyskúšali sme tento podvod za vás a kliknutie na tlačidlo Naplánujte dodávku vás nasmeruje na falošnú stránku tejto spoločnosti. Už letmý pohľad na riadok s adresou napovie, že rozhodne nejde o českú doménu a už vôbec nie o stránku Zásielkovne hoci je v českej a viac ako desiatich lokalizácií.



Všimnite si úplne iný názov stránky a taliansku doménu

Nepodarilo sa nám prepnúť na slovenčinu, aby sme zistili koľko bude zásielka stáť v eurách. V českých korunách je to celkom 99 CZK. Jediné čo treba urobiť, je zadať údaje vašej platobnej karty aj s CVC kódom na zadnej strane.

Správa sama o sebe nepredstavuje vysoké bezpečnostné riziko, neblokuje ju ani prehliadač ako škodlivú. Riziko je v tom, že ide o bežný postup ako z vás vylákať údaje vašej kreditnej karty.

Odporúčame správu vymazať a nevenovať jej ďalšiu pozornosť.

Podvodné e-maily

dar = SCAM

SE **Stefanie Elizabeth <diyarbakir@cukobirlik.com.tr>**
Komu: Mária Vavrová

Ned 12. 2. 2023 6:39

A donation of $1 Million USD has be made to you for community development, if you are interested in expanding this CHARITY WORK kindly verify ownership of your email **(mariavavrova@gkmke.sk)**for further instructions on how to receive your donated money

BUILD THE WORLD A BETTER PLACE

==========

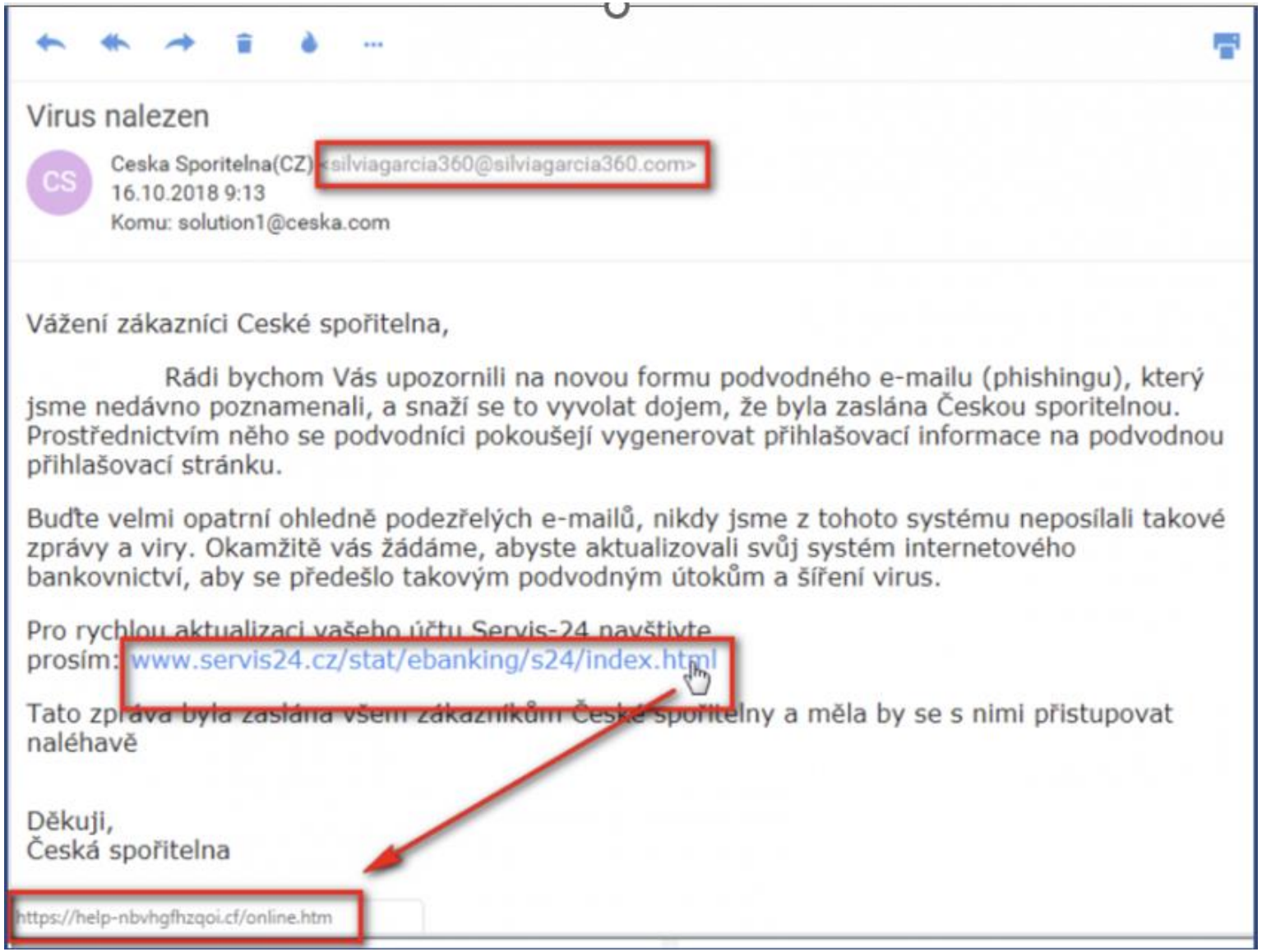
Bol vám poskytnutý dar vo výške 1 milión USD na rozvoj komunity, ak máte záujem o rozšírenie tejto CHARITNEJ PRÁCE, prosím overte vlastníctvo svojho e-mailu **(mariavavrova@gkmke.sk)**, aby ste získali ďalšie pokyny, ako získať vaše darované peniaze.

BUDOVAŤ SVET LEPŠÍM MIESTOM

https://www.youtube.com/watch?v=B1bM5aa4OqI

Zdroj: https://www.youtube.com/watch?v=B1bM5aa4OqI

Podvodné e-maily podozrivý link!

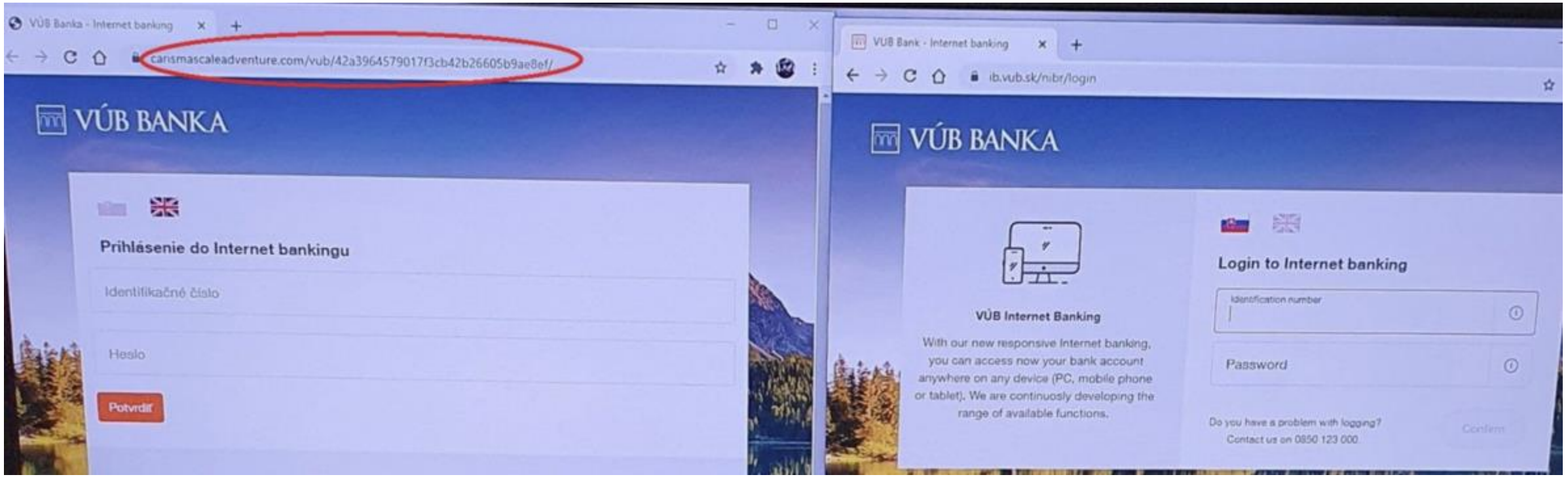


Zdroj: https://viry.cz/virus-nalezen-phishing-varuje-pred-phishingem/

Podvodné e-maily

podozrivý link!

- banka.sk banka.sl
- kia.sk kla.sk
- support.com suqqort.com



Zdroj: https://www.cas.sk/clanok/1071922/pozor-takto-mozete-prist-o-peniaze-policia-upozornuje-na-podvodnu-stranku-ktora-imituje-znamu-slovensku-banku/

Podvodné e-maily

naliehavosť

-------- Preposlaná správa --- Forwarded Message --------
Predmet: Bankový prevod bol prijatý.
Dátum: Fri, 29 May 2020 04:28:07 -0400
Od: Slovenská sporiteľňa <info@georgeslsp.com>
Pre: [redacted]@[redacted].sk

Vážený zákazník,

Dostali sme váš bankový prevod. Pred prevodom na váš bankový účet sa však chceme uistiť, že ste vlastníkom účtu.

Musíte urobiť tieto nevyhnutné postupy:

- Prihláste sa na svoj bankový účet pomocou tohto odkazu.

Na overenie vlastníctva účtu použijeme falošný bankový prevod (táto suma nebud
účtu. Chceme sa iba uistiť, že ste vlastníkom bankového účtu).

- Prijmite bankový prevod

S pozdravom.

'Účet pozastavený, 8 správ zablokovaných !
Od IT- Podpora Dátum Dnes 08:56

Kvôli veľkému počtu nevyžiadaných **E-mailov** sa vyžaduje opätovné overenie účtu **kliknutím sem** v priebehu nasledujúcich 12 hodín, aby ste zabránili trvalému zablokovaniu **účtu**.

Pozn .: Toto je posledné upozornenie !

© IT- Podpora.
CX110T287VCL

Zdroj: https://webex.digital/7-typov-podvodnych-e-mailov-vyzeraju-coraz-doveryhodnejsie--a18-81

Podvodné e-maily

podozrivé súbory!

GT

"Google Community Team <tinabature1@gmail.com>

Komu: me <emailaddress@domain.com>

Pon 27. 2. 2023 7:59

OFFICIAL NOTIFICATION LET...

Google

Hello Google Beneficiary,

The enclosed e-mail contains your Official Notification Letter and Claims Instructions as one of the main beneficiaries-(primary recipient) of the Google Grants/E-mail Electronic Online Reward for individuals and organizations.

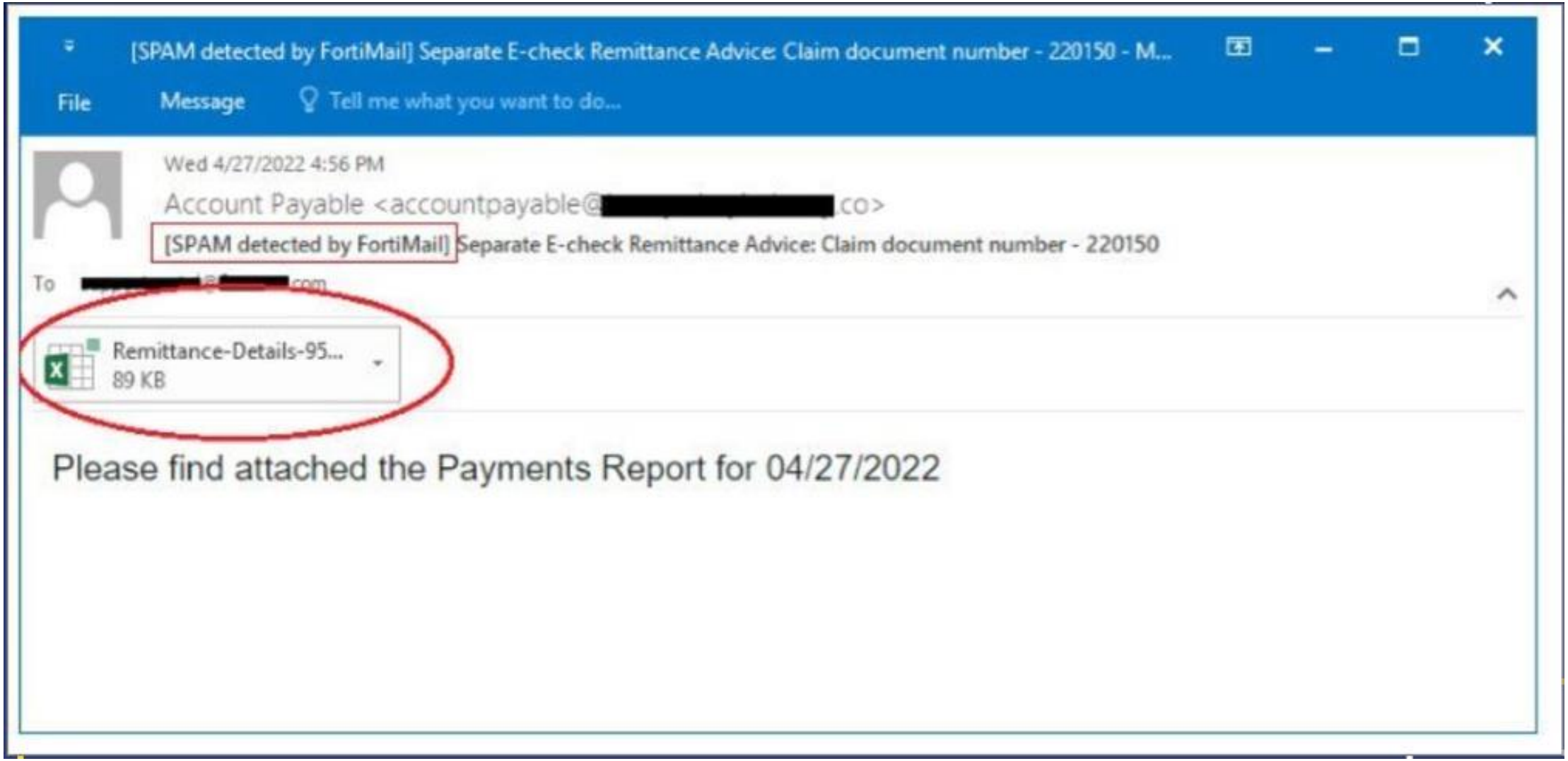
Thank You for Using Google Products/Services.

Sincerely,
The Google.com Team.

Odpovedať Preposlať

Podvodné e-maily

podozrivé súbory!



Zdroj: https://vosveteit.zoznam.sk/pozor-gmailom-outlookom-ale-aj-dalsimi-e-mailovy-sluzbami-sa-siri-podvodna-kampan-na-toto-neklikajte/

Podvodné e-maily  znaky:

- nevhodné alebo všeobecné oslovenie
- útočník vystupuje ako dôveryhodná inštitúcia (pošta, banka)
- naliehavosť
- veľká výhra alebo dedičstvo
- podozrivý odosielateľ
- zlá gramatika
- žiadosť o osobné informácie
- podozrivý link alebo súbor

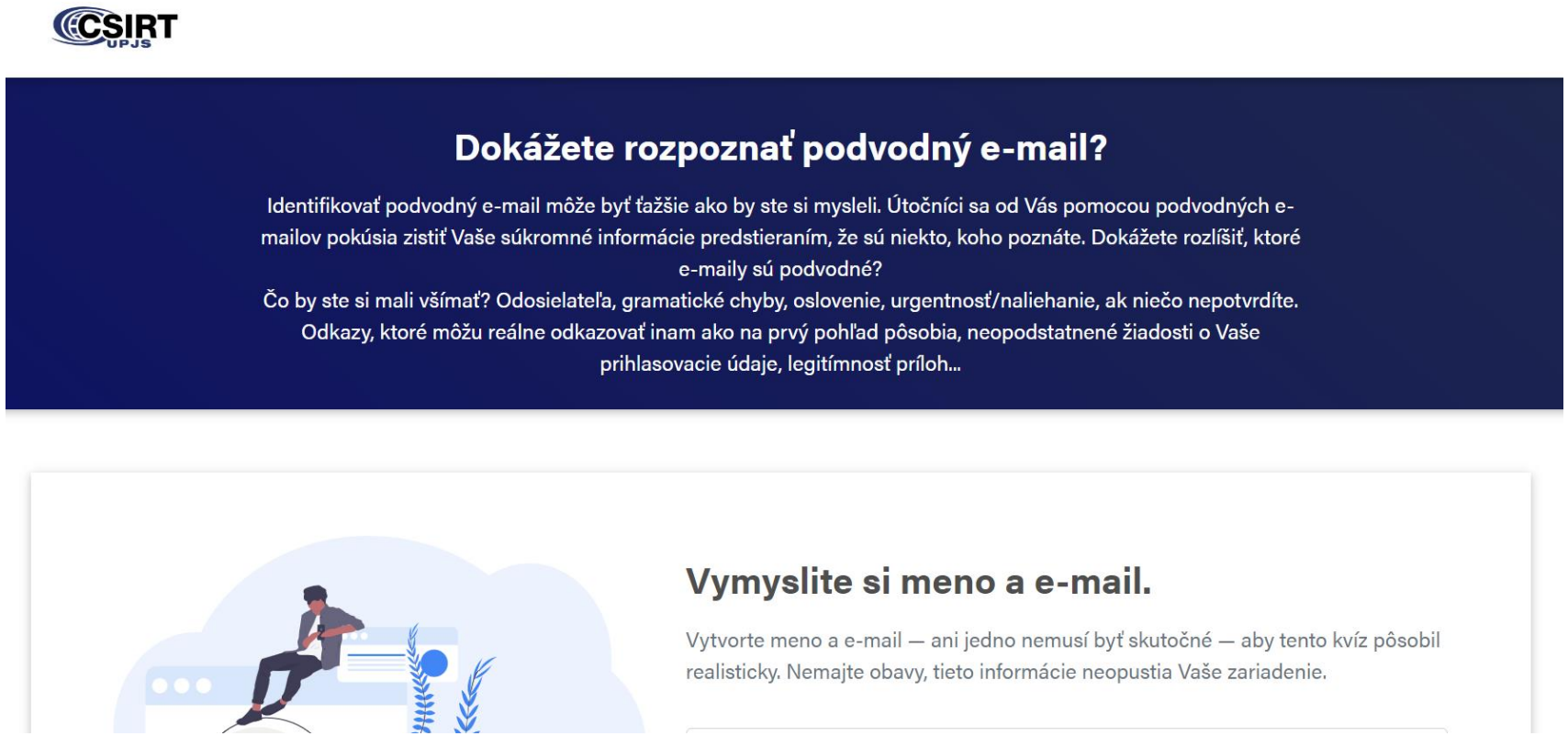
Phishing - Vishing - Scam

Celé video: https://www.youtube.com/watch?v=eIkPYH6aBF8

Zdroj: https://www.youtube.com/watch?v=eIkPYH6aBF8

Phishingový test

Otestujte sa: https://csirt.upjs.sk/phishing/

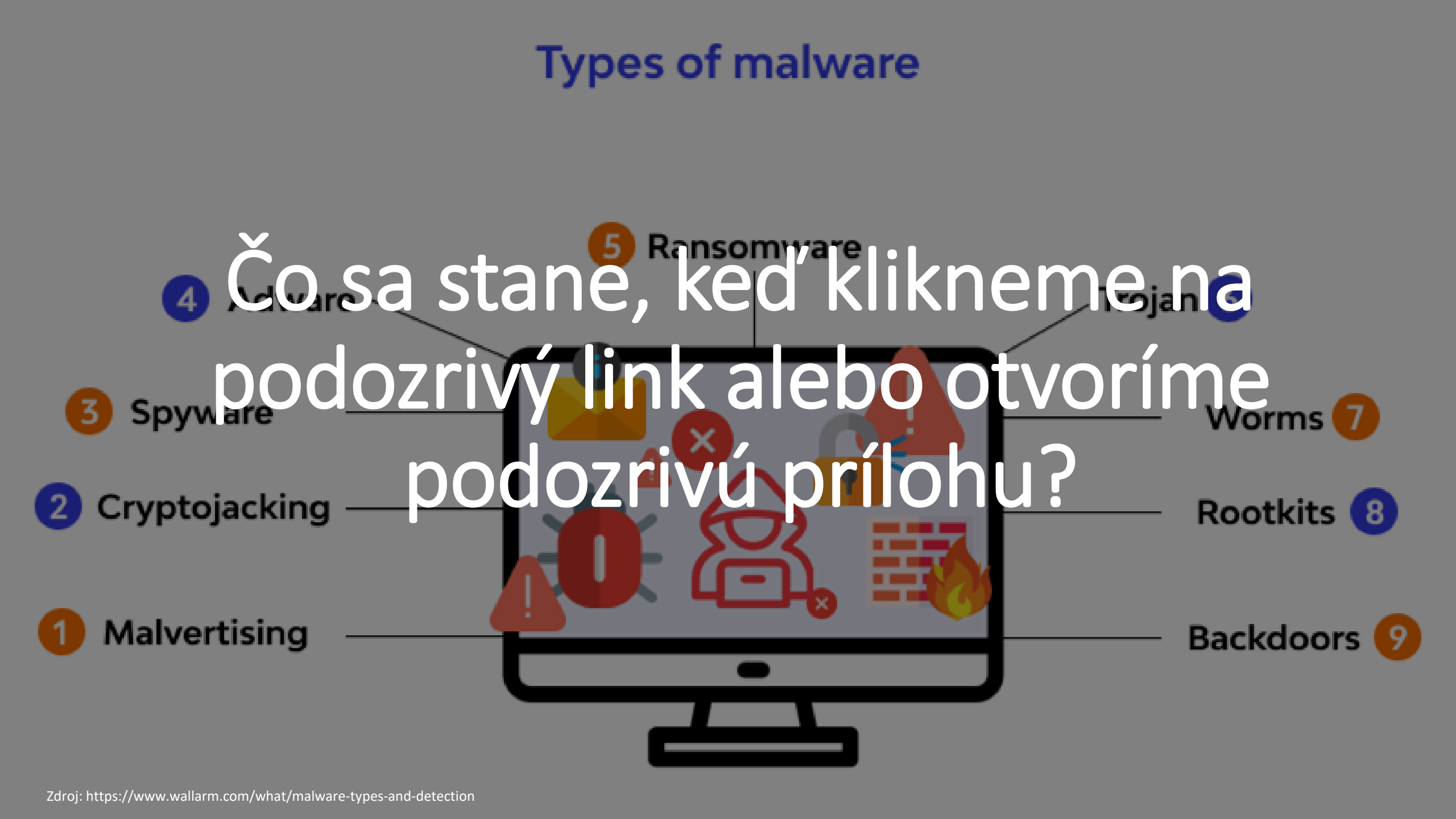


Zdroj: https://csirt.upjs.sk/phishing/

Otestujte sa

- Kvíz SLSP: https://www.slsp.sk/sk/ludia/bezpecnost

https://www.slsp.sk/sk/ludia/bezpecnost#/modalComponent/isOpen/true/url/%2Fsk%2Fconfiguration%2Fleads%2Fbezpecnost-test%2Fotazka1.modal



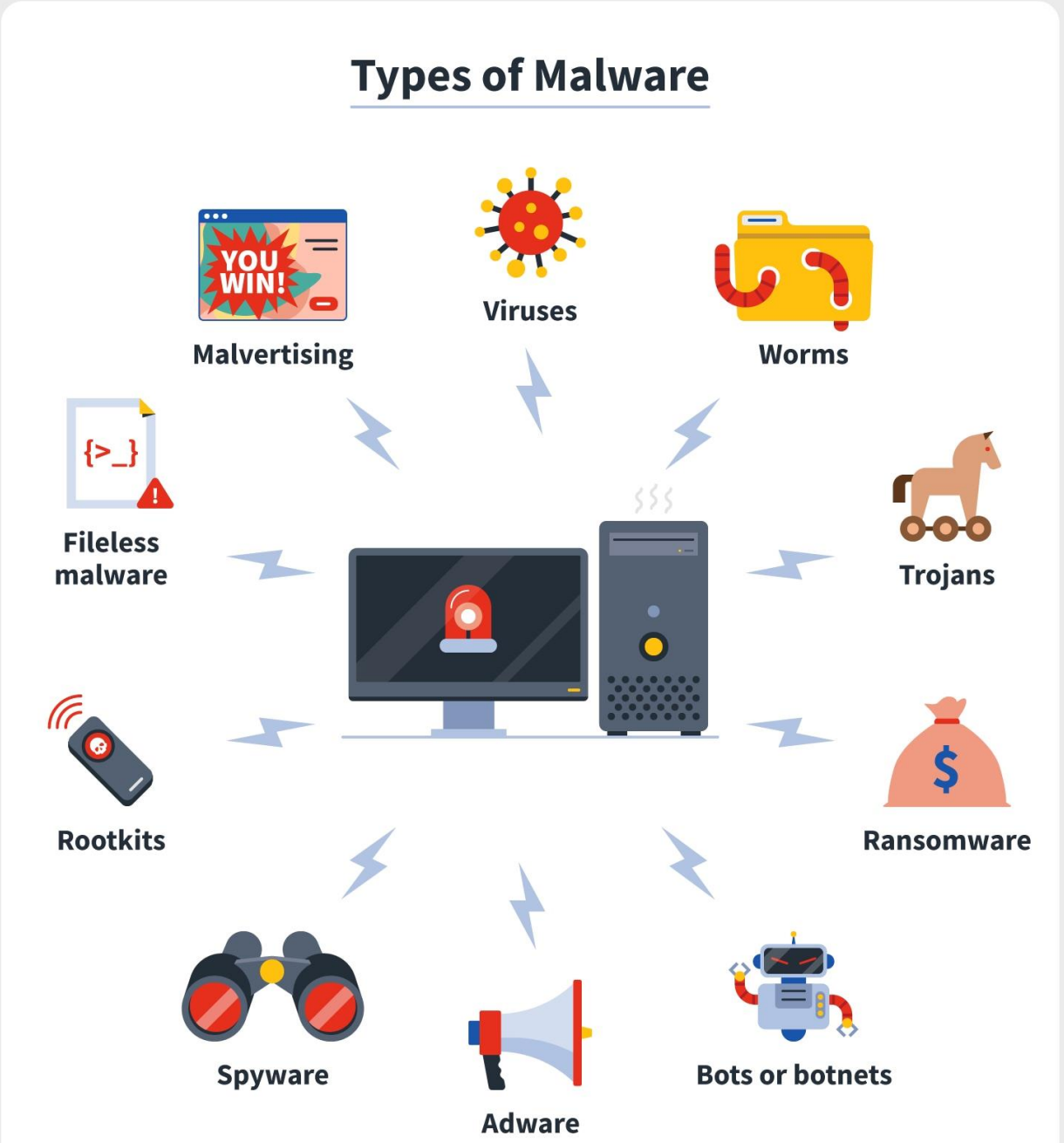
Čo sa stane, keď klikneme na podozrivý link alebo otvoríme podozrivú prílohu?

Zdroj: https://www.wallarm.com/what/malware-types-and-detection

Malvér

- malicious + software = **škodlivý softvér**
- sú to všetky formy **škodlivého kódu**, bez ohľadu na spôsob, akým postihujú obete, ako sa správajú a aké škody spôsobujú.

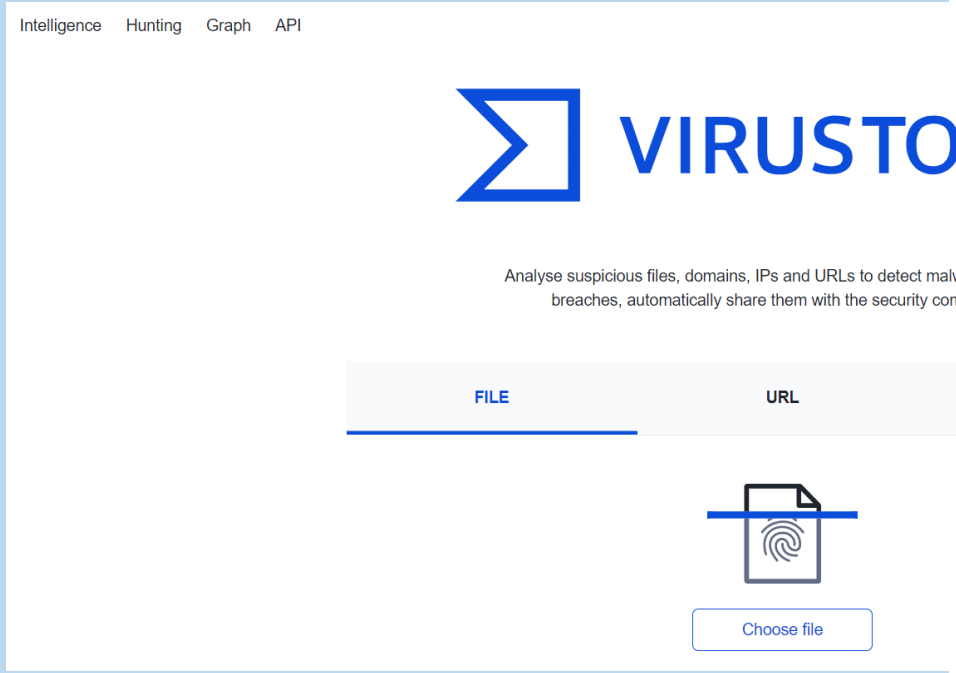
Zdroj: https://www.eset.com/sk/malver/

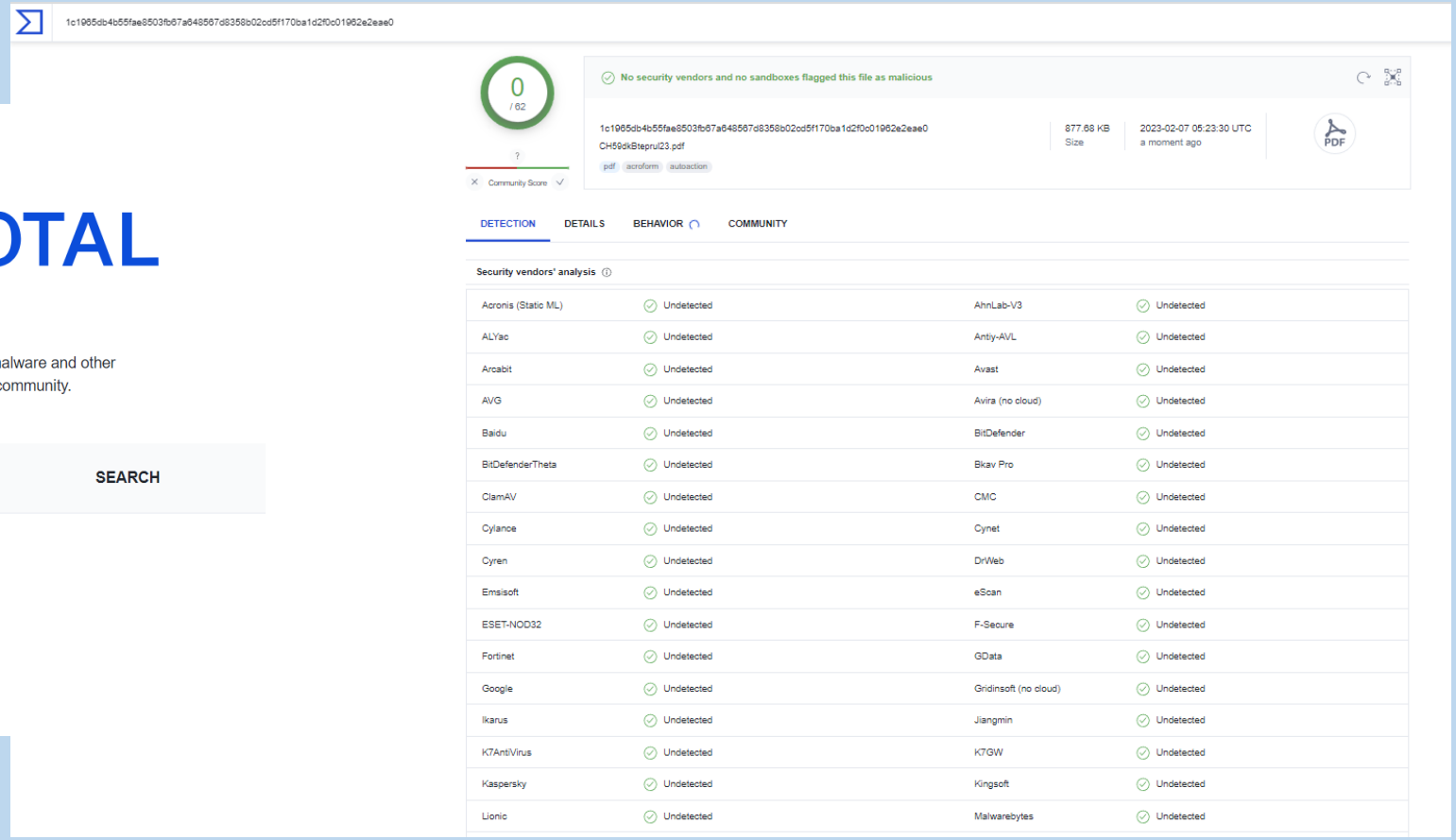


Zdroj: https://us.norton.com/blog/malware/types-of-malware

Zdroj: https://www.webnoviny.sk/europoslanci-vyzyvaju-na-opatrnost-pri-regulacii-digitalneho-sektora/

Otestujte súbor alebo odkaz



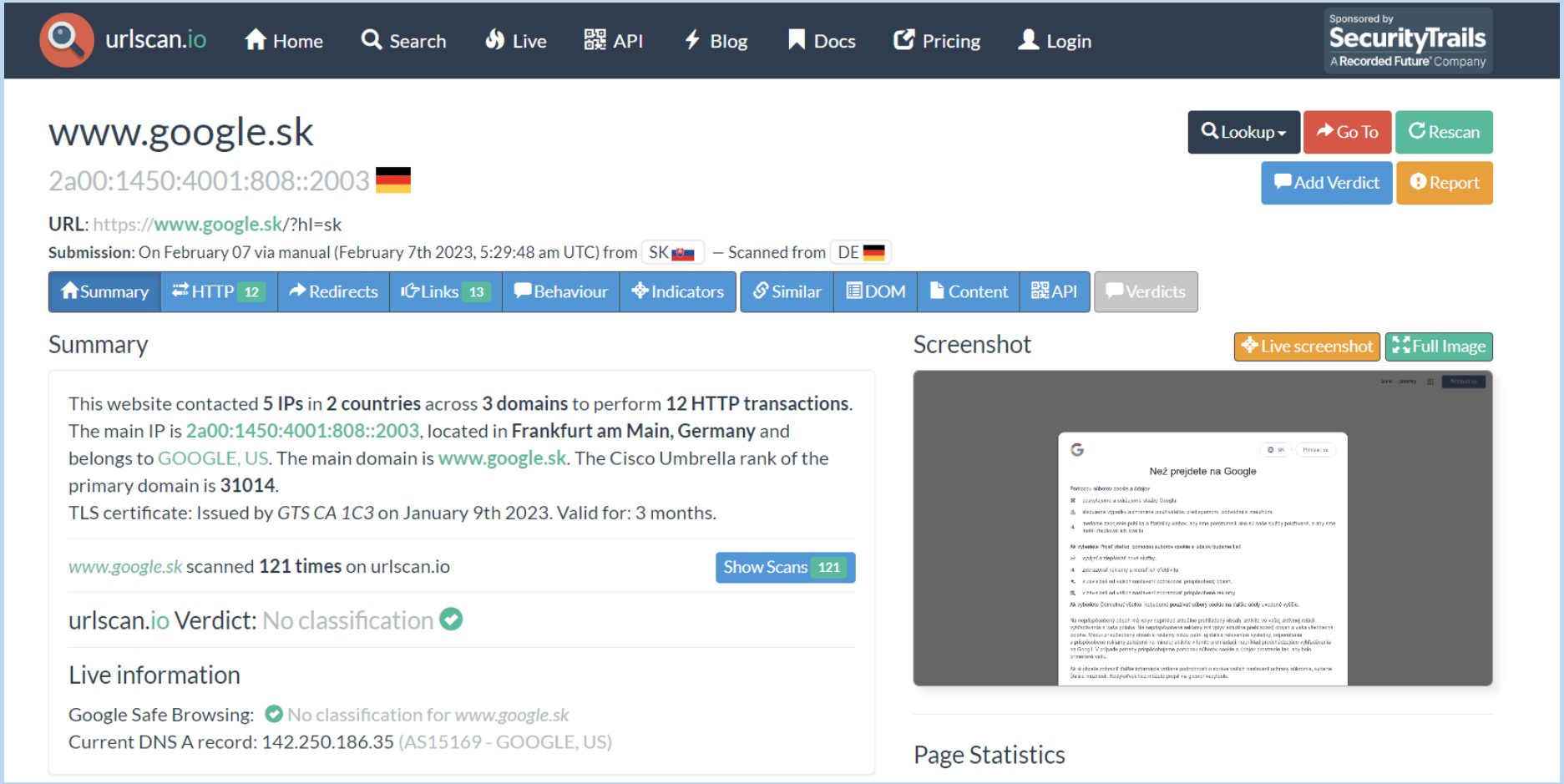


Otestujte súbor alebo URL adresu:

https://www.virustotal.com/gui/home/upload

Zdroj: https://www.virustotal.com/gui/home/url

Otestujte odkaz



Otestujte URL adresu: https://urlscan.io/

Zdroj: https://urlscan.io/

AKO SA CHRÁNIŤ

- **Informujte sa o nových phishingových technikách**: sledujte v médiách správy o phishingových útokoch, keďže útočníci vždy môžu prísť s novými technikami

- **Buďte obozretní pri poskytovaní osobných údajov:** overte si obsah správy priamo u odosielateľa alebo organizácie, ktorú navonok zastupuje (použite však zaručene správne kontaktné údaje, teda nie tie uvedené v správe)

- **Kliknutie si dvakrát premyslite**: neklikajte na odkazy a nesťahujte prílohy v podozrivých správach
- **Pravidelne kontrolujte svoje online účty**: aj keď nemáte podozrenie, že sa niekto pokúša ukradnúť vaše prístupové údaje, skontrolujte si svoj bankový účet a ostatné online účty, aby ste sa presvedčili, že v nich nedošlo k žiadnej podozrivej aktivite

Útočník:

- vyvoláva pocit paniky,
- zneužíva emócie,
- zneužíva ľudskú zraniteľnosť,
- používa rôzne formy sociálneho inžinierstva.

Pravidlá ochrany:

- ✓ Majte aktuálne verzie softvérov!
- ✓ Nenaleťte na super ponuky!
- ✓ Nakupujte u overených obchodníkov!

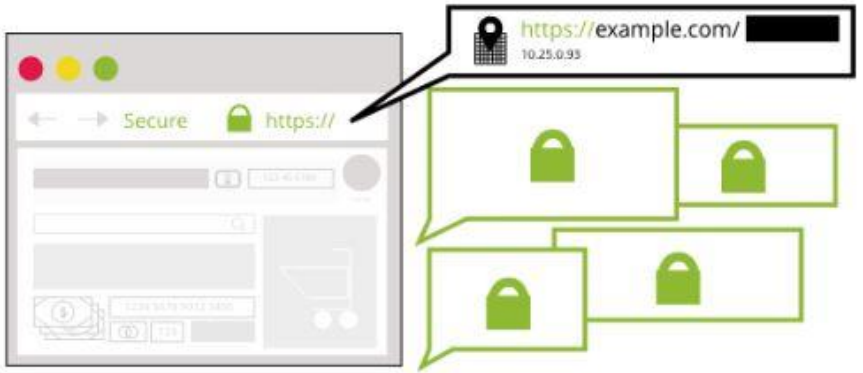
HTTP vs HTTPS

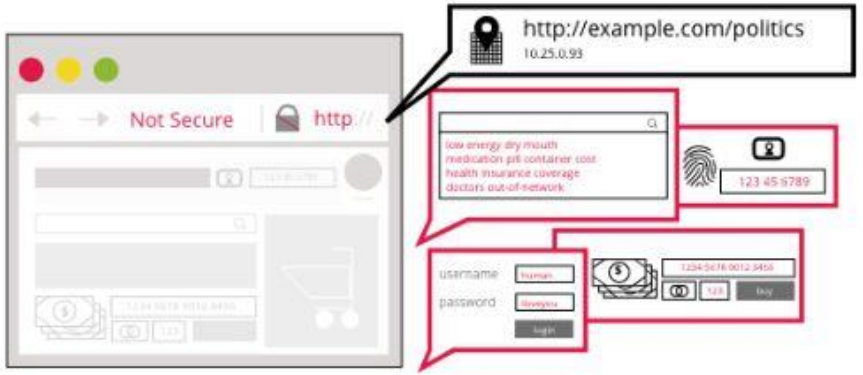
Webové stránky

Zdroj: https://www.datarain.com.br/blog/tecnologia-e-inovacao/qual-a-diferenca-entre-http-e-https/

https://Everywhere

http://





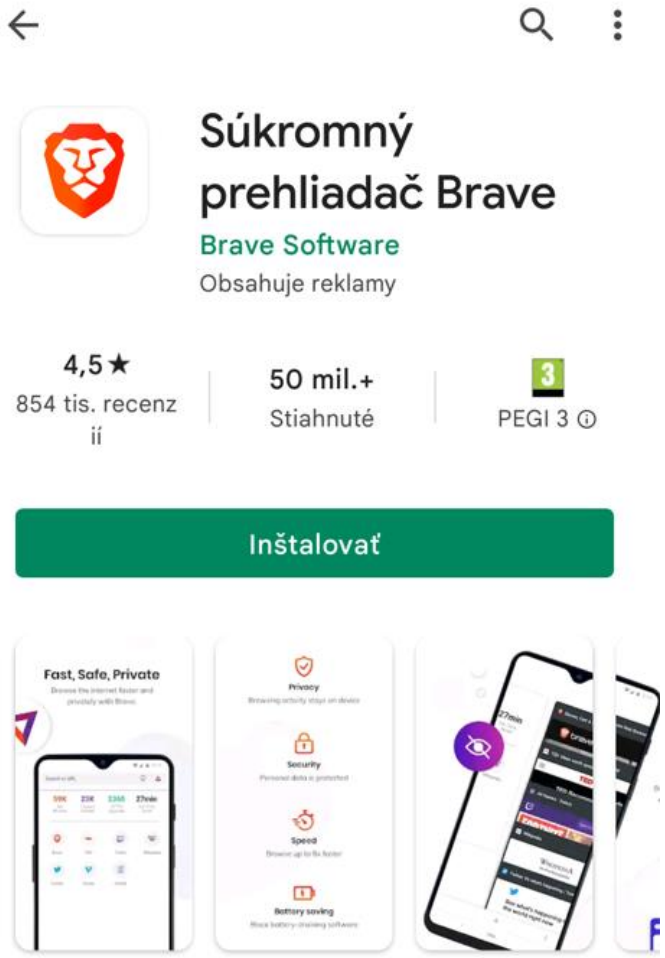
Zdroj: https://www.eff.org/https-everywhere
https://www.patriotgroup.eu/de/blog/article13

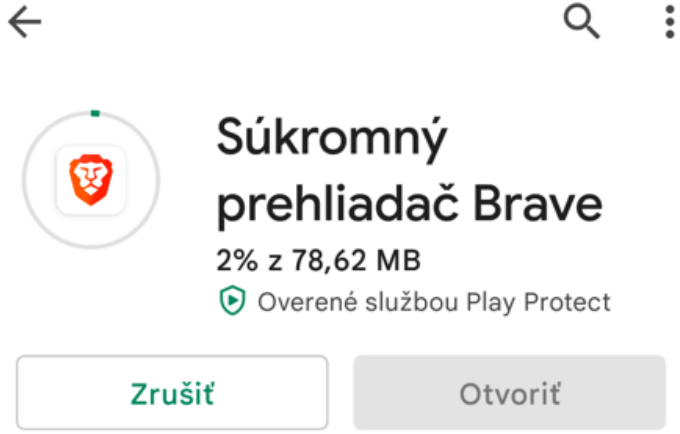
Blokovanie reklám v prehliadači

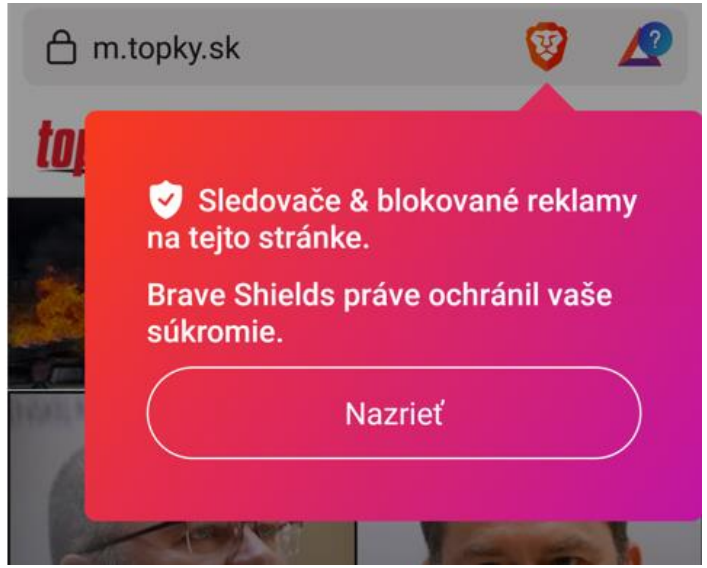
- efektívny blokovač
- nezaťažuje CPU ani pamäť
- dokáže načítať a vynútiť o niekoľko tisíc filtrov viac ako iné populárne blokovače

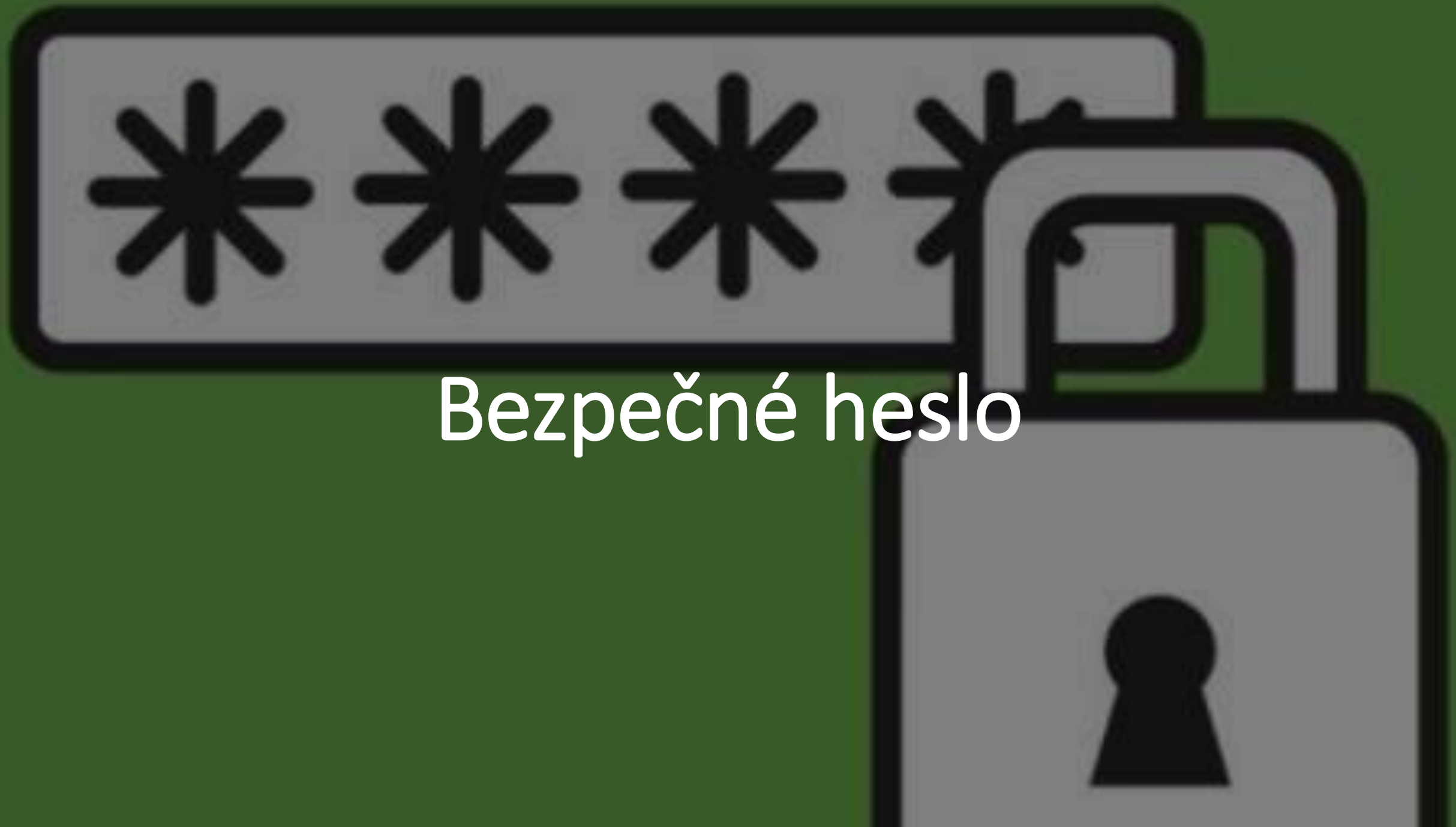
Zdroj: https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm

Prehliadač BRAVE – blokuje reklamy





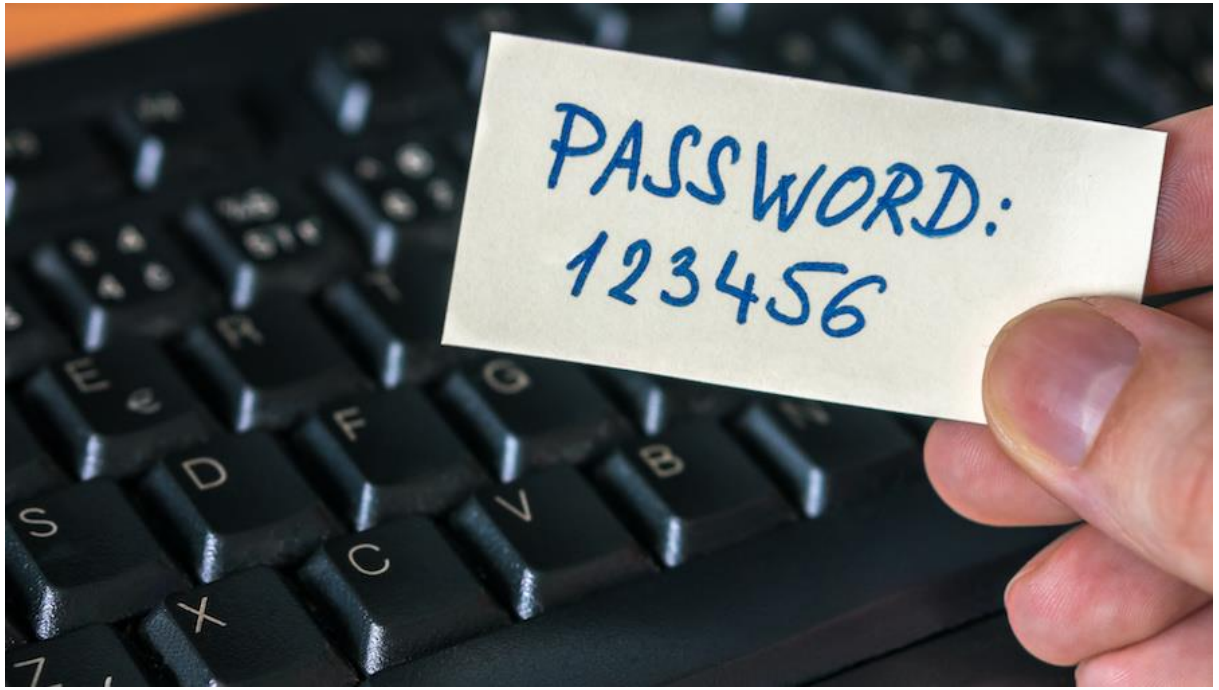


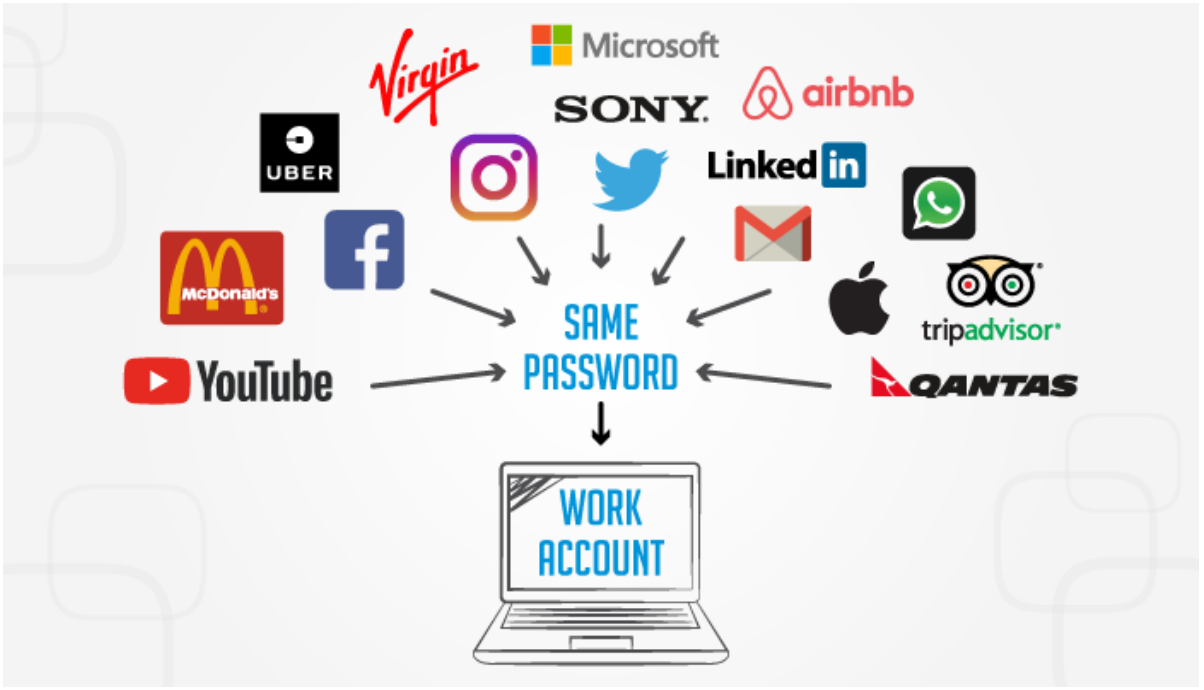


Bezpečné heslo

Heslo – časté chyby

- slabé heslá
- rovnaké heslá na viacerých účtoch

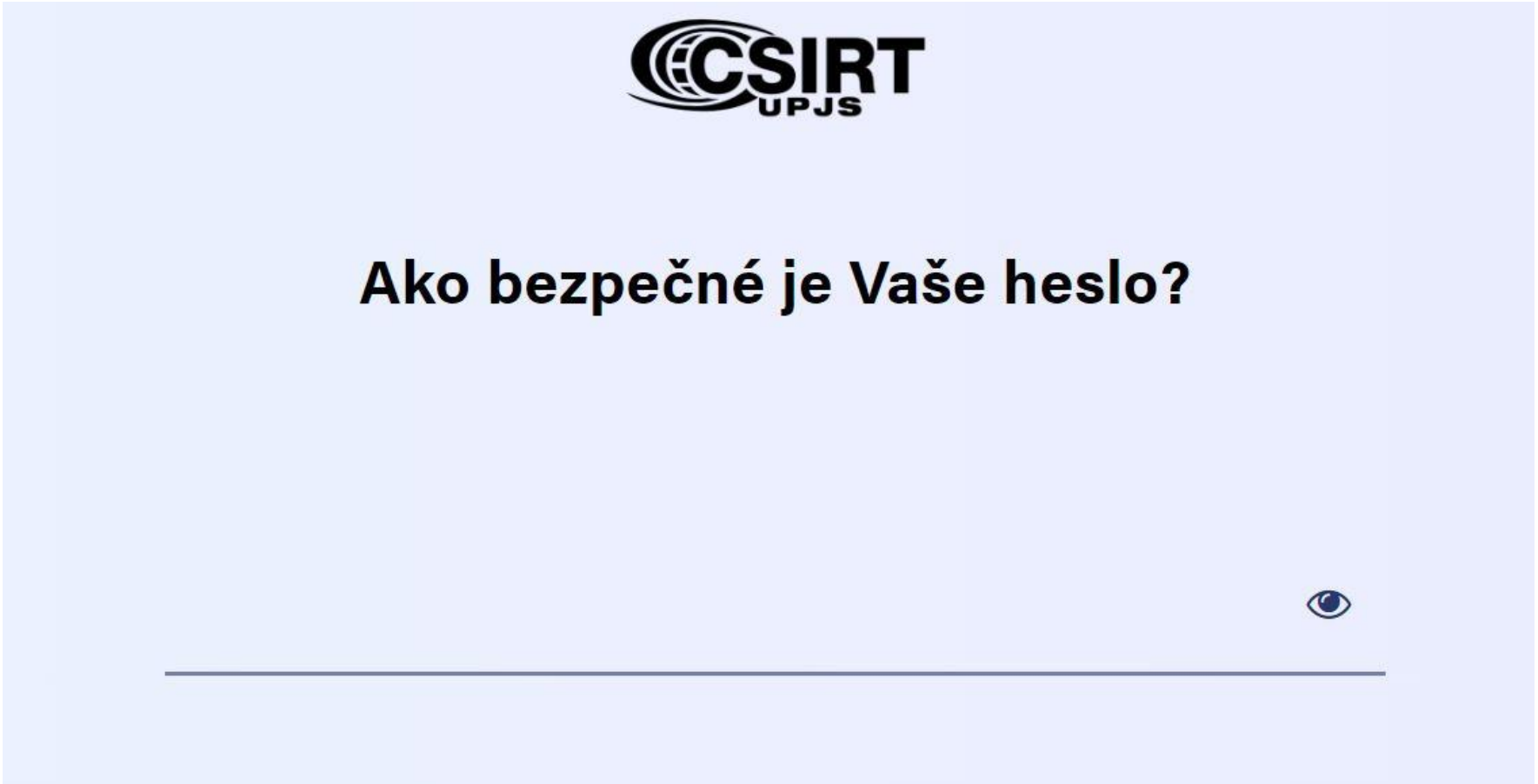




Zdroj: https://www.securedatamgt.com/blog/passwords-all-employees-should-avoid/ ; https://computerone.com.au/reusing-old-passwords-spells-future-trouble/

Bezpečné heslo

Tester hesiel: https://hesla.csirt.upjs.sk/



Zdroj: https://hesla.csirt.upjs.sk/

Otestujte silu hesiel:

- **0000**
- **Heslo**
- **Dunčo**
- **1234**
- **mamRADcokoladu+čipsy**
- **0808200417**
- **kybertímGKMKE**
- **N1dT1trouS1Bl2sk1!**

Bezpečné heslo

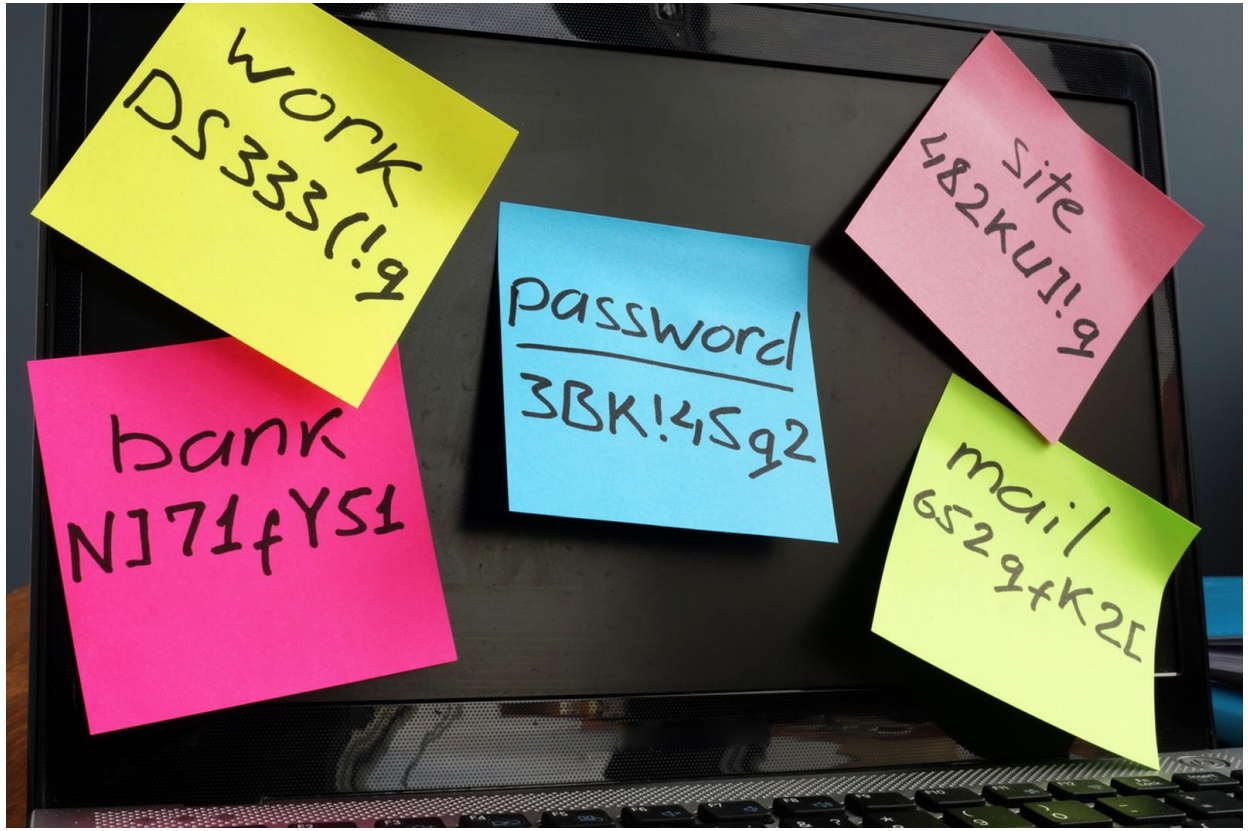
- viac ako 12 znakov
- Veľké aj malé písmená
- čísla
- špeciálne znaky *</_?:!#

✓ čím je heslo náhodnejšie, tým je bezpečnejšie !

✓ neobsahuje osobné údaje !

✓ na každý účet používame iné heslo !

Správa hesiel



Zdroj: https://www.iplocation.net/

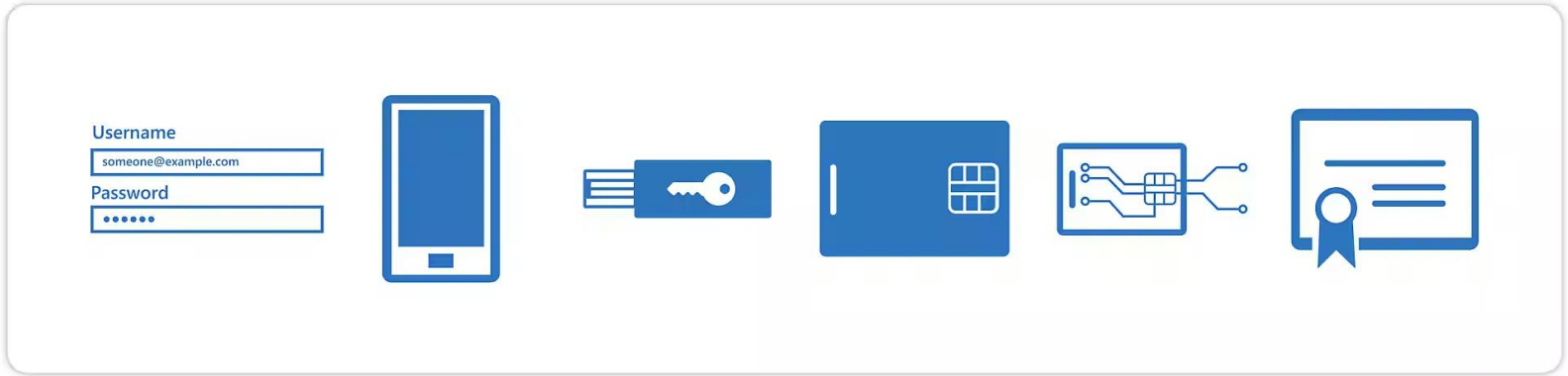
Multifaktorová autentifikácia

- viacfaktorové overovanie pridáva k prihlasovaciemu procesu ďalšiu vrstvu ochrany,
- pri získavaní prístupu ku kontám alebo aplikáciám používatelia

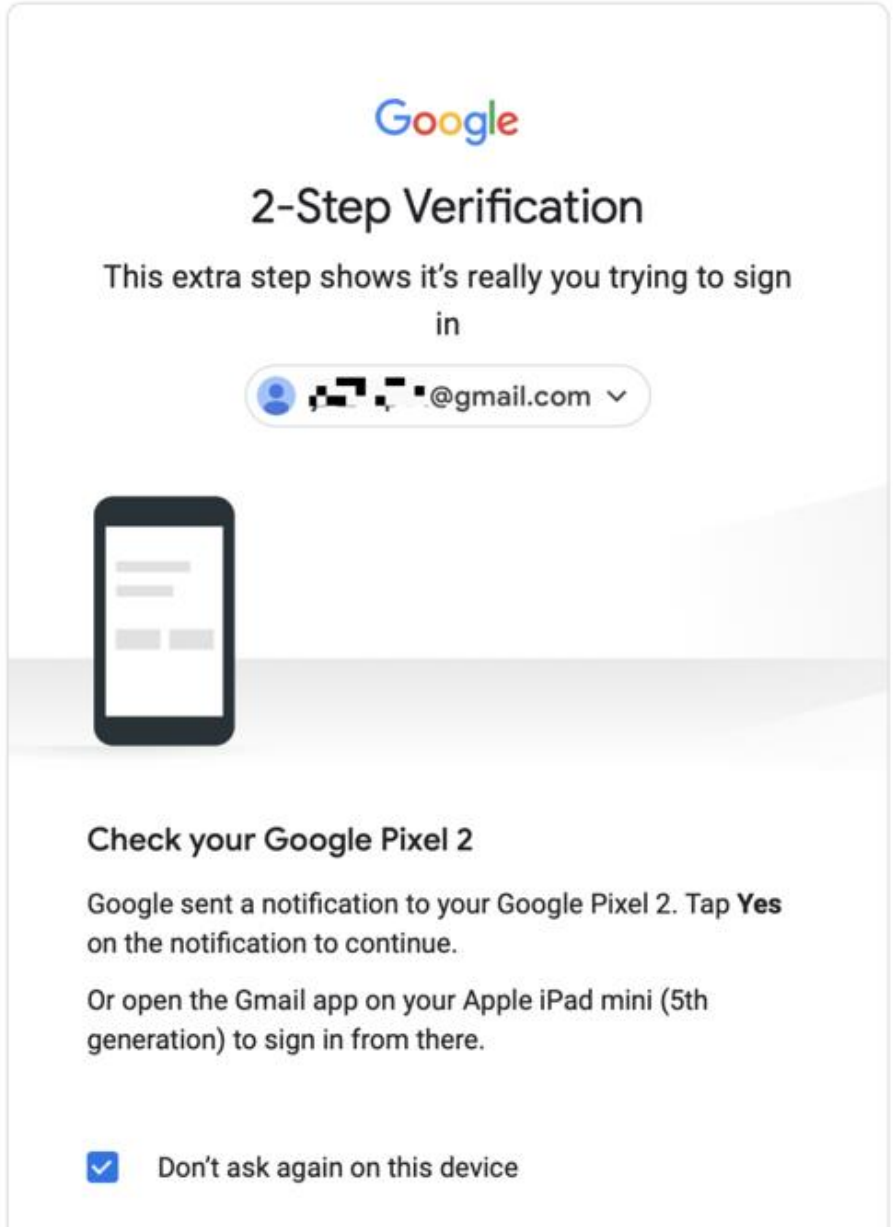
využívajú ďalšie overenie identity:

skenovanie odtlačku prsta

zadávanie kódu prijatého cez telefón.



Zdroj: https://www.microsoft.com/sk-sk/security/business/identity-access/azure-active-directory-mfa-multi-factor-authentication

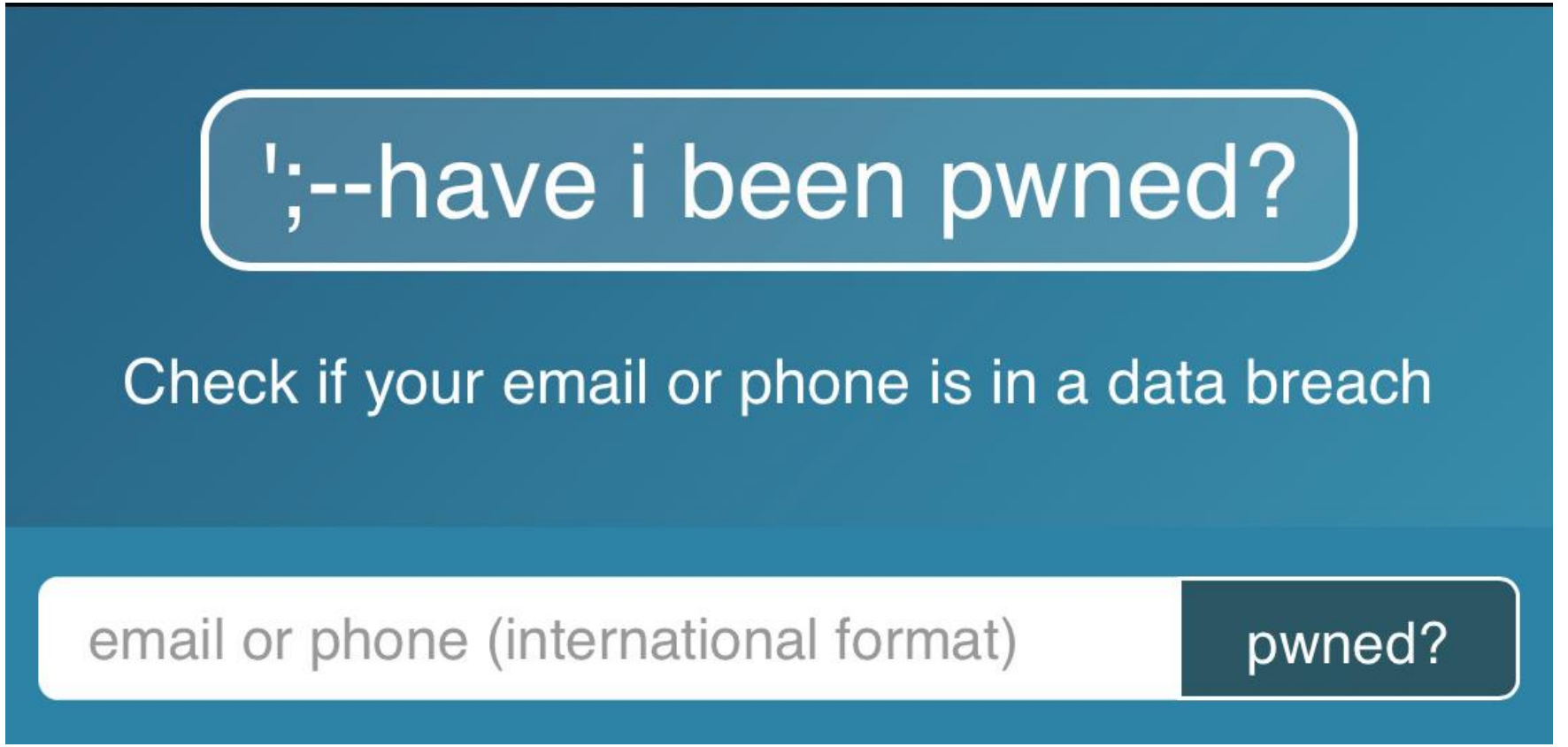


Zdroj: https://zapier.com/blog/google-two-step-verification/, https://www.groovypost.com/unplugged/two-factor-authentication-guide-secure-online-accounts/

Úniky údajov

Zdroj: https://ochrana-online.sk/ohlasovanie-porusenia-ochrany-osobnych-udajov/

Úniky údajov



https://haveibeenpwned.com/

Zdroj: https://haveibeenpwned.com/

Bezpečnosť mobilu

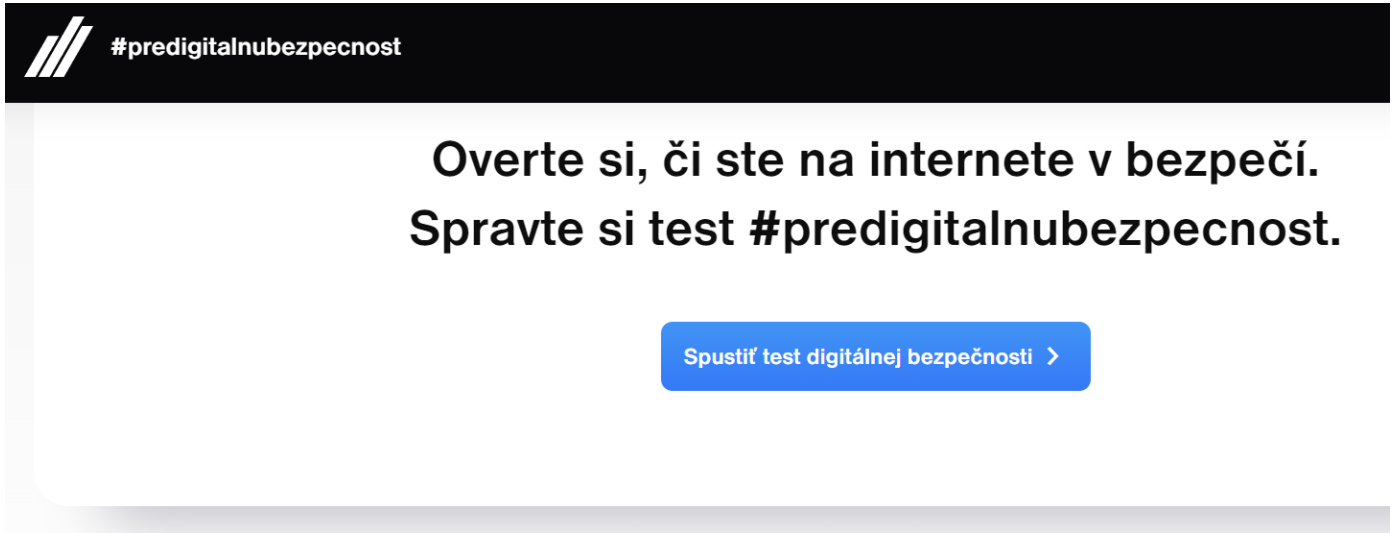
Zdroj: https://ochrana-online.sk/ohlasovanie-porusenia-ochrany-osobnych-udajov/

Bezpečnosť webového prehliadača

Zdroj: https://ochrana-online.sk/ohlasovanie-porusenia-ochrany-osobnych-udajov/

Test digitálnej bezpečnosti

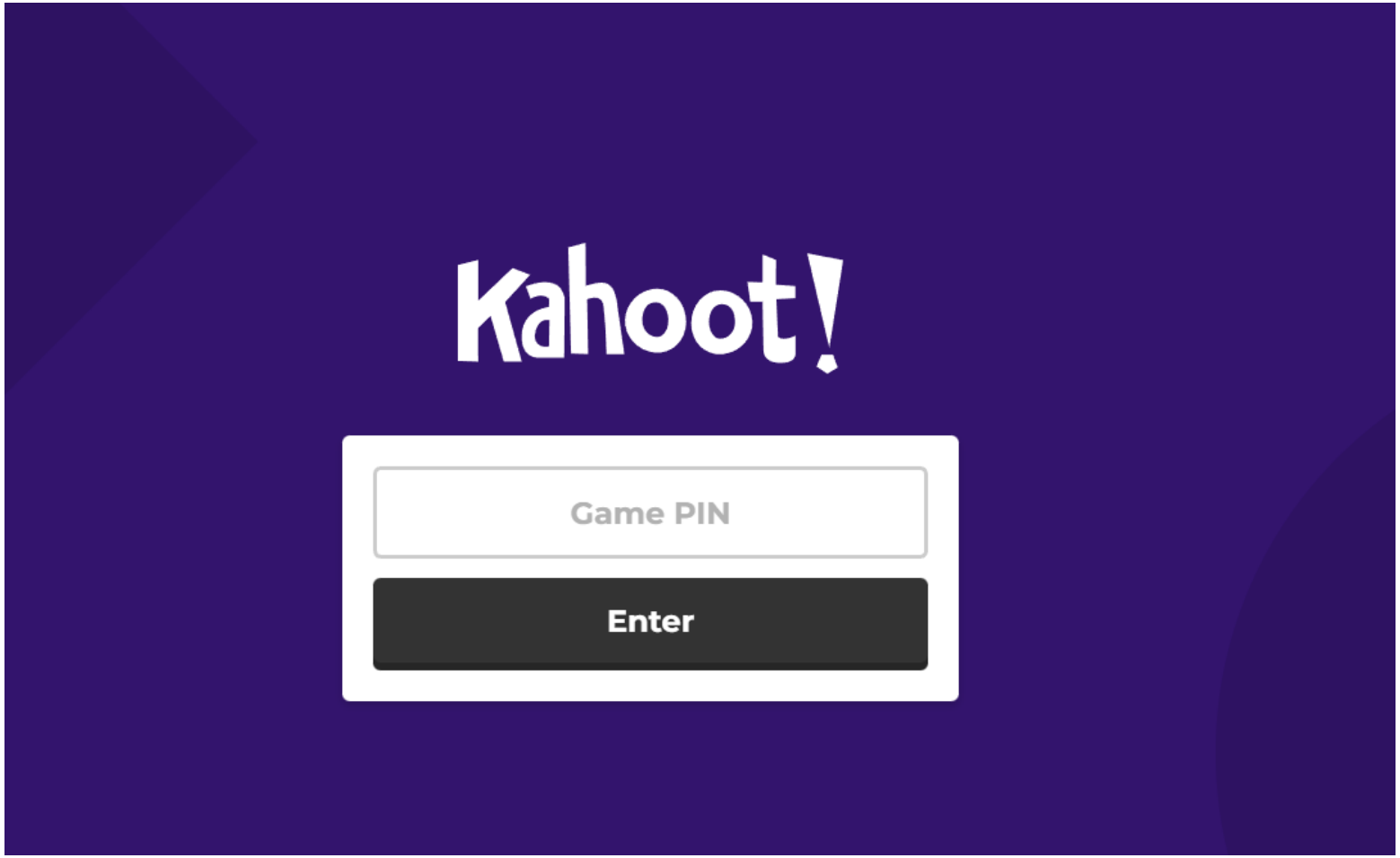
https://www.tatrabanka.sk/predigitalnubezpecnost/test-digitalnej-bezpecnosti/?utm_source=SilverpopMailing&utm_medium=email&utm_campaign=16687255&utm_content=spustit_test&mktid=874F4C0D08322FF2867D8C9FAA1D5FF0



Zdroj: https://www.tatrabanka.sk/predigitalnubezpecnost/test-digitalnej-bezpecnosti/?utm_source=SilverpopMailing&utm_medium=email&utm_campaign=16687255&utm_content=spustit_test&mktid=874F4C0D08322FF2867D8C9FAA1D5FF0

Kvíz

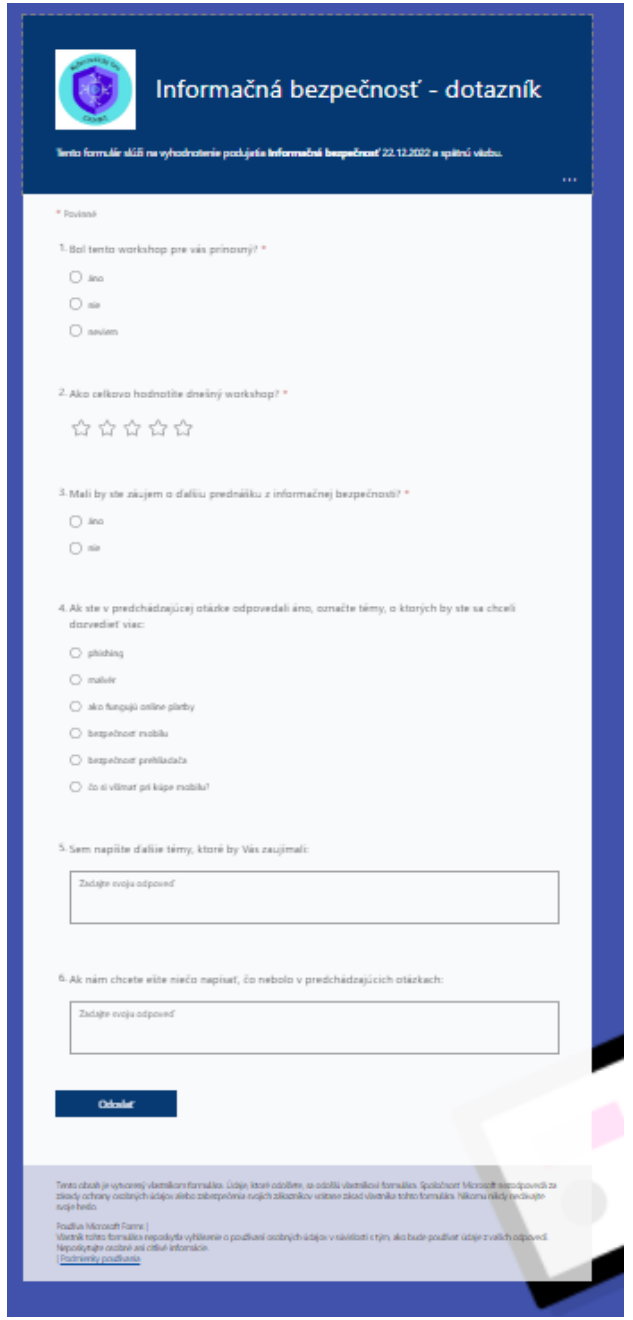
https://kahoot.it/



Zdroj: https://kahoot.it/

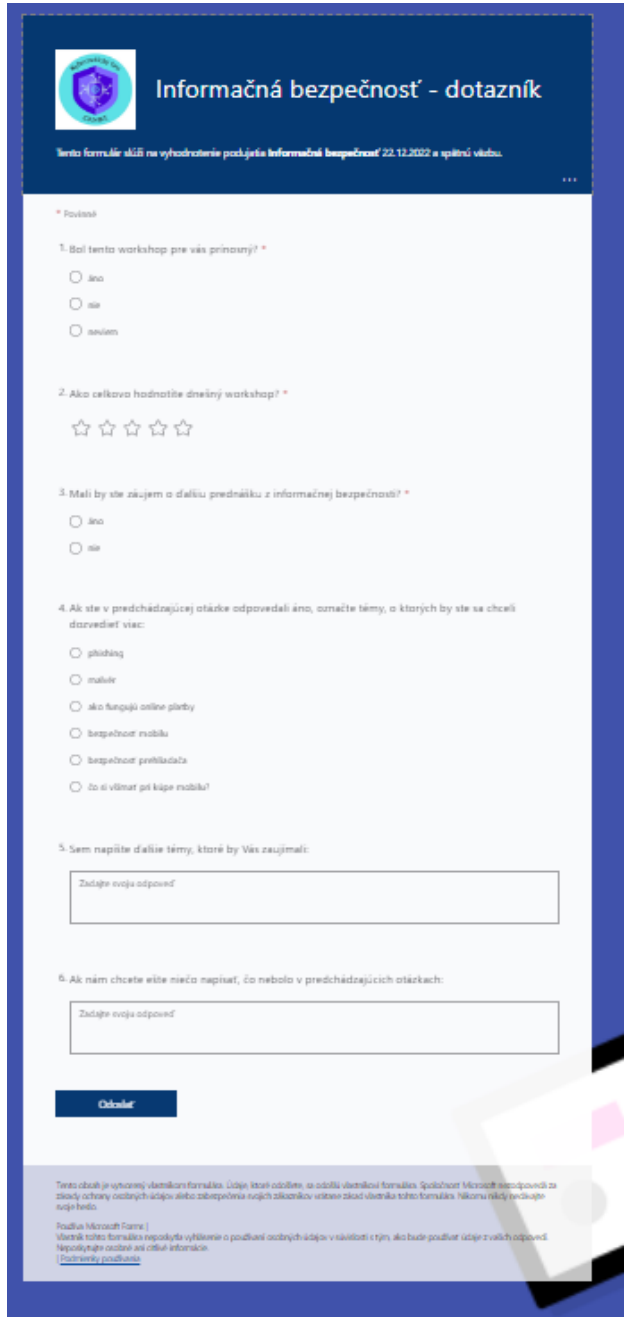
Spätná väzba

https://forms.office.com/e/m0aHySwNRZ



Spätná väzba

Vyplňte formulár - spätnú väzbu:



Domov dôchodcov:

https://forms.office.com/e/0m898uquRb

ZPP Radosť:

https://forms.office.com/e/xybF5YEABG

ZŠ:

https://forms.office.com/e/MHLX29mWnS

Ďakujeme za pozornosť

Kontakt:

Mária Vavrová

mariavavrova@gkmke.sk

Informácie o KyberTíme:

https://gym.gkmke.sk/it-aktivity/kyberneticka-bezpecnost/

Informačná bezpečnosť

Kybernetický bezpečnostný tím GKMKE

Ďakujeme za pozornosť!