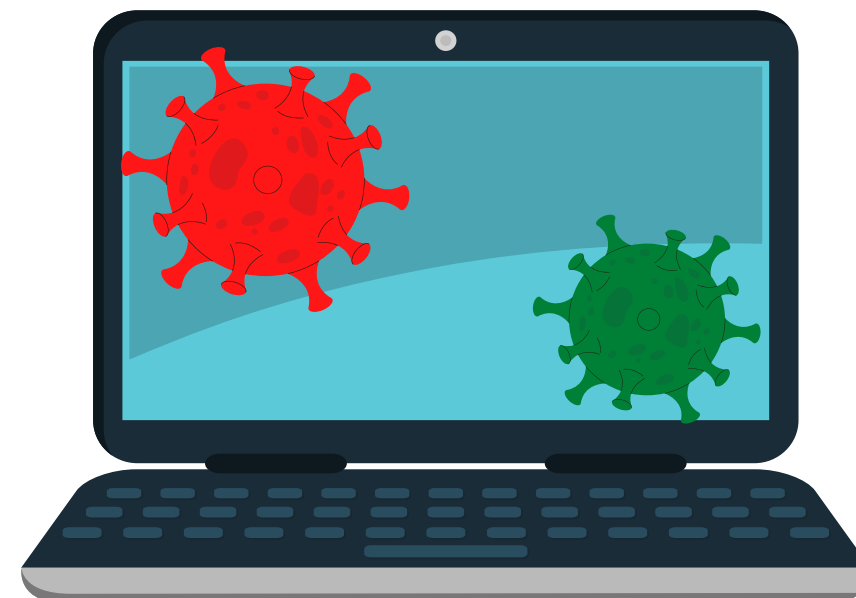




Informačná bezpečnosť



Kybernetický bezpečnostný tím GKMKE





Gymnázium sv. Košických mučeníkov



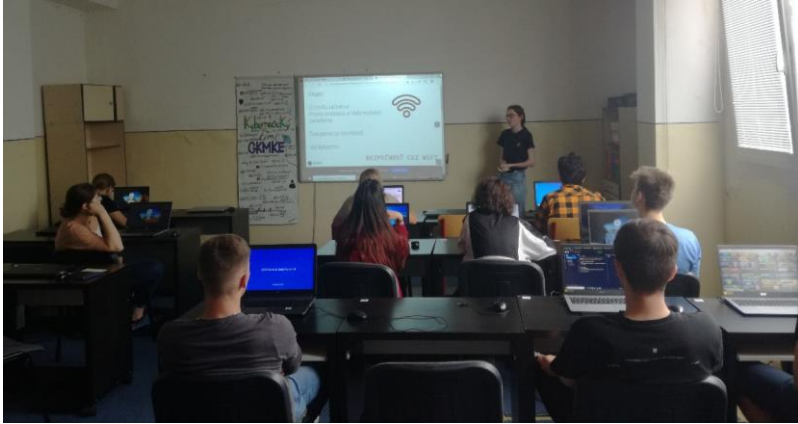
Čordákova 50, Košice - KVP

KyberTím GKMKE

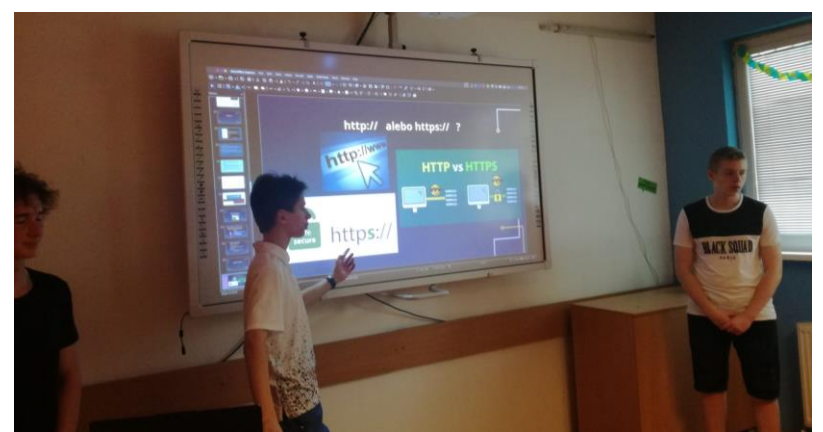
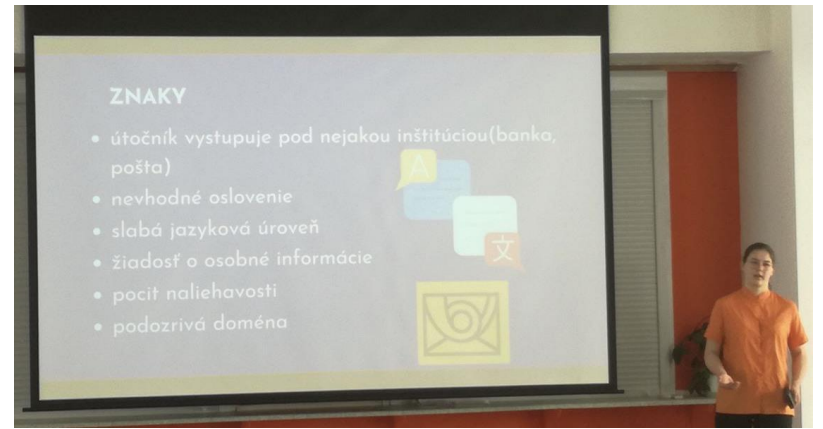
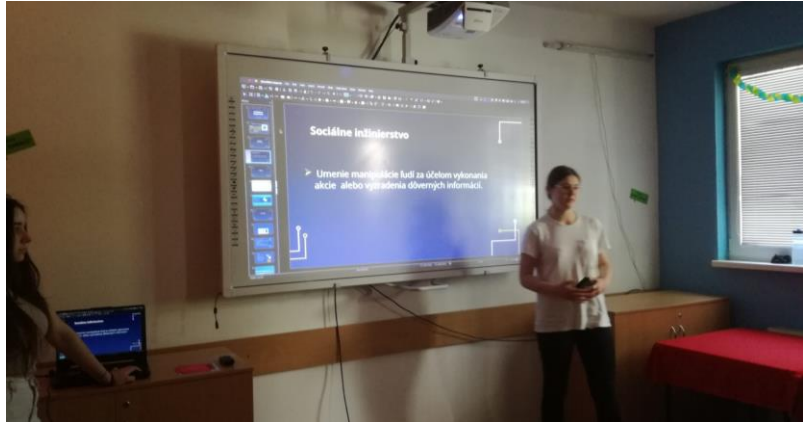


- od šk. roka 2021/2022
- projekt CSIRT UPJŠ: **Nauč sa základy informačnej bezpečnosti a vzdelávaj svoje okolie** - vzdelávanie (<https://csirt.upjs.sk/#/projekty/zvysovani-e-bezpecnostneho-povedomia-na-SS>)
- aktivity: <https://gym.gkmke.sk/it-aktivity/kyberneticka-bezpecnost/>
- projekt **Výnimočné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

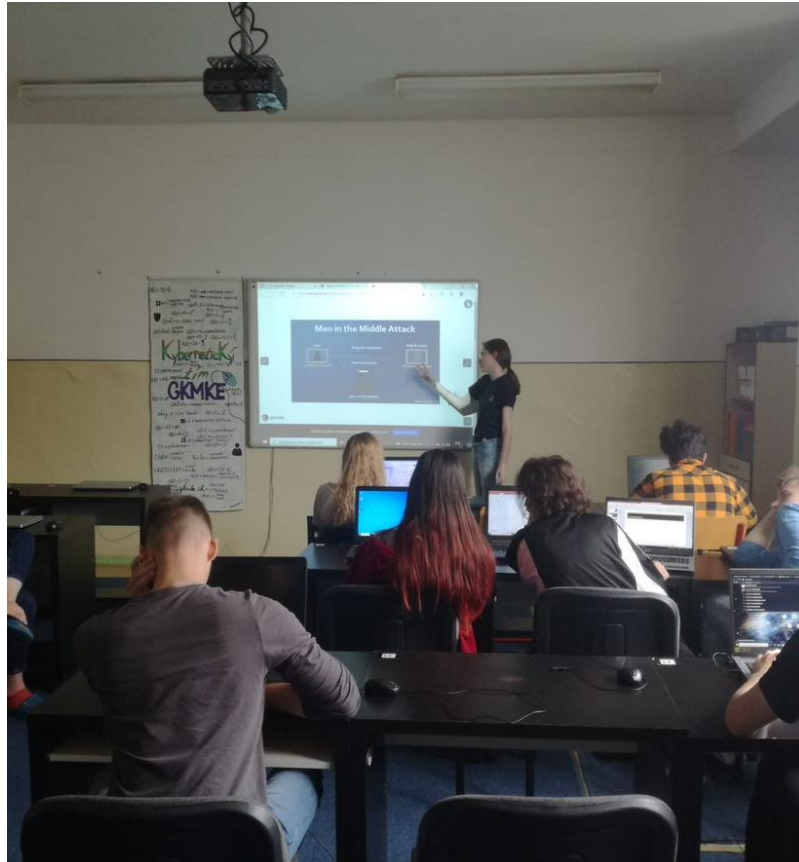




Vzdelávacie aktivity pre žiakov našej školy
2021/2022



Workshopy pre rodičov, Centrum Dorka
2021/2022



Workshopy pre žiakov, ZPP Radosť seniorov, 2022/2023

CyberSecurity Day pre ZŠ

Zaujima Ťa informačná bezpečnosť?
 Si zvedavý, ako prebieha kybernetický bezpečnostný útok?
 Čo všetko o Tebe vie internet?
 Chceš vedieť, ako sa nestáť obeťou podvodných správ?
 Vieš, ako bezpečne používať svoje mobilné zariadenie?

Odpovede na tieto otázky nájdeš u nás!

Akciu pripravuje KyberTím GKMKE v spolupráci s bezpečnostným tímom CSIRT-UPJS a s odborníkmi z praxe.

Kedy? 24. februára 2023 v čase 9.00 – 13.00 h
Kde? Gymnázium sv. Košických mučeníkov, Čordákova 50, Košice
Pre koho? Akcia je určená žiakom ZŠ (7. – 9. roč.) a ich učiteľom, ktorí sa zaujímajú o Informačnú bezpečnosť.

Prihlasovací formulár:
<https://forms.office.com/e/ZetUG7x6TG>

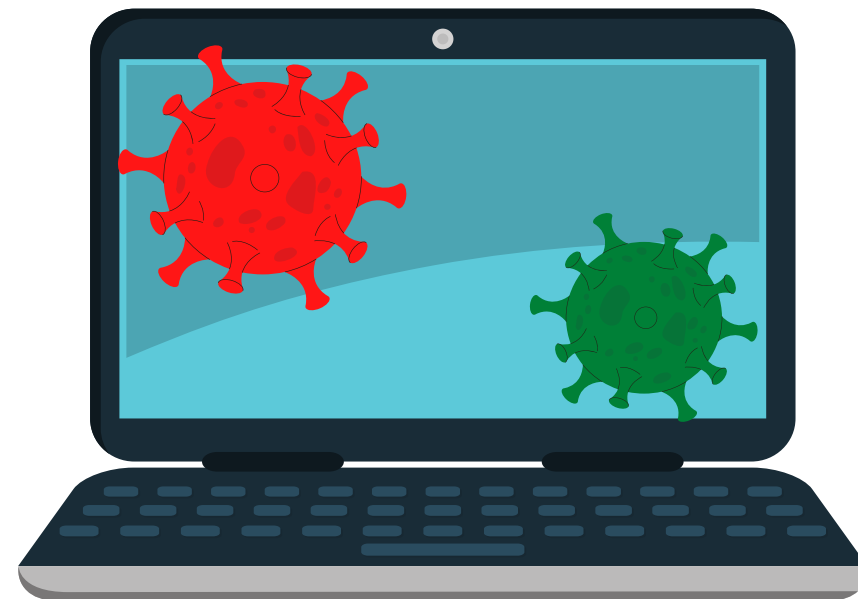
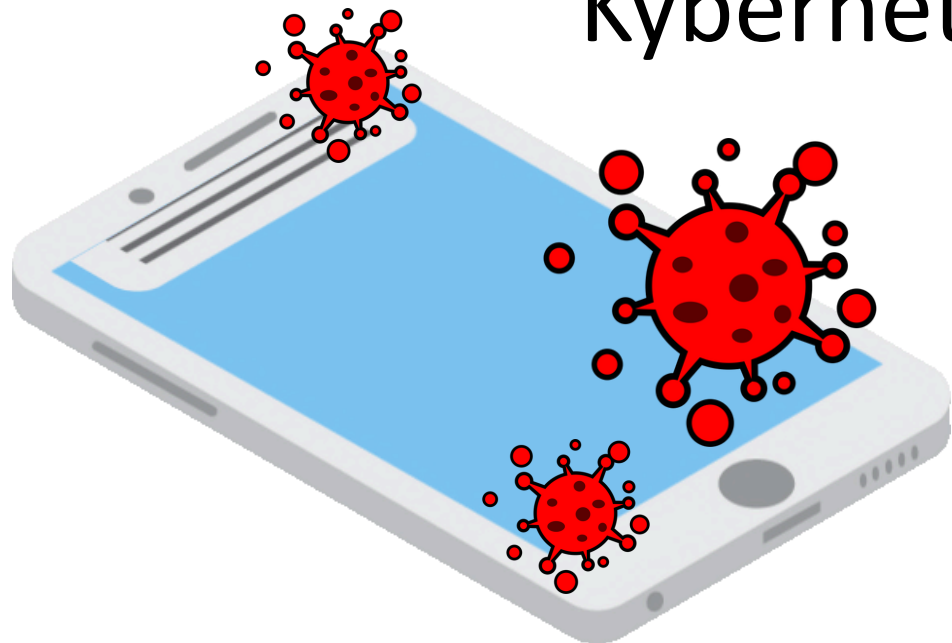
Viac informácií:
<https://gym.gkmke.sk/cybersecurityday/>



Ako sa nestat' obeťou podvodných správ



Kybernetický tím GKMKE



USERNAME

IDENTITY

ACCOUNT

PASSWORD

Čo podvodníkov zaujíma?

HACK

BANK

SPY

ZAÚJÍMAVÉ 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

The illustration depicts a digital security threat. On the right, a stylized hacker wearing a black balaclava and a black beanie is shown from the chest up, holding a smartphone. A long, thin black line extends from the phone's screen towards the left, ending at a laptop screen. The laptop screen displays several icons representing digital assets: a pink piggy bank, a document labeled 'SOFTWARE LICENSE' with a blue icon, a red credit card, and a dollar bill with a large '\$' symbol. A speech bubble icon is also visible in the top left corner of the laptop screen. The background is a solid teal color.

An illustration depicting digital theft. On the right, a character wearing a black balaclava and a black beanie is shown from the chest up, holding a long fishing rod. The rod is positioned over a laptop screen on the left. The laptop screen displays various digital assets: a pink piggy bank, a stack of papers, a document labeled 'SOFTWARE LICENSE', a gold coin, and a dollar bill. The background is a light blue gradient.

**36 miliárd phishingových správ
ročne!**

Nezabudnite

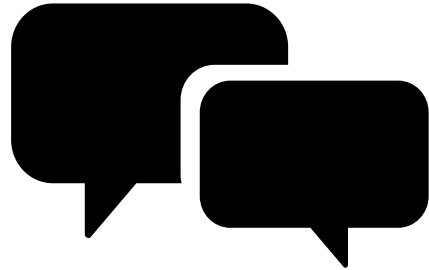
„Peniaze na účte v banke sú v bezpečí a ich najväčším rizikom je majiteľ účtu, ktorý, hoc aj nevedomky, poskytne svoje údaje podvodníkovi. Až v 99,9 % prípadov sa o peniaze pripraví sám majiteľ účtu tým, že podvodníkovi nadiktuje svoje osobné či prihlasovacie údaje do internetbankingu, údaje k platobným 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.“

The background features a light blue gradient. On the right, a large smartphone is shown with a thief character on its screen. The thief is wearing a black balaclava, a black beanie, and a black turtleneck, with a wide, toothy grin. On the left, a laptop screen displays various financial icons: a pink piggy bank, a stack of white papers, a gold coin, a red wallet, and a blue banknote with a white dollar sign. The main text is centered over the laptop screen.

**Človek DOBROVOĽNE odovzdá
svoje údaje.**

Možnosti útokov

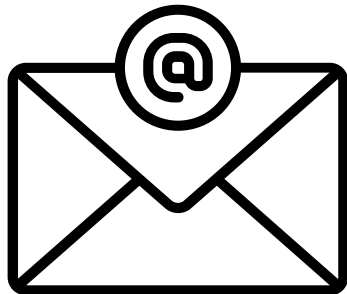
CEZ SMS



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

17:48

Si to ty vo videu? 😨😨
<http://tiktok.1401y.us/E2Wehqv>

Pi 19:50

Si to ty vo videu? 😨
😨
<http://tiktok.1401y.us/9vUX5Z7>

BitDefender

Malware

G-Data

Malware



Nachytali ma, čo teraz?

S priateľom, ktorý vám falošné správy posielala, 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.

Otestujte odkaz

www.google.sk

2a00:1450:4001:808::2003 

URL: <https://www.google.sk/?hl=sk>

Submission: On February 07 via manual (February 7th 2023, 5:29:48 am UTC) from  — Scanned from 

- Summary
- HTTP 12
- Redirects
- Links 13
- Behaviour
- Indicators
- Similar
- DOM
- Content
- API
- Verdicts


- Lookup
- Go To
- Rescan
- Add Verdict
- Report

Summary

This website contacted 5 IPs in 2 countries across 3 domains to perform 12 HTTP transactions. The main IP is 2a00:1450:4001:808::2003, located in Frankfurt am Main, Germany and belongs to GOOGLE, US. The main domain is www.google.sk. The Cisco Umbrella rank of the primary domain is 31014. TLS certificate: Issued by GTS CA 1C3 on January 9th 2023. Valid for: 3 months.

www.google.sk scanned 121 times on urlscan.io

Show Scans 121

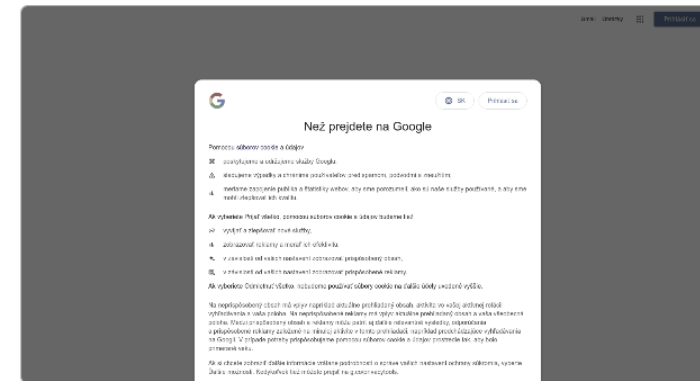
urlscan.io Verdict: No classification 

Live information

Google Safe Browsing:  No classification for www.google.sk
Current DNS A record: 142.250.186.35 (AS15169 - GOOGLE, US)

Screenshot

- Live screenshot
- Full Image



Page Statistics

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

Podvodný odkaz

- P. tlačidlom myši skopírovať, NEKLIKAŤ!!!

<https://is.gd/UsBkHq>

- Nakopírovať do: <https://urlscan.io/>

The screenshot shows the urlscan.io interface. At the top, there's a navigation bar with icons for Home, Search, Live, API, Blog, Docs, Pricing, and Login. The main content area displays the URL <https://is.gd/UsBkHq> and its IP address 2606:4700:20::6819:ea35 with a US flag. Below this, it states the submission date and time, and the source country (SK). A row of navigation tabs includes Summary, HTTP (2), Redirects, Behaviour, Indicators, Similar, DOM, Content, API, and Verdicts. The Summary section provides technical details: 'This website contacted 1 IPs in 1 countries across 1 domains to perform 2 HTTP transactions. The main IP is 2606:4700:20::6819:ea35, located in United States and belongs to CLOUDFLARENET, US. The main domain is is.gd. The Cisco Umbrella rank of the primary domain is 63773. TLS certificate: Issued by Cloudflare Inc ECC CA-3 on April 11th 2023. Valid for: a year.' It also shows that 'is.gd' has been scanned 10000+ times on urlscan.io. A 'Screenshot' tab is visible on the right, showing a placeholder for a disabled link.

Link Disabled

This shortened URL has been disabled due to a violation of our [terms & conditions](#). Most likely this link was being used maliciously or was used in spam. Please be careful when visiting links you receive from somebody you don't know.

If you received spam, please be aware that we did not send it - is.gd is a URL shortening/redirection service and does not operate any email servers or lists. We have no contact with or association with spammers so are unable to unsubscribe you from any such lists.

is.gd takes all abuse of our service very seriously and we use a combination of automated measures and manual investigation of all complaints to prevent it wherever possible. Please see our [policy on fighting spam](#) for more details. We are sorry for any inconvenience that the misuse of this URL may have caused you.

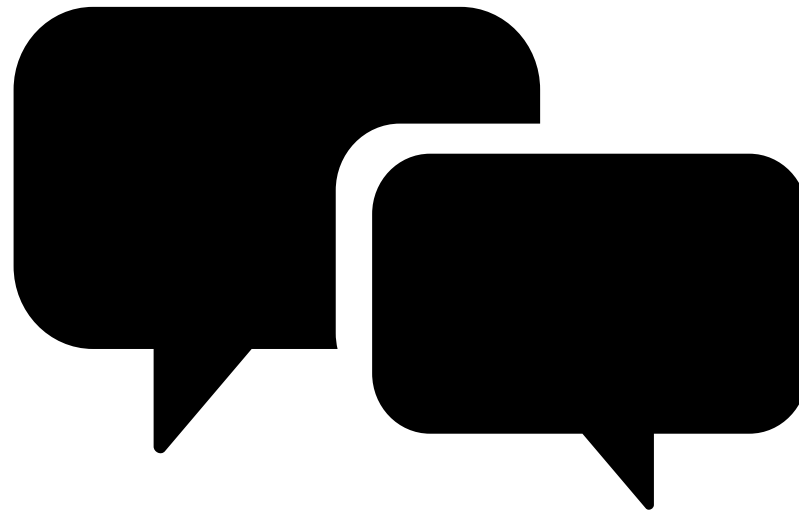
For reference and to help those fighting spam the original destination of this URL is given below (we strongly recommend you don't visit it since it may damage your PC): -
https://posts.cyou/#/?_from=__mail

is.gd

is.gd is a free service used to shorten long URLs. For further information or to contact us (for example if you think this URL was disabled in error) please visit our website at <https://is.gd/>.

Podvodné sms správy

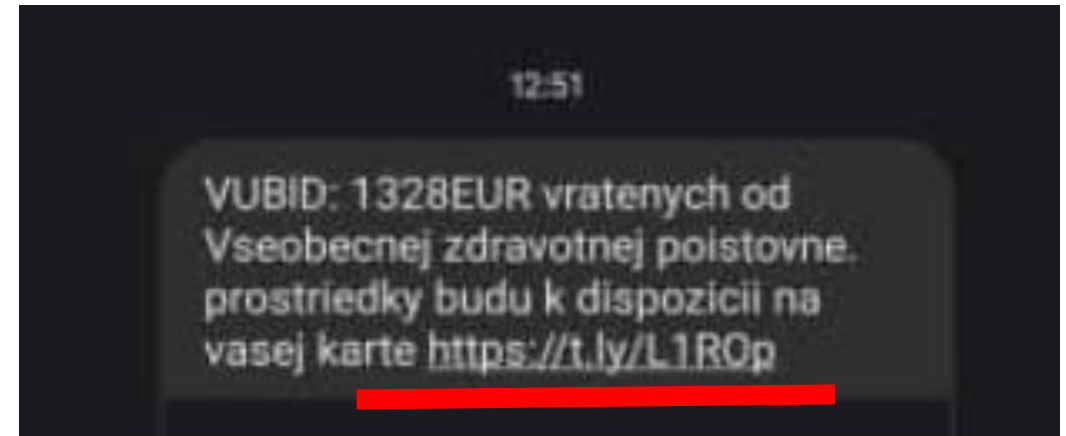
SMISHING



Podvodné sms správy

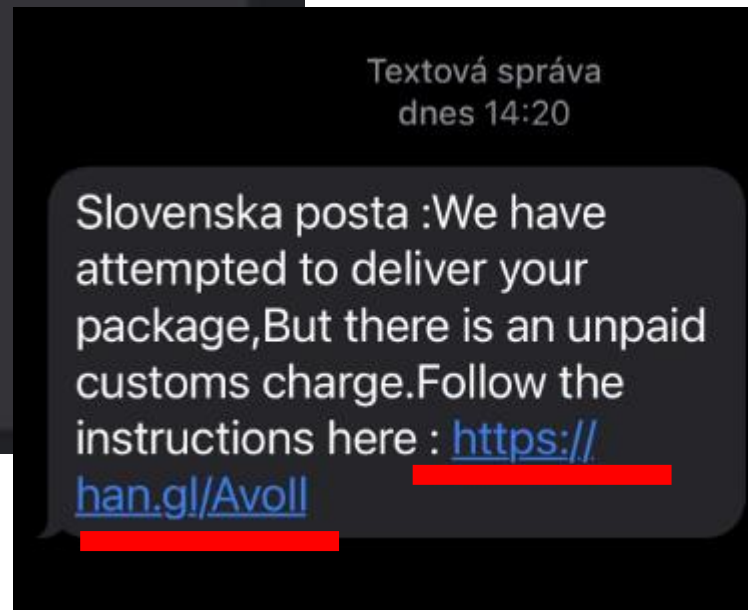
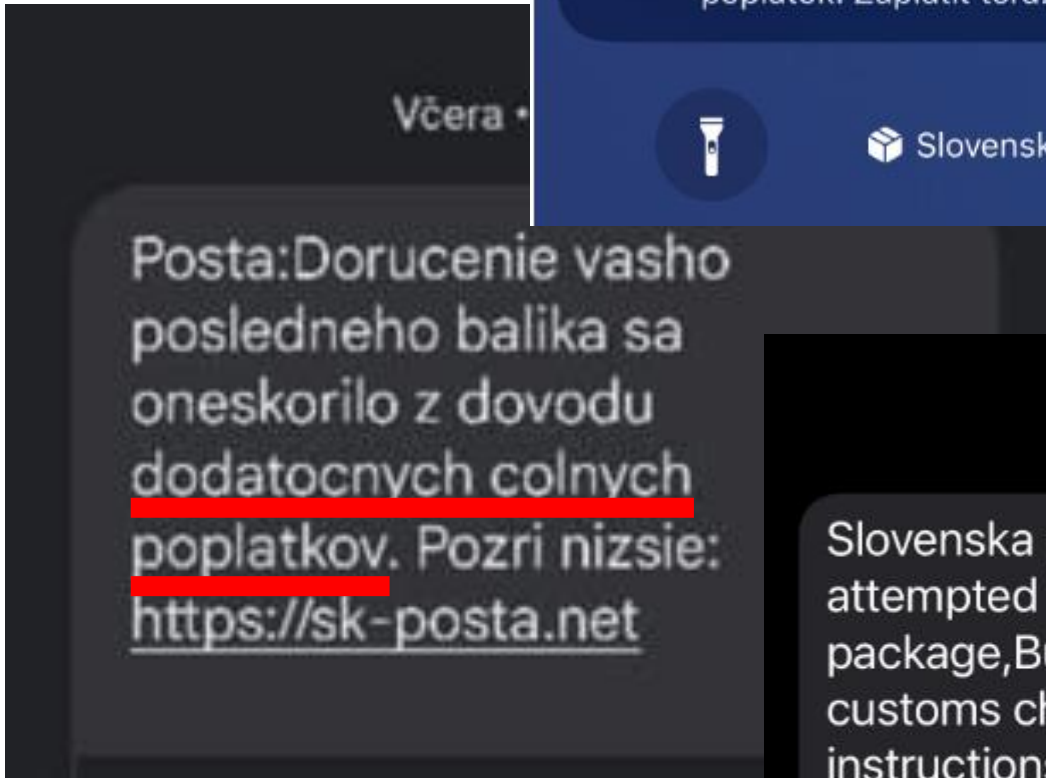
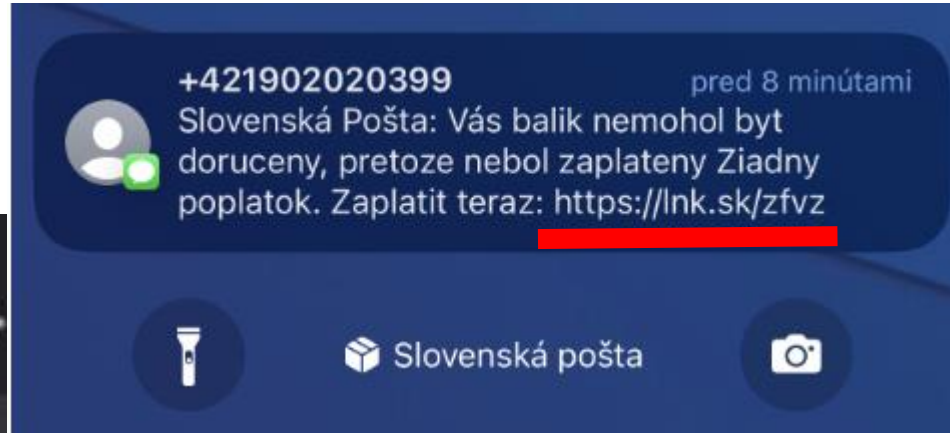


- od **Všeobecnej zdravotnej poisťovne**
- vrátenie peňazí na platobnú kartu
- podvodný link !
- **poisťovňa nevracia finančné prostriedky takouto formou!!!**



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 balik.** 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

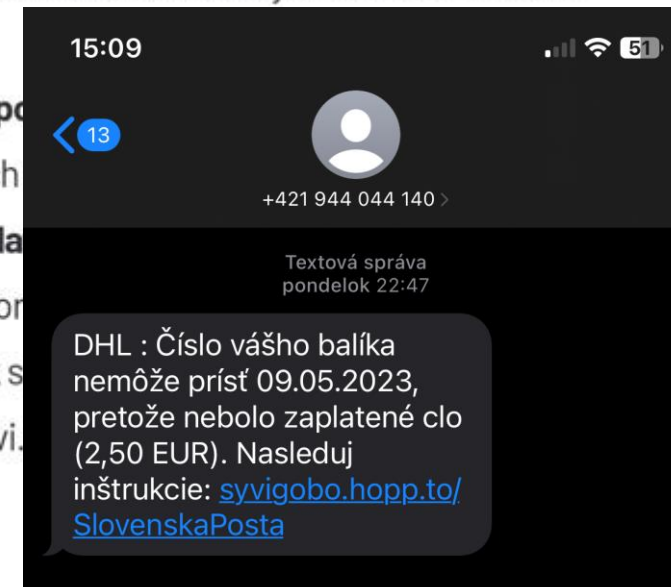
že od svojich

žiadne popla

náklady s dor

uhradiť, tak s

rúk kuriérovi.



Podvodné sms správy

- od **banky**

Today 16:07

Vas online ucet je docasne
zablokovany z dovodu podozrivej
aktivity, Prihlaste sa a overte svoje
informacie : [https://bit.ly/
SLPSLOVENSKA](https://bit.ly/SLPSLOVENSKA)

Moja.Tatrabanka: Vas ucet bol
zablokovany. prihlaste sa teraz,
inak bude ucet zruseny. [https://
moja-tatrabanka-blokovany.info](https://moja-tatrabanka-blokovany.info)



Podvodné sms správy

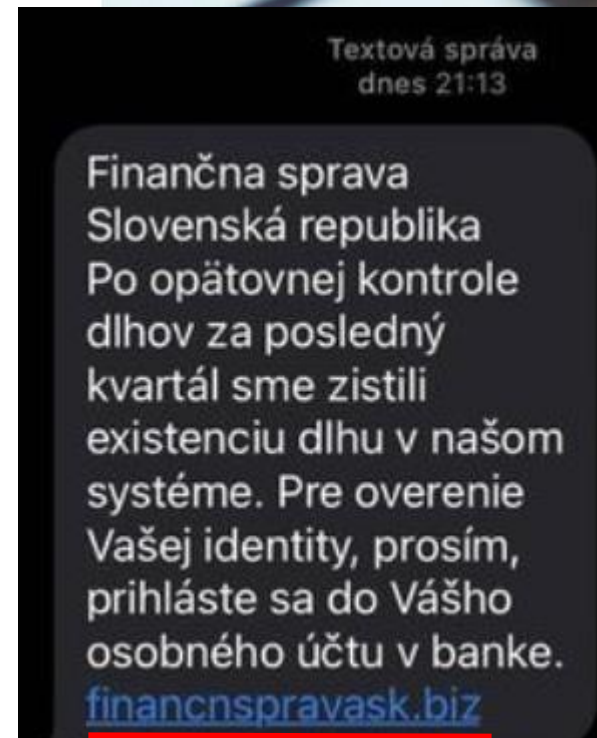
- od **Finančnej správy SR**
- evidujeme dlh,
- pre overenie identity sa prihláste do svojho účtu v banke,
- Link !
- **štátne inštitúcie neinformujú občanov o dôležitých informáciách formou SMS správ ani prostredníctvom odkazov, na ktoré je potrebné kliknúť !!!**

Ďalší podvod cez SMS-ky: Podvodníci zneužívajú meno úradu, na takéto správy nereagujte!

20:19 22.03.2023

BRATISLAVA

SPRÁVY » DOMÁCE



Podvodné telefonáty

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

VISHING



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

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

álnej sieti.



“

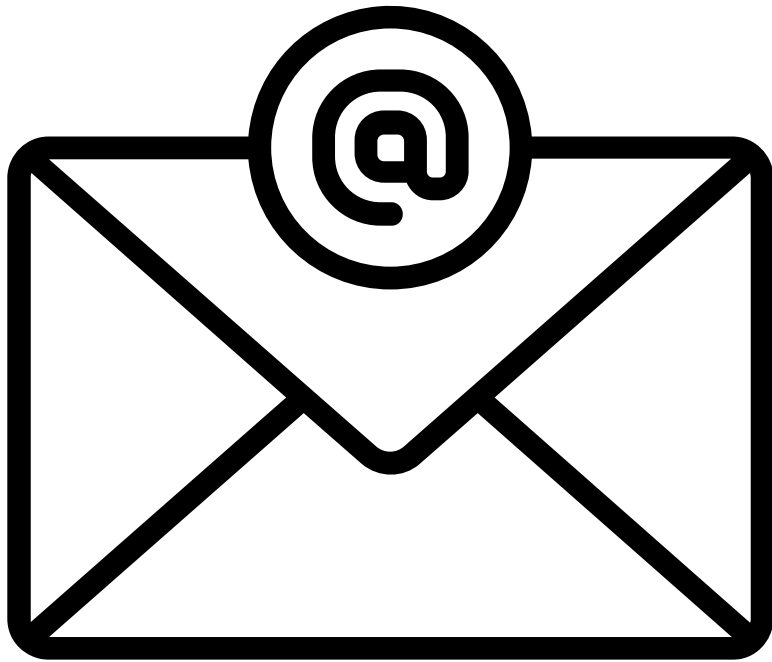
„Polícia s občanmi v žiadnom prípade takýmto spôsobom nekomunikuje. Ak vám zavolá človek alebo robot hovoriaci po anglicky, ktorý sa bude vydávať za políciu, hovor okamžite ukončíte a telefónne číslo si zablokujete.“

 Microsoft

Podvodné e-maily

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

PHISHING



Podvodné e-maily



nevhodné oslovenie



Allen <lisa@traxtaavern.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 priechinka nevyžiadanej pošty / hromadného obsahu, je to z dôvodu obmedzení implementovaných vašim 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 UŽIVATEĽA, 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 vašim 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.

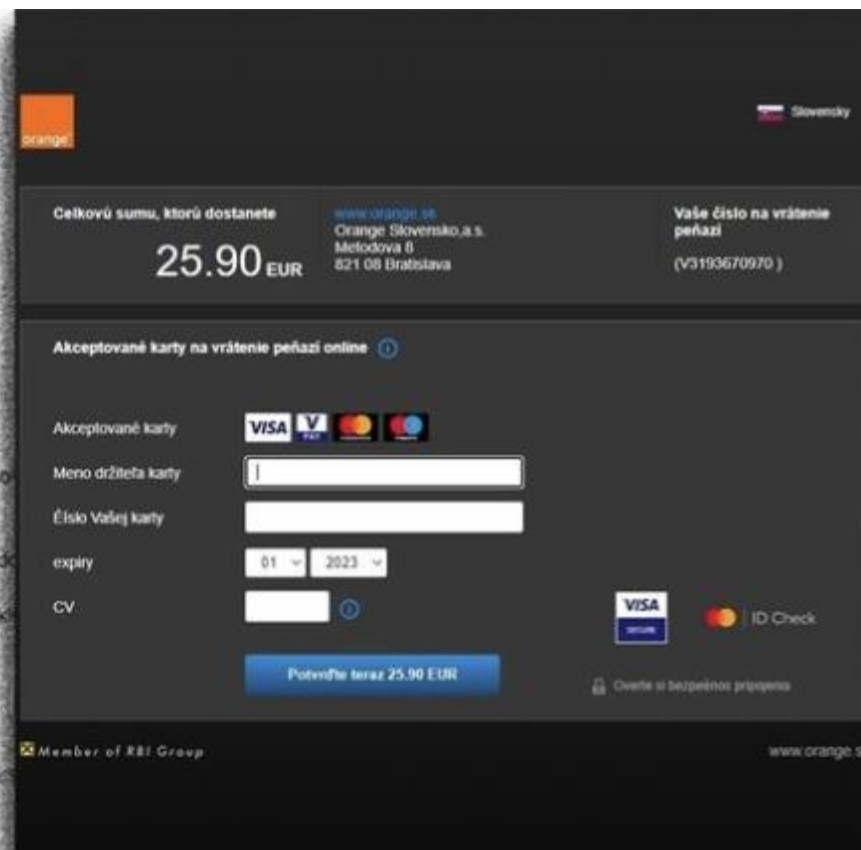
Nepochybujte o tomto liste alebo ho ignorujte, pretože sme pripravení odovzdať vám vaše neuveriteľné ocenenie od Facebooku

[Odpovedať](#) | [Odpovedať všetkým](#) | [Preposlať](#)

Podvodné e-maily



AKTUÁLNE!



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



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 €

Pripojte k zábave aj blízkeho

Ak si teraz vezme náš povný
internet, obaja získate 5 GB
mesačne na rok bez poplatkov.

[Zistiť viac](#)

Bezpečný
internet
so sebou
ako darček

Zabezpečte si svoje online súkromie

Aktivujte si bezplatne službu
Online ochrana, ktorá chráni
vaše zariadenia pred vírusmi.

[Zistiť viac](#)

Ak si neželáte dostávať spolu s faktúrou aj marketingové informácie, môžete sa po prihlásení a Vašej identifikácii odhásiť 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.

Právne informácie / 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

[dôležité](#)

[pracovné](#)

[osobné](#)

[odpísať](#)



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

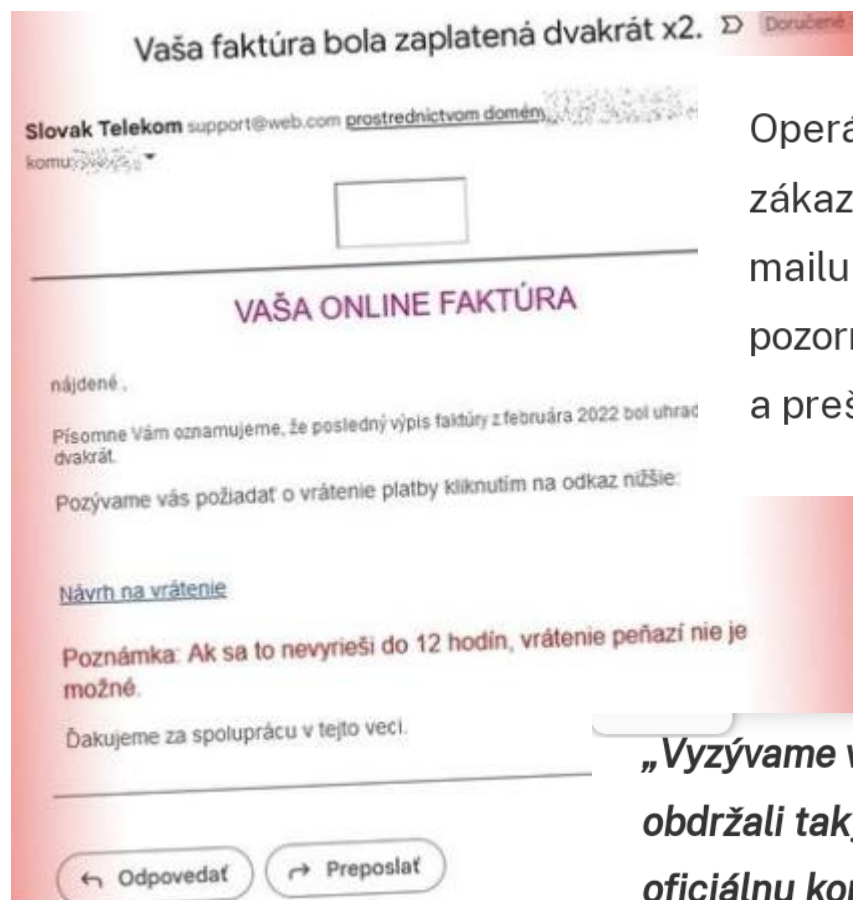


Telekom

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.

Podvodné e-maily



banka!

SLSP upozorňuje na množiace sa podvody

Slovenská sporiteľňa pár dní dozadu informovala, že sa množia podvodníci, ktorí používajú jej značku. Podvodníci sa snažia získať najmä prihlasovacie údaje k účtom v Tatra banke, aby sa dostali k ich peniazom.



„Upozorňujeme vás na podvodné e-maily, textové správy a SMS, ktorými sa podvodníci snažia získať prístupové heslá k účtom našich klientov.“, píše banka v oznámení.

SLSP vysvetľuje, že za týmto účelom útočníci posielajú podvodné e-maily a SMS. Rovnako upozorňuje aj na to, že sa množia podvodné SMS správy a kľúčové slová.

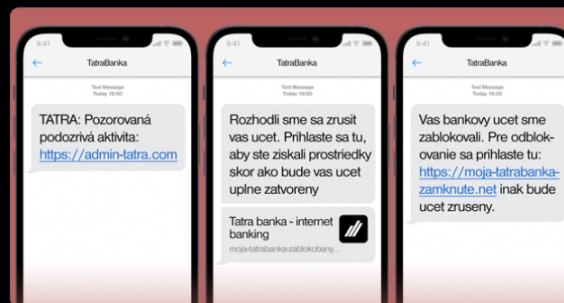
Tieto podvody majú jedného spoločného menovateľa, snažia sa dostať k peniazom od obete požadujú vyplnenie prihlasovacích údajov alebo informácie z účtu. Ak používateľ tieto údaje vyplní, tak prakticky ich odovzdá útočníkovi, ktorý sa môže pozrieť, ako tieto podvody vyzerajú.

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/>

Bezpečnosť

rozosielanie podvodných SMS správ a e-mailov neúčtíča, a preto Vám dávame do pozornosti bezpečnostné odporúčania.

Nedajte sa nachytať. Obzvlášť v situáciách, ktoré vo Vás vyvolávajú pocit naliehavosti alebo Vás napríklad zavádzajú informáciami o blokovaní či zrušení účtu alebo karty.



Banka nikdy neoslovuje klientov touto formou a nežiada od nich citlivé osobné a bankové informácie cez akékoľvek priložené linky.

9:34

BEZPEČNOSTNÉ UPOZORN...



Vážená pani [redacted]á,

dajte si pozor na podvodné praktiky zlodějov pri predaji a kúpe cez inzertné portály.

Nezadávejte osobné a identifikačné údaje na stránke, na ktorú ste sa preklikli cez odkaz v e-maile, v SMS alebo v čítovej službe.

Tieto správy vyzerajú ako oficiálna komunikácia daného inzertného portálu alebo aplikácie, no môžu pochádzať od podvodníka.

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.

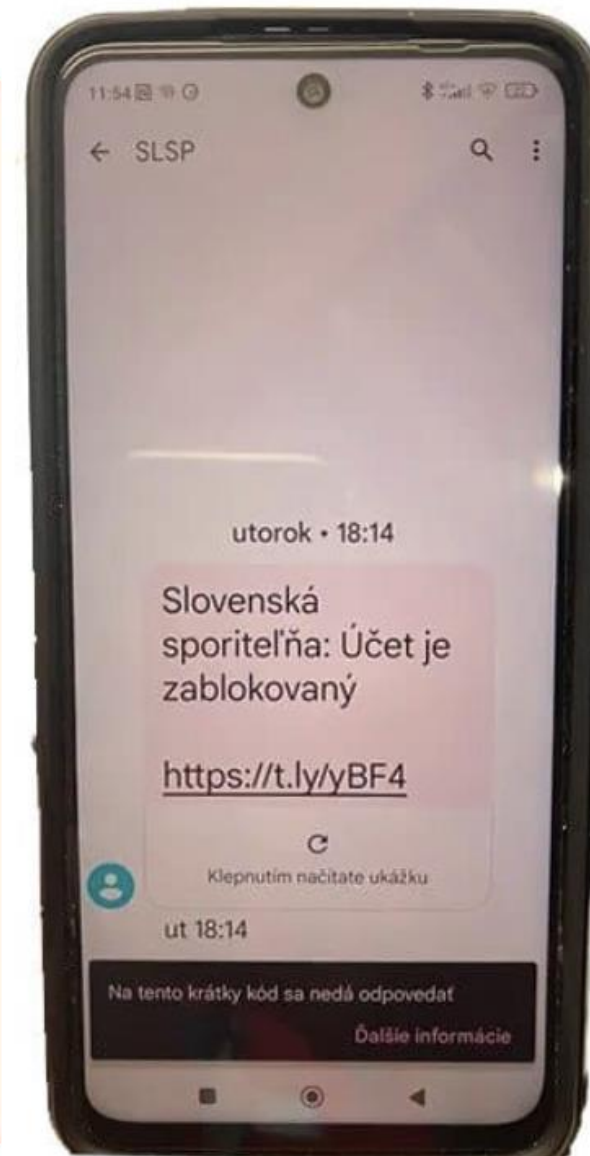
Tel: +421 25826 8111, 0850 111 888

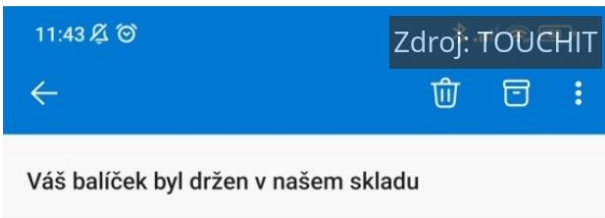
Mail: info@slsp.sk

web: www.slsp.sk

Slovenská sporiteľňa

SLOVENSKÁ
SPORITELŇA





Zásilkovna Česká republika
mreiter@touchit.sk 11:31



Dobrý den , máte (1) balíček čeká na doručení.

Sledovací číslo: [#Z35154225](#)

Naplánujte si doručení* :

Naplánujte dodávku

*Pokud neobdržíme odpověď do 5 pracovních dnů, váš balíček bude vrácen odesílateli.

OČEKÁVANÉ ZMEŠKANÉ DORUČENÍ
Pokus o doručení: Je vyžadován podpis
Sledovací číslo: [#Z35154225](#)

← Odpovědět

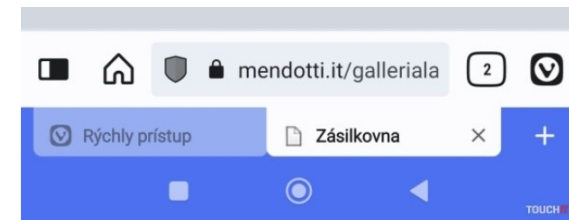
Zdroj: <https://touchit.sk/>



Zásielkovňa

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-mailly



dar = SCAM



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>

Podvodné e-maily



podozrivý link!

Virus nalezen

Ceska Sporitelna(CZ) <silviagarcia360@silviagarcia360.com>
16.10.2018 9:13
Komu: solution1@ceska.com

Vážení zákazníci České spořitelna,

Rádi bychom Vás upozornili na novou formu podvodného e-mailu (phishingu), který jsme nedávno poznamenali, a snaží se to vyvolat dojem, že byla zaslána Českou spořitelnou. Prostřednictvím něho se podvodníci pokoušejí vygenerovat přihlašovací informace na podvodnou přihlašovací stránku.

Buďte velmi opatrní ohledně podezřelých e-mailů, nikdy jsme z tohoto systému neposílali takové zprávy a viry. Okamžitě vás žádáme, abyste aktualizovali svůj systém internetového bankovníctví, aby se předešlo takovým podvodným útokům a šíření virus.

Pro rychlou aktualizaci vašeho účtu Servis-24 navštivte prosím: www.servis24.cz/stat/ebanking/s24/index.html

Tato zpráva byla zaslána všem zákazníkům České spořitelny a měla by se s nimi přistupovat naléhavě

Děkuji,
Česká spořitelna

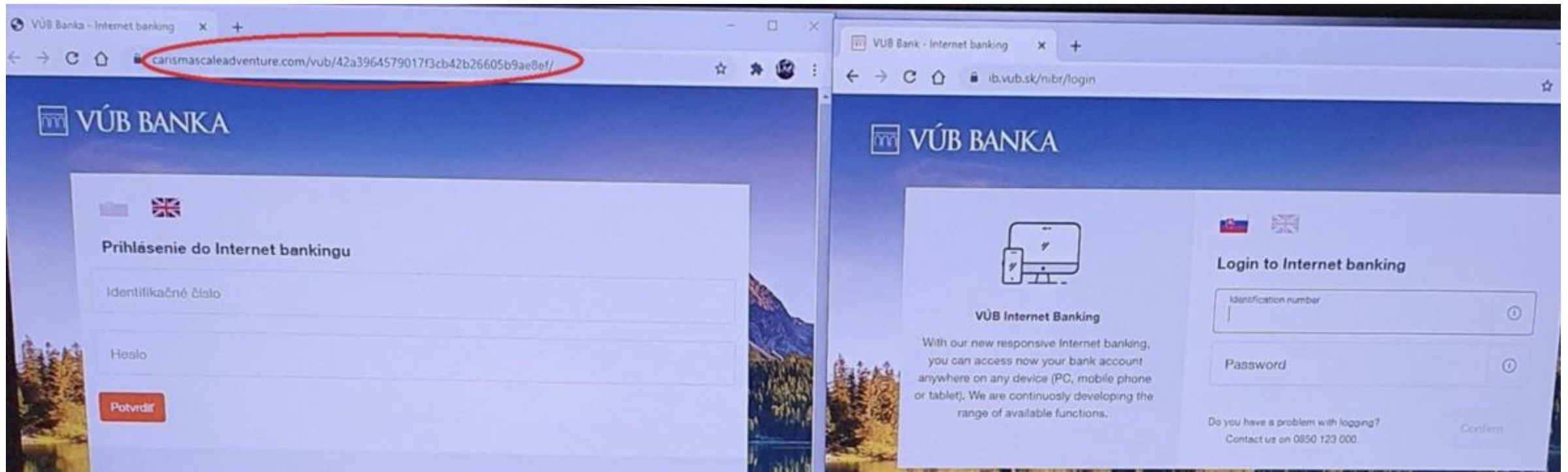
<https://help-nbvghfzqoi.cf/online.htm>

Podvodné e-mailly



podozrivý link!

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



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:.....@......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 nebude 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

Podvodné e-mailly



podozrivé súbory!



"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.

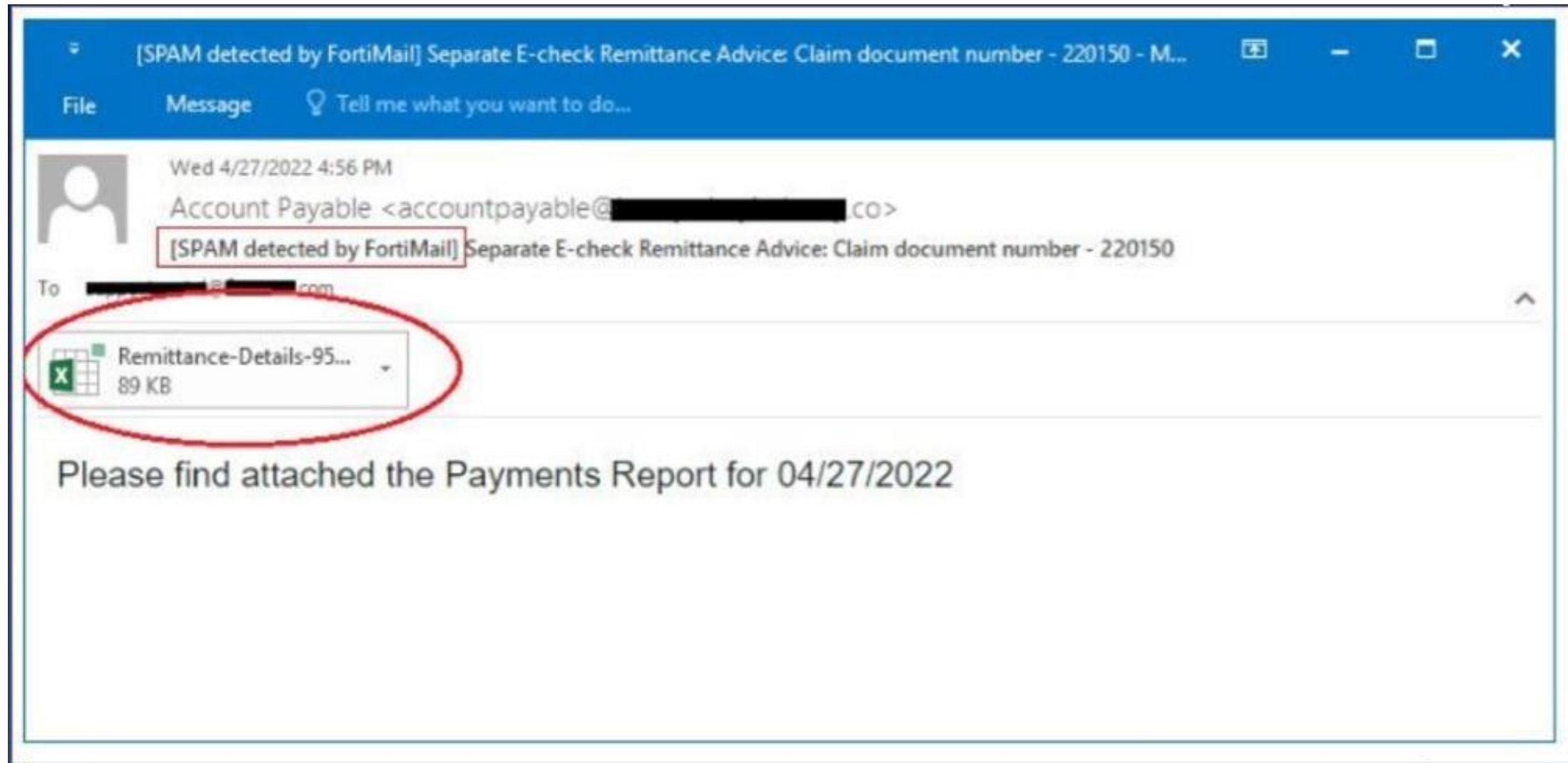
← Odpovedať

↪ Preposlať

Podvodné e-maily



podozrivé súbory!



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=elkPYH6aBF8>



Phishingový test



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



Dokážete rozpoznať podvodný e-mail?

Identifikovať podvodný e-mail môže byť ťažšie ako by ste si mysleli. Útočníci sa od Vás pomocou podvodných e-mailov pokúsia zistiť Vaše súkromné informácie predstieraním, že sú niekto, koho poznáte. Dokážete rozlíšiť, ktoré e-maily sú podvodné?

Čo by ste si mali všímať? Odosielateľa, gramatické chyby, oslovenie, urgentnosť/naliehanie, ak niečo nepotvrdíte. Odkazy, ktoré môžu reálne odkazovať inam ako na prvý pohľad pôsobia, neopodstatnené žiadosti o Vaše prihlasovacie údaje, legitímnosť príloh...



Vymyslíte si meno a e-mail.

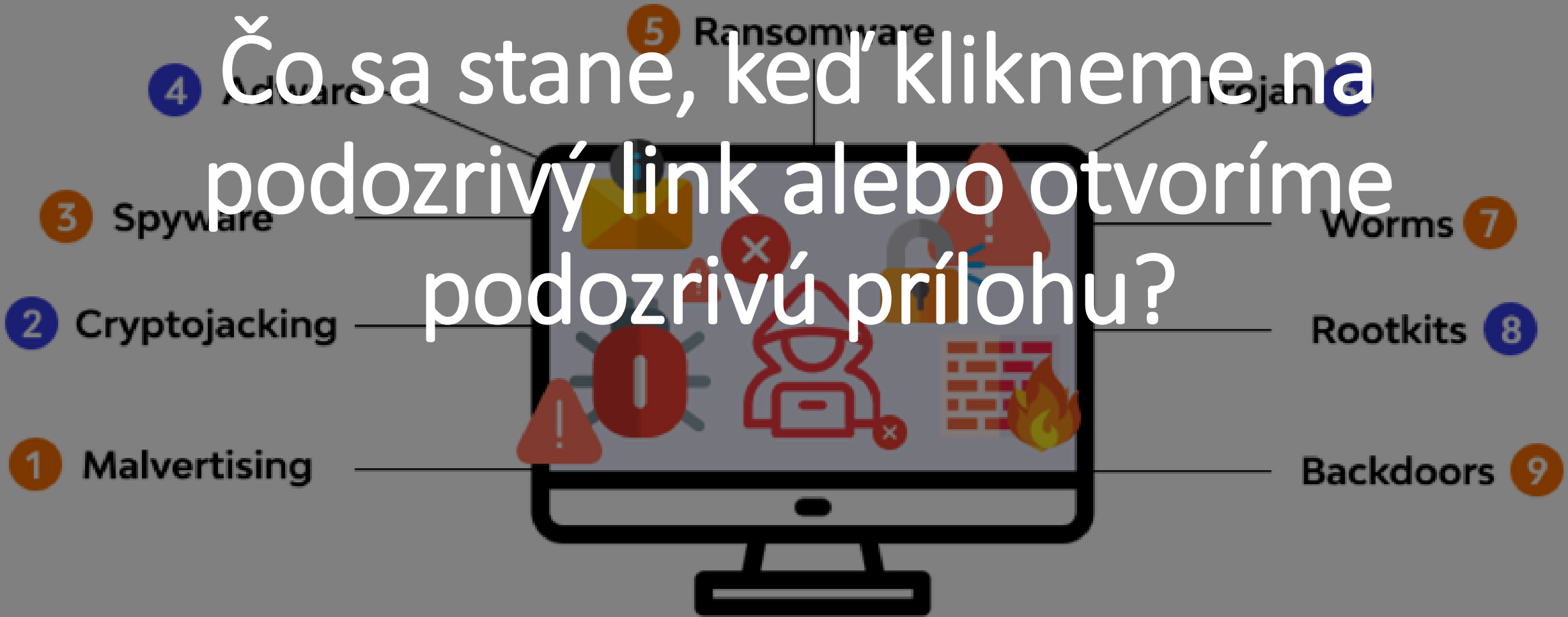
Vytvorte meno a e-mail — ani jedno nemusí byť skutočné — aby tento kvíz pôsobil realisticky. Nemaňte obavy, tieto informácie neopustia Vaše zariadenie.

Otestujte sa

- Kvíz SLSP: <https://www.slsp.sk/sk/ludia/bezpecnost>
<https://www.slsp.sk/sk/ludia/bezpecnost#/modalComponent/isOpen/t rue/url/%2Fsk%2Fconfiguration%2Fleads%2Fbezpecnost-test%2Fotazka1.modal>

Types of malware

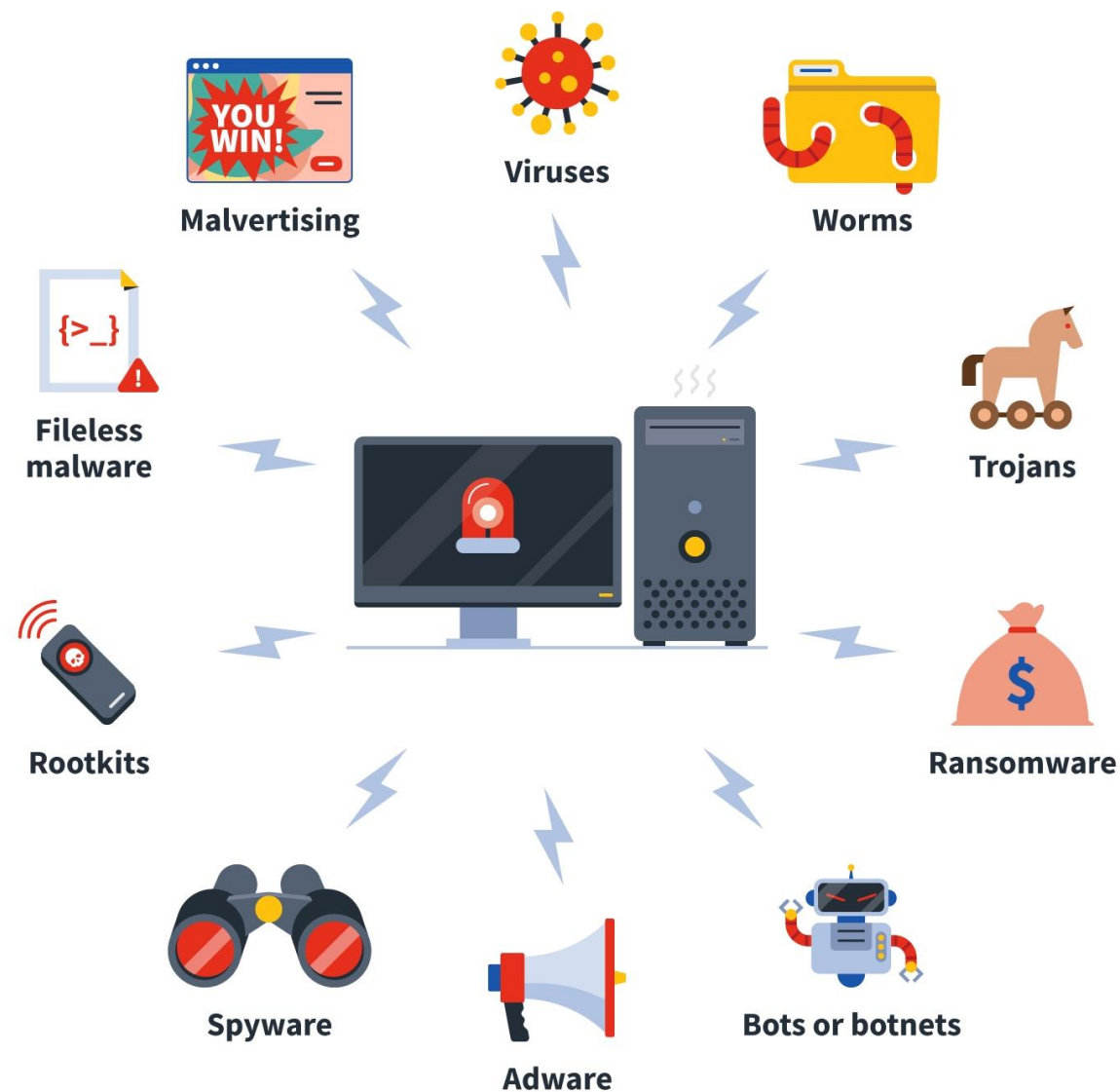
Čo sa stane, keď klikneme na podozrivý link alebo otvoríme podozrivú prílohu?



Malvér

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

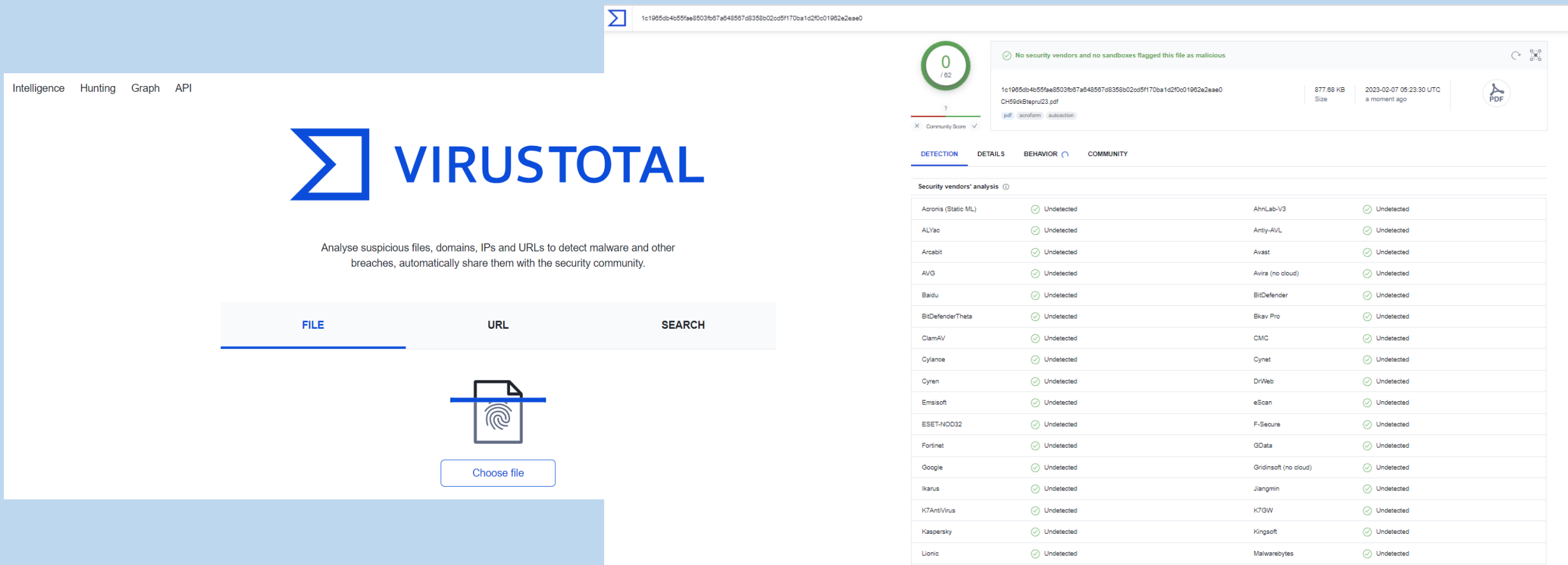
Types of Malware



A person's hands are shown typing on a laptop keyboard. The background is a dark blue, semi-transparent digital interface with various icons representing security and communication, such as padlocks, envelopes, and mobile devices, connected by a network of dots and lines. The overall aesthetic is futuristic and tech-oriented.

Bud'te opatrní!

Otestujte súbor alebo odkaz



The image shows the VirusTotal website interface. On the left, the main navigation menu includes 'Intelligence', 'Hunting', 'Graph', and 'API'. The VirusTotal logo is prominently displayed, along with the tagline: 'Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.' Below this, there are three tabs: 'FILE', 'URL', and 'SEARCH'. The 'FILE' tab is active, showing a document icon with a fingerprint and a 'Choose file' button.

On the right, a detailed analysis report is shown for a file with the hash `1c1965db4b55fae8503fb67a648507d8358b02cd5f170ba1d2f0c01962e2eae0`. The file is identified as `CH59dix8tepru23.pdf`, with a size of 877.88 KB and a date of 2023-02-07 05:23:30 UTC. A green circle with '0 / 62' indicates the community score. A message states: 'No security vendors and no sandboxes flagged this file as malicious'. Below this, there are tabs for 'DETECTION', 'DETAILS', 'BEHAVIOR', and 'COMMUNITY'. The 'DETECTION' tab is active, showing a table of security vendors' analysis results.

Vendor	Status	Vendor	Status
Acronis (Statio ML)	Undetected	AhnLab-V3	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected
BitDefenderTheta	Undetected	Bkav Pro	Undetected
ClamAV	Undetected	CMC	Undetected
Cylance	Undetected	Cynet	Undetected
Cyren	Undetected	DnWeb	Undetected
Emsisoft	Undetected	eScan	Undetected
ESET-NOD32	Undetected	F-Secure	Undetected
Fortinet	Undetected	GData	Undetected
Google	Undetected	Gridinsoft (no cloud)	Undetected
Ikarus	Undetected	Jiangmin	Undetected
K7AntiVirus	Undetected	K7GW	Undetected
Kaspersky	Undetected	Kingsoft	Undetected
Lionic	Undetected	Malwarebytes	Undetected

Otestujte súbor alebo URL adresu:

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

Otestujte odkaz

The screenshot shows the urlscan.io interface for the URL [www.google.sk](https://www.google.sk/?hl=sk). The URL is scanned from Frankfurt am Main, Germany. The interface includes a navigation bar with links for Home, Search, Live, API, Blog, Docs, Pricing, and Login. A search bar contains the URL, and buttons for 'Lookup', 'Go To', 'Rescan', 'Add Verdict', and 'Report' are visible. A summary section provides details on the scan: 5 IPs in 2 countries across 3 domains, 12 HTTP transactions, and a TLS certificate issued by GTS CA 1C3. A 'Screenshot' section shows a live screenshot of the Google homepage with a warning message in Slovak. 'Page Statistics' are also visible.

urlscan.io Home Search Live API Blog Docs Pricing Login

Sponsored by SecurityTrails A Recorded Future Company

www.google.sk

2a00:1450:4001:808::2003

URL: <https://www.google.sk/?hl=sk>

Submission: On February 07 via manual (February 7th 2023, 5:29:48 am UTC) from — Scanned from

Summary HTTP 12 Redirects Links 13 Behaviour Indicators Similar DOM Content API Verdicts

Summary

This website contacted **5 IPs** in **2 countries** across **3 domains** to perform **12 HTTP transactions**. The main IP is **2a00:1450:4001:808::2003**, located in **Frankfurt am Main, Germany** and belongs to **GOOGLE, US**. The main domain is **www.google.sk**. The Cisco Umbrella rank of the primary domain is **31014**.
TLS certificate: Issued by **GTS CA 1C3** on January 9th 2023. Valid for: 3 months.

www.google.sk scanned **121 times** on urlscan.io [Show Scans 121](#)

urlscan.io Verdict: **No classification**

Live information

Google Safe Browsing: No classification for www.google.sk
Current DNS A record: **142.250.186.35 (AS15169 - GOOGLE, US)**

Screenshot

[Live screenshot](#) [Full Image](#)

Než prejdete na Google

Pretože ste vybrali jazyk Google, ktorý nie je v zozname jazykov, ktoré podporujeme, možno budete musieť použiť angličtinu.

Google

Page Statistics

Otestujte URL adresu: <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 nestahujte 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:

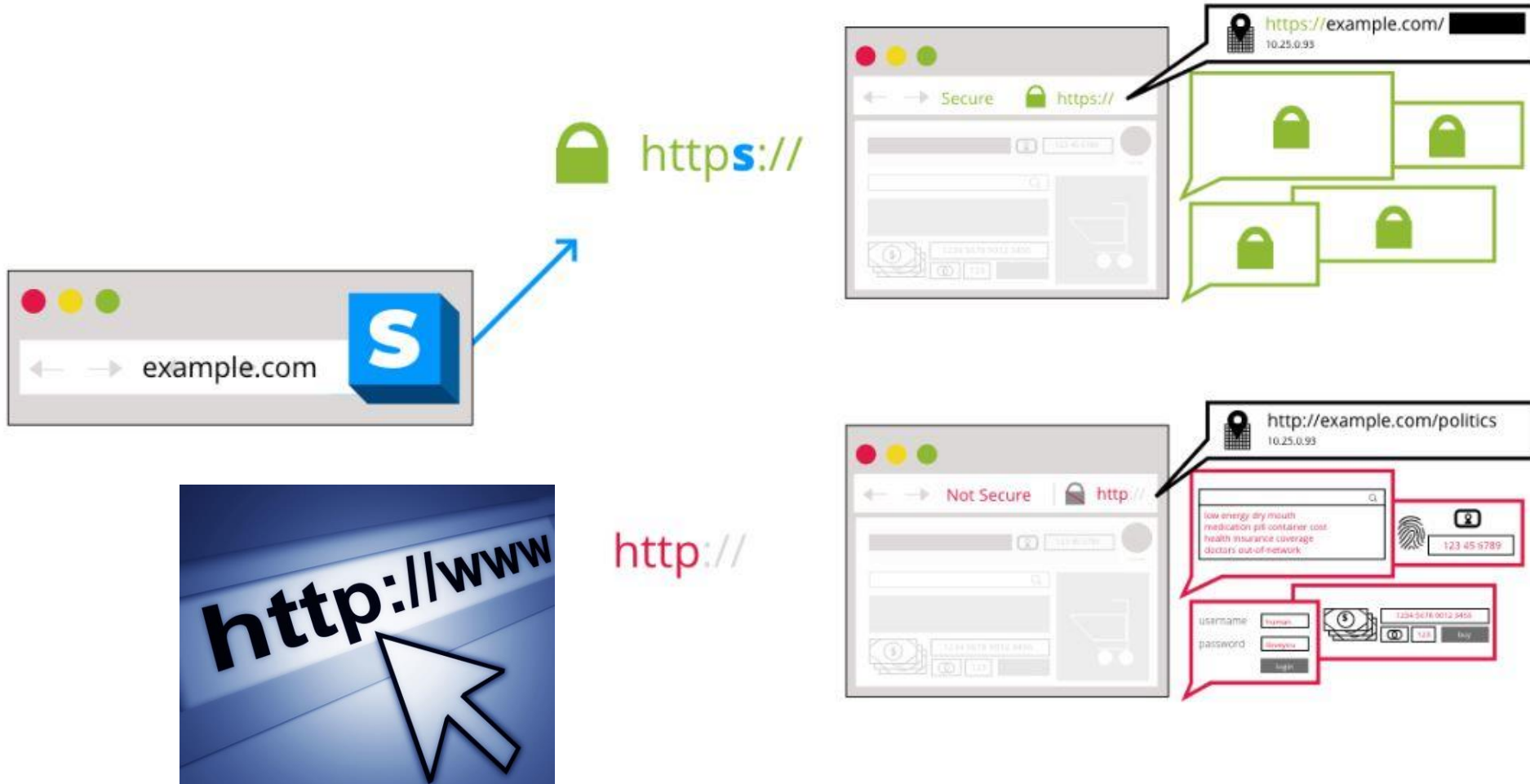
- ✓ Majte aktuálne verzie softvérov!
- ✓ Nenaletzte na super ponuky!
- ✓ Nakupujte u overených obchodníkov!

HTTP vs HTTPS

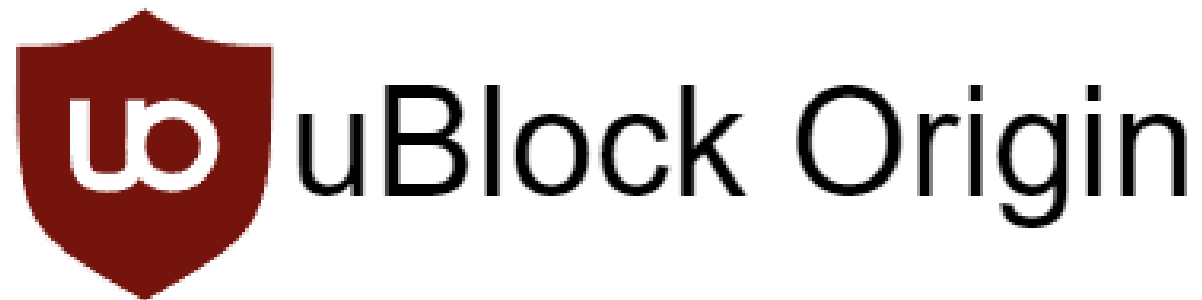
Webové stránky



https://Everywhere

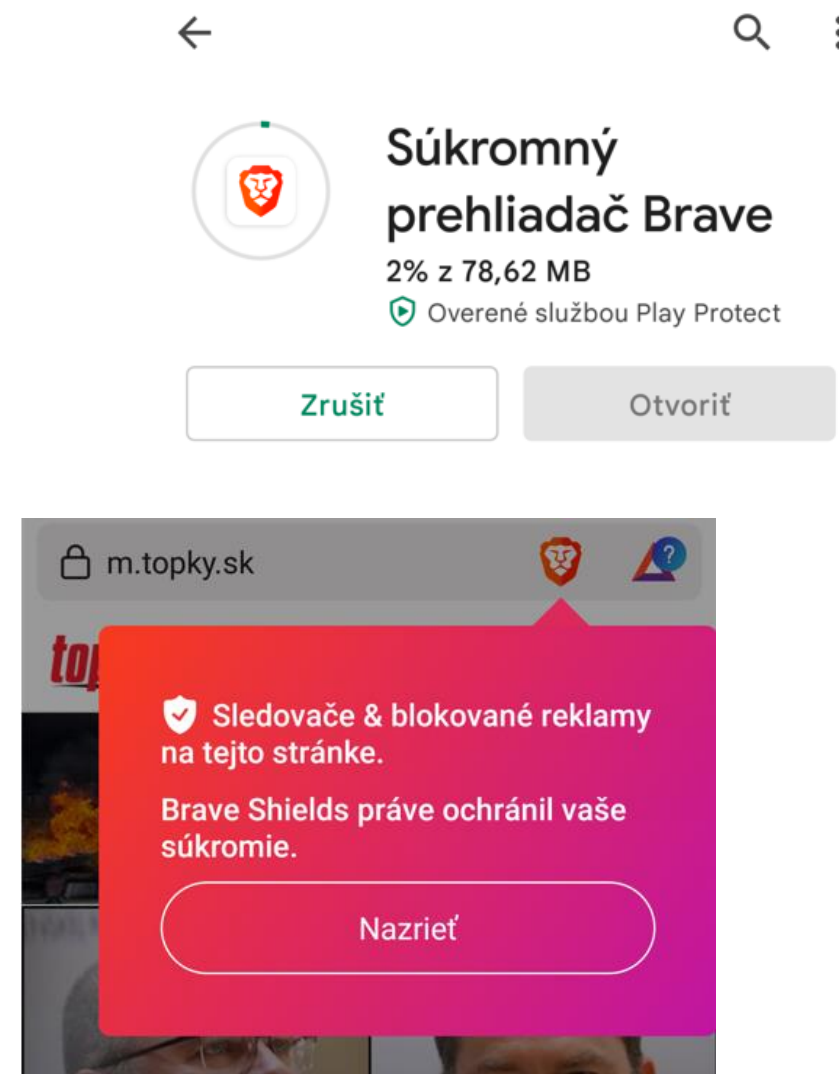
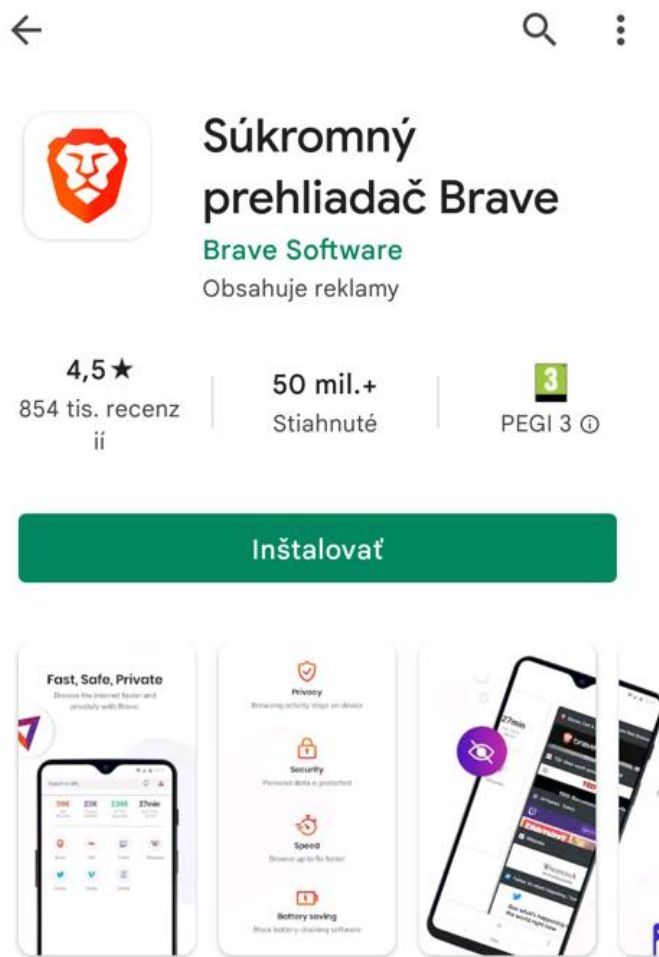


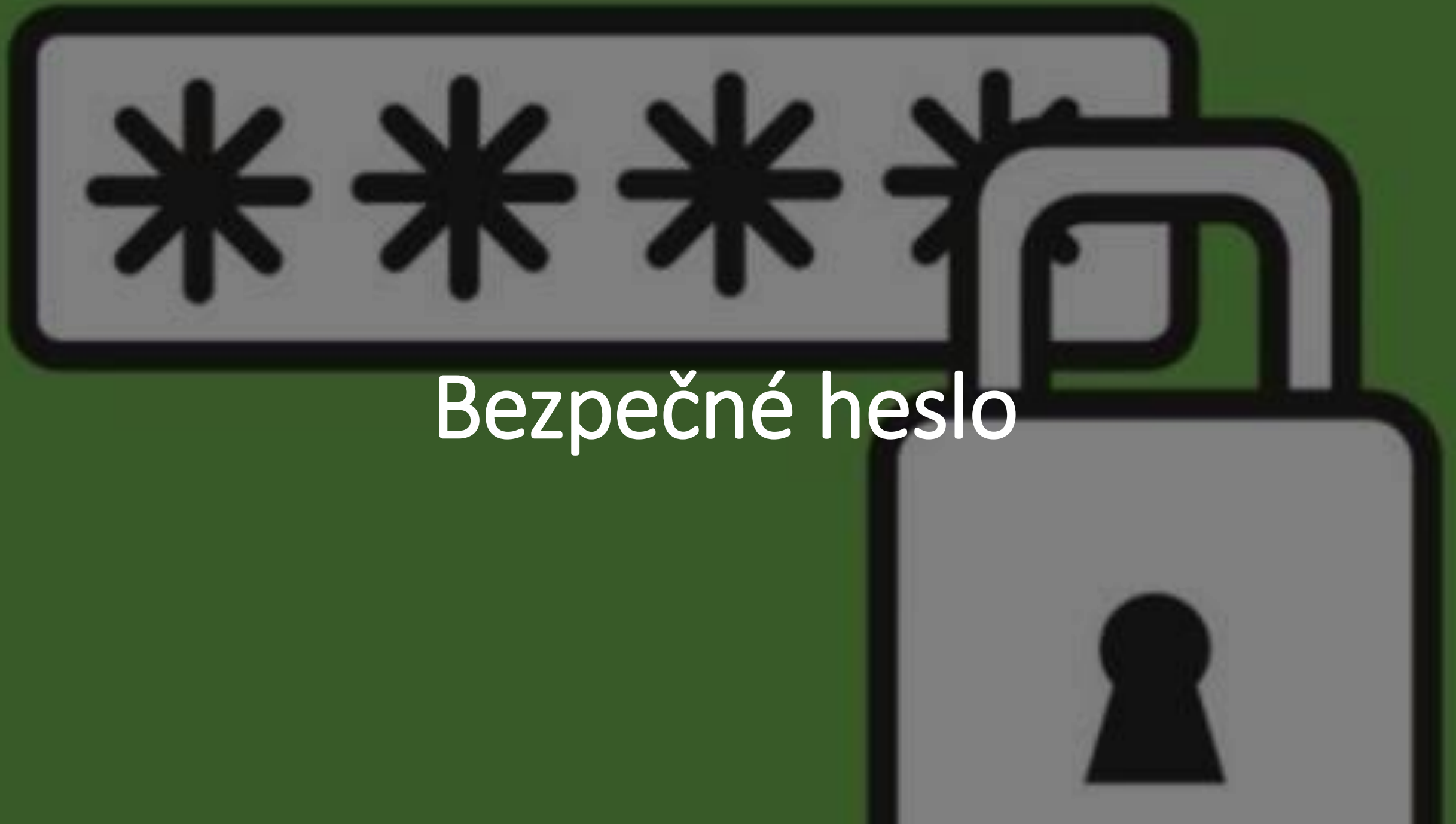
Blokovanie reklám v prehliadači



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

Prehliadač BRAVE – blokuje reklamy

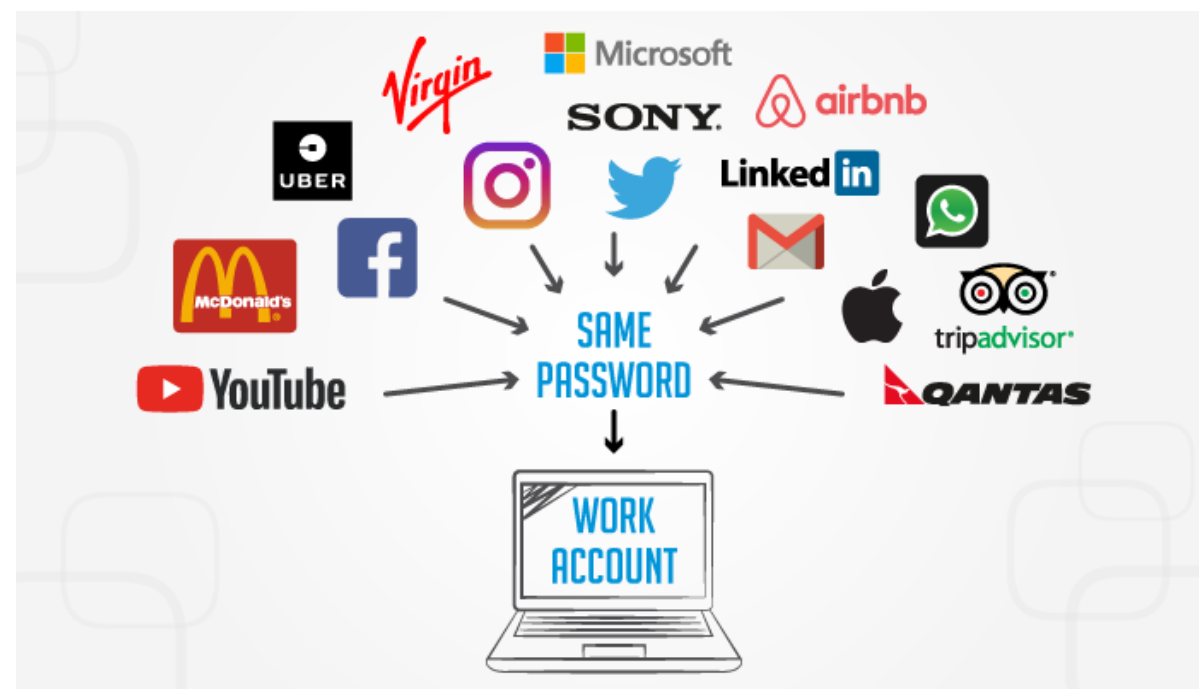
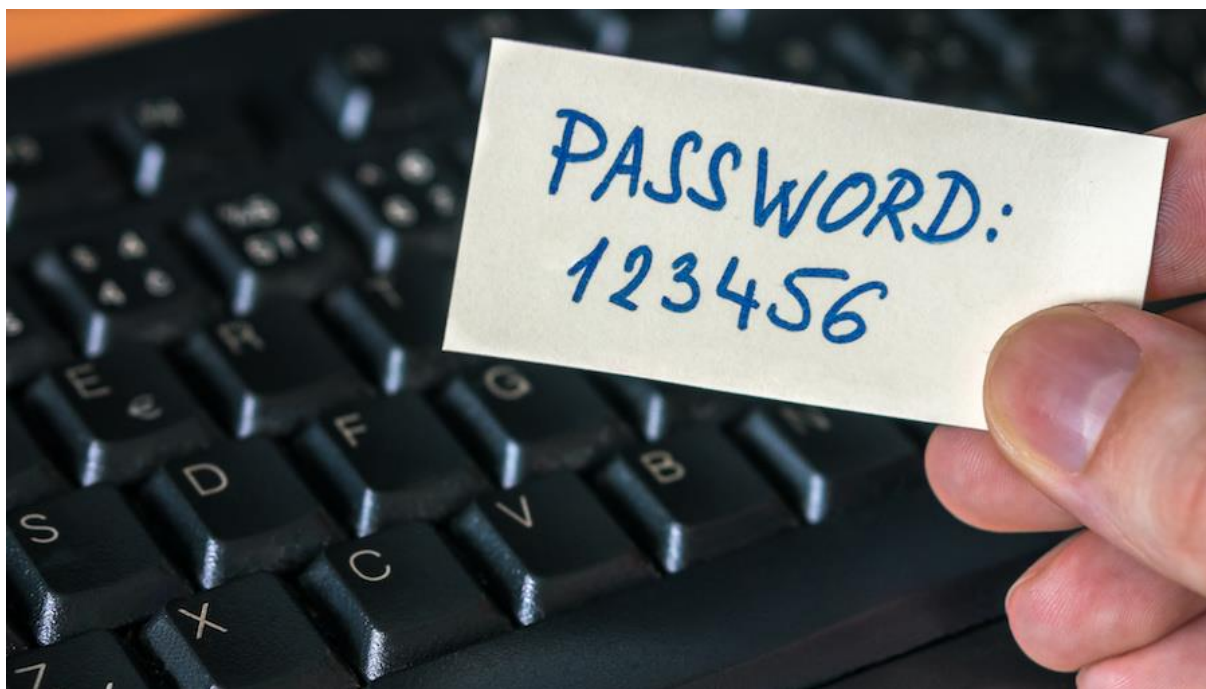




Bezpečné heslo

Heslo – časté chyby

- slabé heslá
- rovnaké heslá na viacerých účtoch



Bezpečné heslo

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



Ako bezpečné je Vaše heslo?



Otestujte silu hesiel:

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

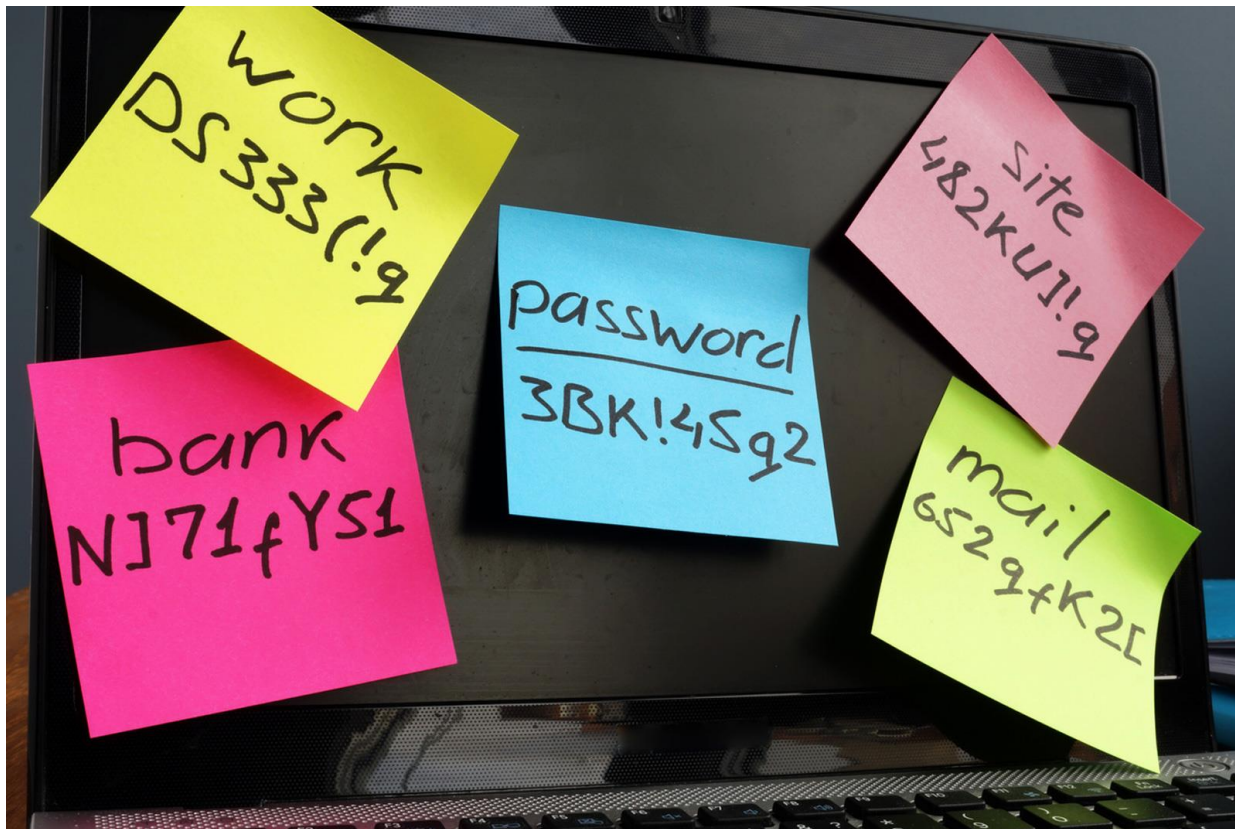


Bezpečné heslo

- 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

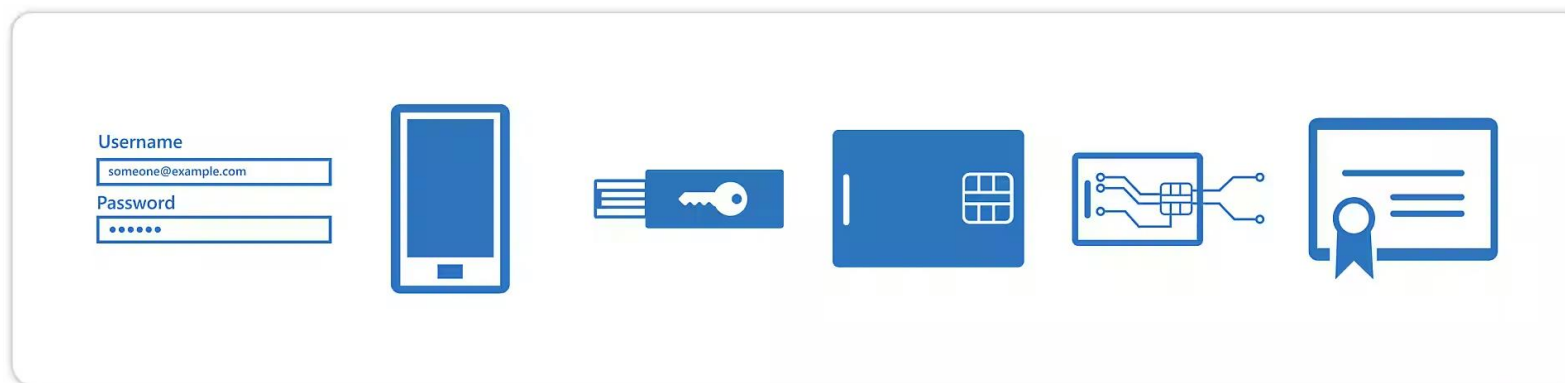


Multifaktorová autentifikácia

- viacfaktorové overovanie pridáva k prihlasovaciemu procesu ďalšiu vrstvu ochrany,
- pri získavaní prístupu ku kontám alebo aplikáciám používateľa využívajú ďalšie overenie identity:

skenovanie odtlačku prsta

zadávanie kódu prijatého cez telefón.





2-Step Verification

This extra step shows it's really you trying to sign in

 [blurred]@gmail.com ▾



Check your Google Pixel 2

Google sent a notification to your Google Pixel 2. Tap **Yes** on the notification to continue.

Or open the Gmail app on your Apple iPad mini (5th generation) to sign in from there.

Don't ask again on this device





Úniky údajov

Úniky údajov

';--have i been pwned?

Check if your email or phone is in a data breach

email or phone (international format)

pwned?



<https://haveibeenpwned.com/>

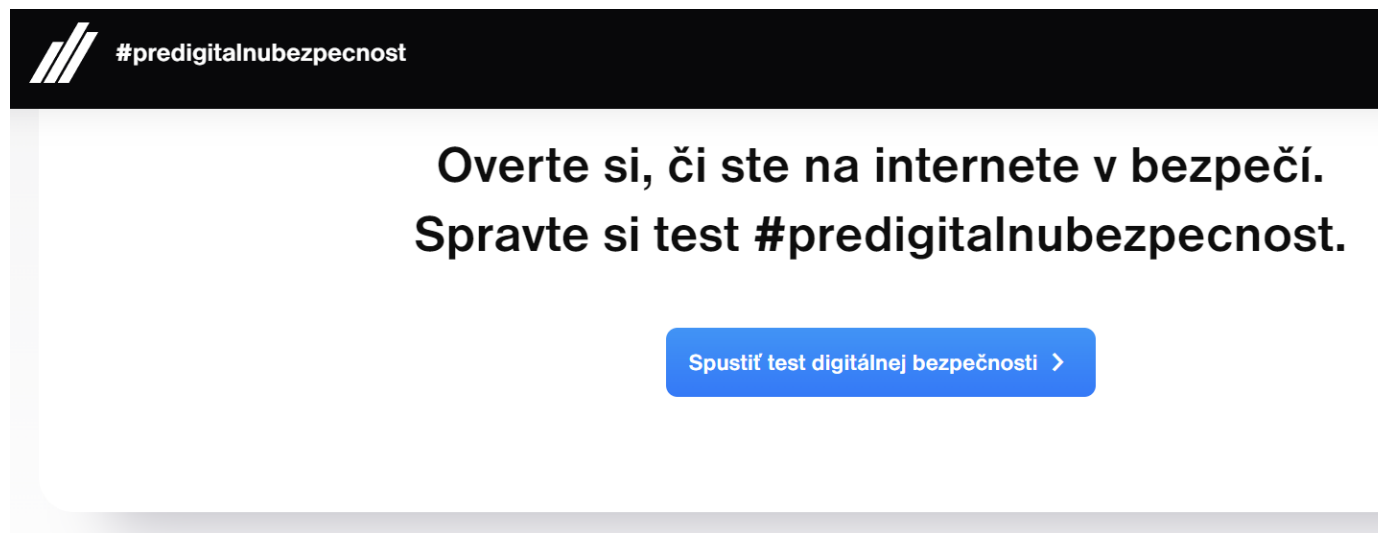
Bezpečnosť mobilu

Bezpečnosť webového prehliadača



Test digitálnej bezpečnosti

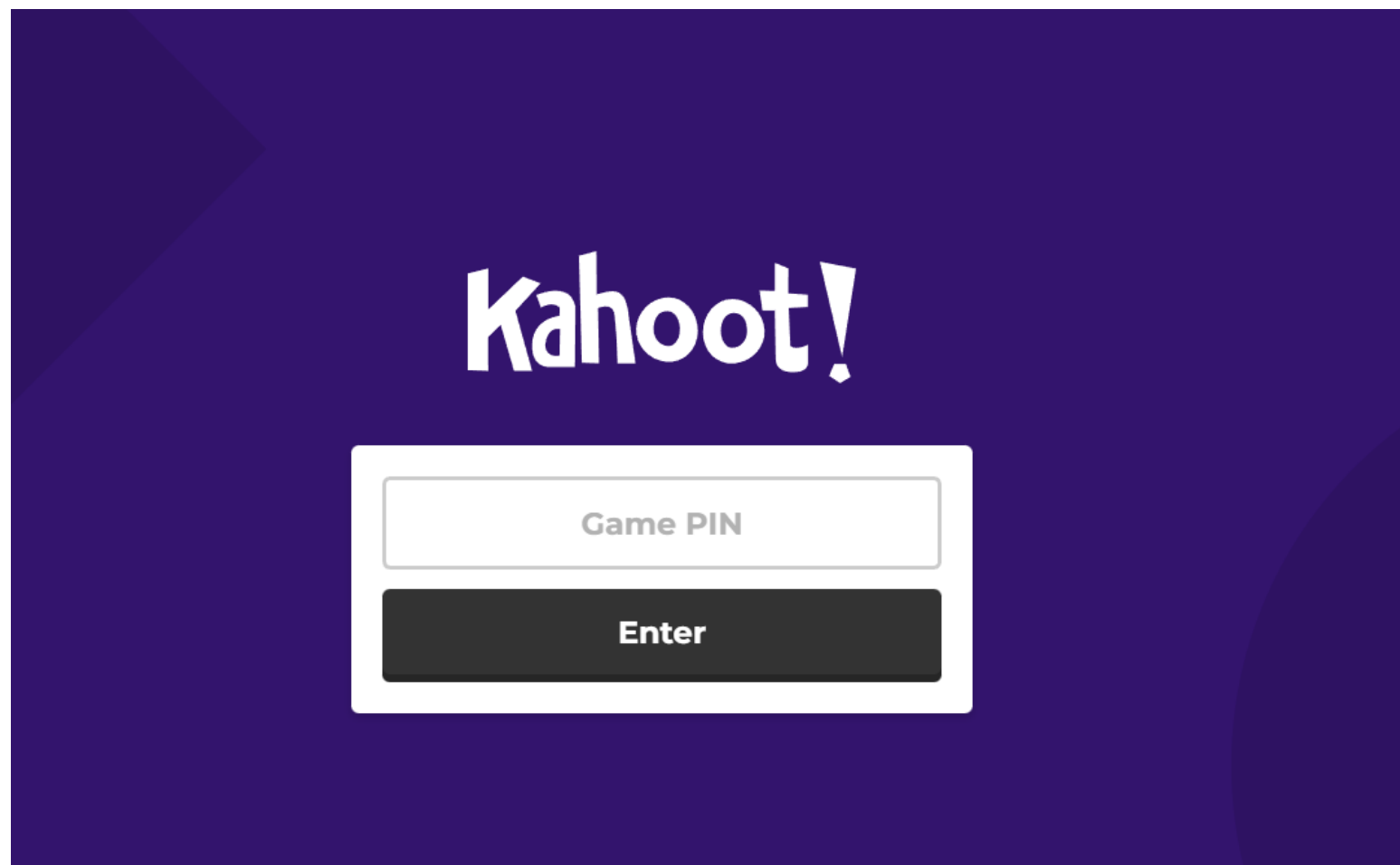
https://www.tatrabanka.sk/predigitalnubezpecnost/test-digitalnej-bezpecnosti/?utm_source=SilverpopMailing&utm_medium=email&utm_campaign=16687255&utm_content=spustit_test&mktid=874F4C0D08322FF2867D8C9FAA1D5FF0



The image shows a promotional banner for a digital security test. At the top left, there is a logo consisting of three slanted parallel lines followed by the hashtag #predigitalnubezpecnost. The main text in the center reads: "Overte si, či ste na internete v bezpečí. Spravte si test #predigitalnubezpecnost." Below this text is a blue button with the text "Spustiť test digitálnej bezpečnosti >".

Kvíz


<https://kahoot.it/>



Spätaná väzba

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



 Informačná bezpečnosť - dotazník

Tento formulár slúži na vyhodnotenie podujatia Informačná bezpečnosť 22.12.2022 a spätnú väzbu.

* Povinná

1. Bol tento workshop pre vás prínosný? *

áno
 nie
 aniem

2. Ako celkovo hodnotíte dňový workshop? *

☆☆☆☆

3. Mali by ste záujem o ďalšiu prednášku z informačnej bezpečnosti? *

áno
 nie

4. Ak ste v predchádzajúcej otázke odpovedali áno, označte témy, o ktorých by ste sa chceli dozvedieť viac:

phishing
 mobil
 ako fungujú online platby
 bezpečnosť osobných
 bezpečnosť prehládania
 čo si všimnúť pri kúpe mobilu?

5. Sem napíšte ďalšie témy, ktoré by Vás zaujímali:

Začítajte svoju odpoveď

6. Ak nám chcete ešte niečo napísať, čo nebolo v predchádzajúcich otázkach:

Začítajte svoju odpoveď

Odoslať

Tento obsah je určený vlastným formulárom. Údaje ktoré odobrem, sa odobrá vlastným formulárom. Spoločnosť Microsoft nepodporuje ani zdieľať ochranu osobných údajov alebo zabezpečenie svojich zákazníkov vrátane zdieľania údajov z tohto formulára. Nikomu nikdy nevydajte svoje heslo.

Podlaha Microsoft Formy |
Všetky údaje formulára nepodliehajú vyhláseniu o poskytnutí osobných údajov v súvislosti s tým, ako bude používať údaje z vašich odpovedí.
Nepodliehajú ochrane ani ďalšiu informáciu.
[Zistiť viac o našich službách](#)

Spätná väzba

Vyplňte formulár - spätnú väzbu:

Domov dôchodcov:

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

ZPP Radost':

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

ZŠ:

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

A screenshot of a Microsoft Forms survey titled 'Informačná bezpečnosť - dotazník'. The survey is in Slovak and contains five questions. Question 1 asks if the workshop was interesting, with radio buttons for 'áno', 'nie', and 'aniem'. Question 2 asks for a rating of the workshop, with five star icons. Question 3 asks if the respondent is interested in further topics on information security, with radio buttons for 'áno' and 'nie'. Question 4 asks for topics to be covered in a future workshop, with radio buttons for 'pláškiny', 'mobil', 'ako fungujú online platby', 'bezpečnosť mobilu', 'bezpečnosť prehládania', and 'čo si všímať pri kúpe mobilu?'. Question 5 asks for other topics of interest, with a text input field. Question 6 asks for additional comments, also with a text input field. At the bottom, there is a blue 'Odoslať' button and a footer with legal disclaimers and a 'Dotazník používajú' link.



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!

