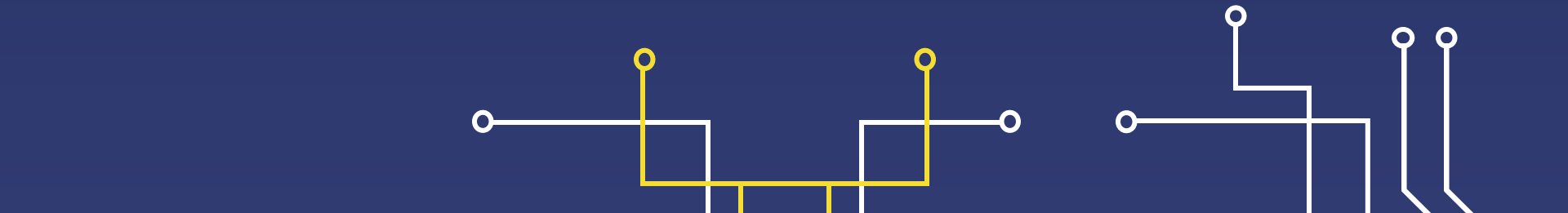


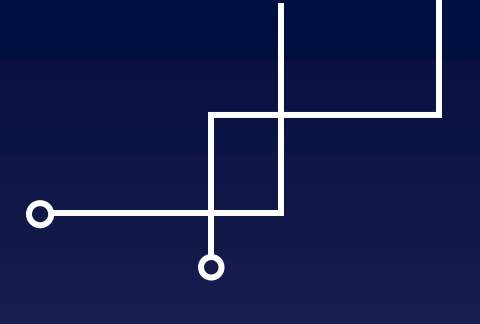
Kybernetický tým GKMKE

Počítačová bezpečnost'

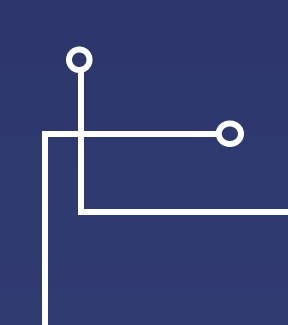


Spojená škola sv. Košických mučeníkov



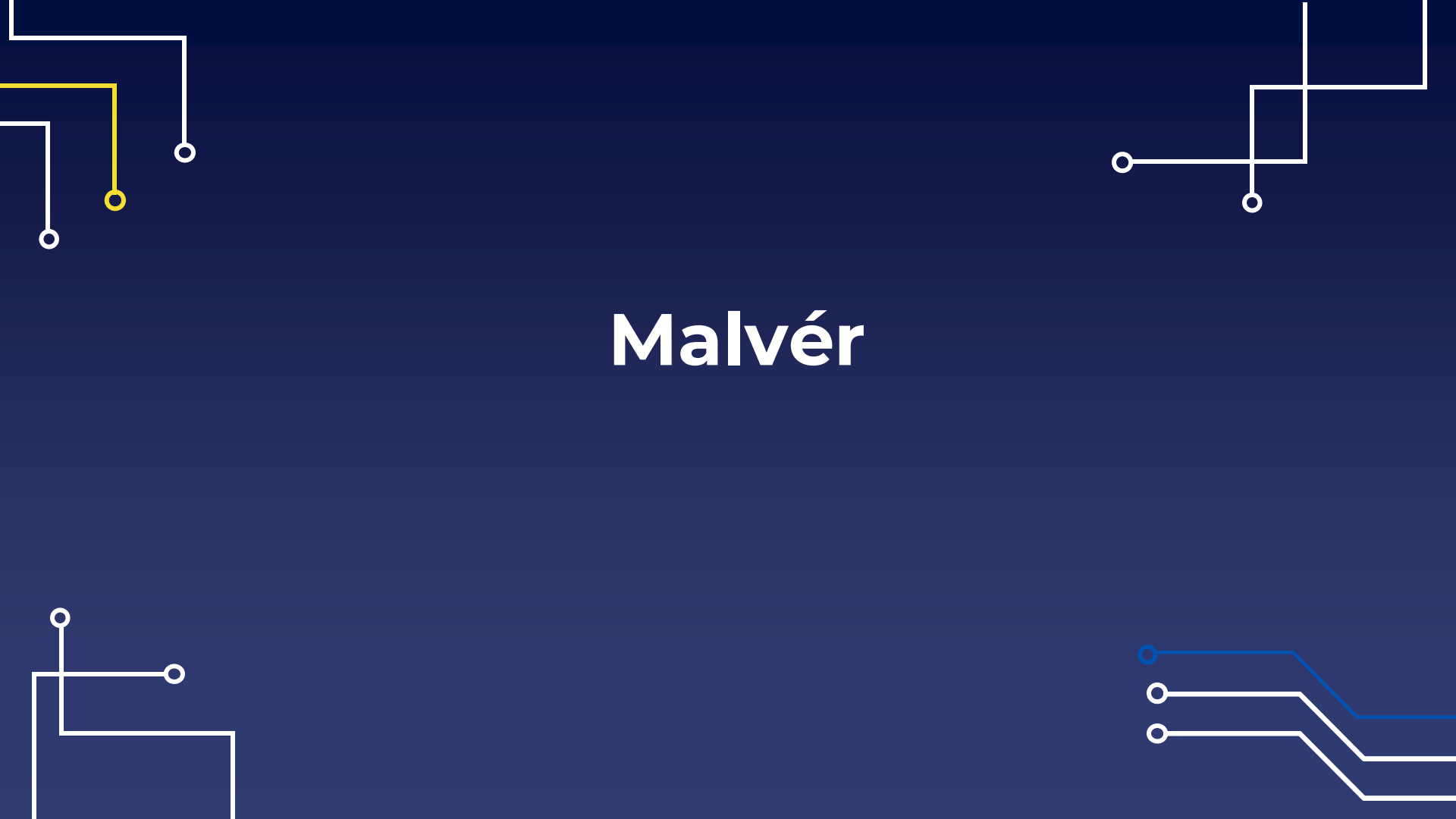


Sociálne inžinierstvo



Sociálne inžinierstvo

- Umenie manipulácie ľudí za účelom vykonania akcie alebo vyzradenia dôverných informácií.

The image features a dark blue background with the word "Malvér" centered in a white, bold, sans-serif font. The corners of the image are decorated with stylized circuit board traces. In the top-left, a white trace leads to a white circle, and a yellow trace leads to a yellow circle. In the top-right, a white trace leads to a white circle. In the bottom-left, a white trace leads to a white circle. In the bottom-right, a blue trace leads to a blue circle, and two white traces lead to white circles.

Malvér

MALWARE



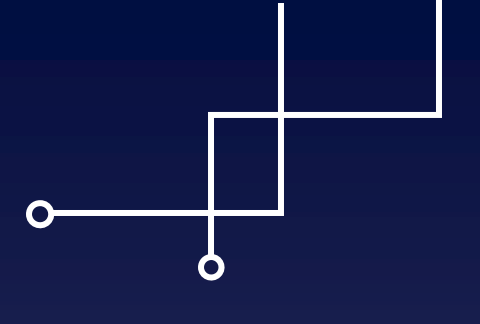
- zahŕňa všetky druhy škodlivého softvéru vrátane najznámejších foriem, ako sú **trójske kone**, **ransomware**, **vírusy**, **červy** a **bankový malvér**
- ukradnúť alebo zašifrovať citlivé údaje, ktoré môže prediť alebo vymáhať finančnú čiastku od obete



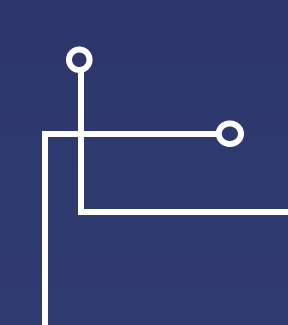
58% 
zo všetkých e-mailov je spam

77% 
zo všetkých spamov obsahuje
škodlivý obsah (malware)





Phishing



PHISHING

- pokus o podvodné získanie citlivých informácií, ako sú heslá a podrobnosti o kreditných kartách, maskovaním sa za dôveryhodnú osobu alebo obchod pri elektronickej komunikácii



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

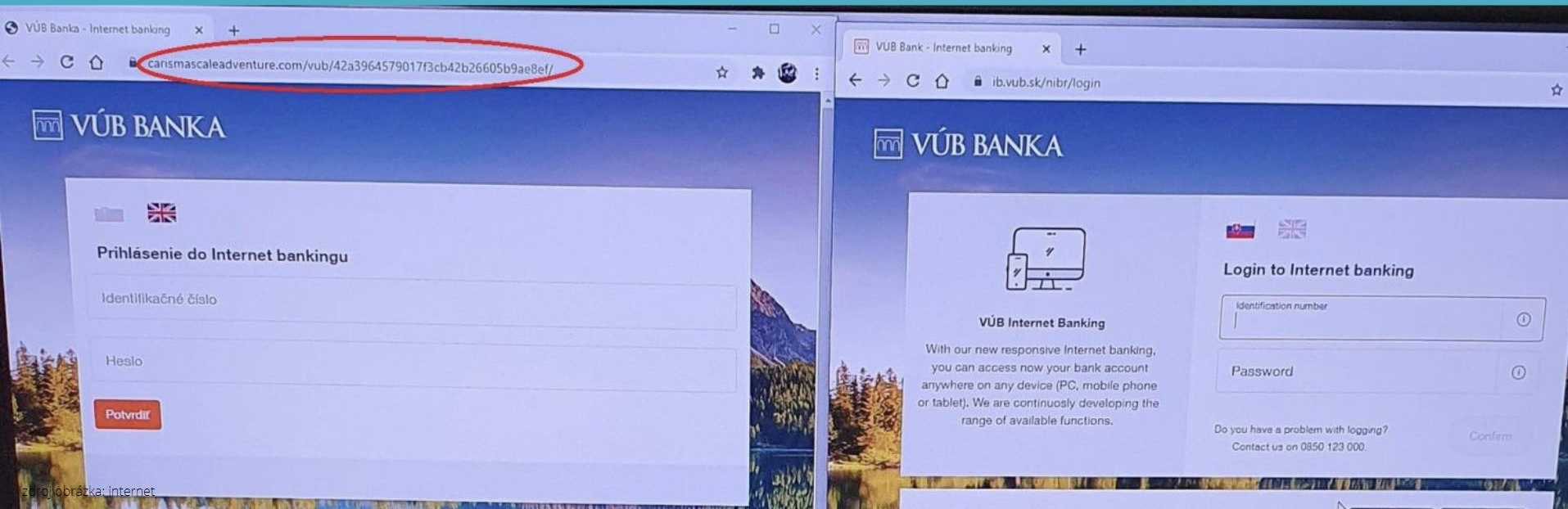


ZNAKY

- útočník vystupuje pod nejakou inštitúciou (banka, pošta)
- nevhodné oslovenie
- slabá jazyková úroveň
- žiadosť o osobné informácie
- pocit naliehavosti
- podozrivá doména



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





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 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:

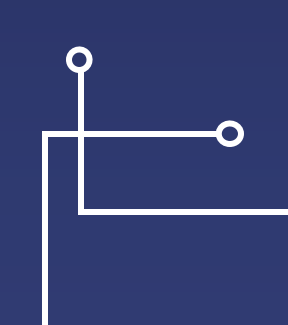
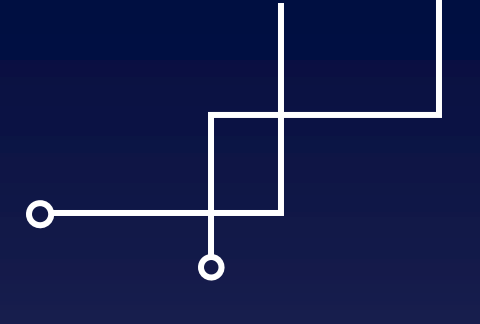
Kontaktná osoba: pán David M. Wehner, finančný riaditeľ európskeho regiónu UK

* 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

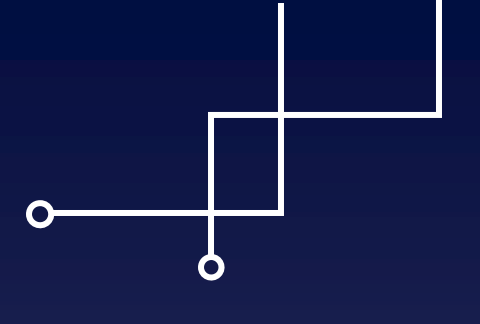


Vishing

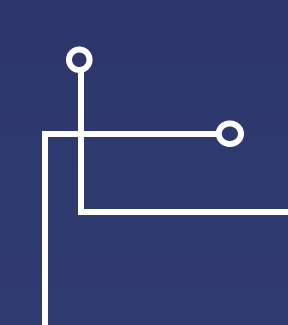
VISHING

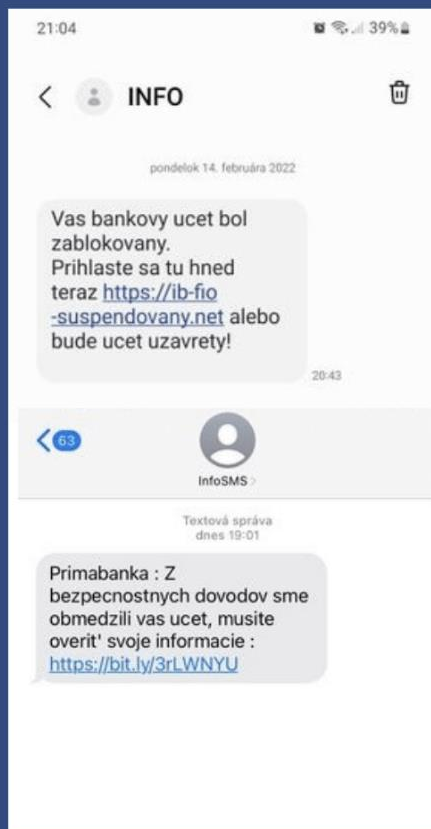
- ohrozené zabezpečenie vášho počítača
- bola zistená podozrivá transakcia
- osobné údaje, prístupové heslá do Internetbankingu, čísla platobných kariet a pod.





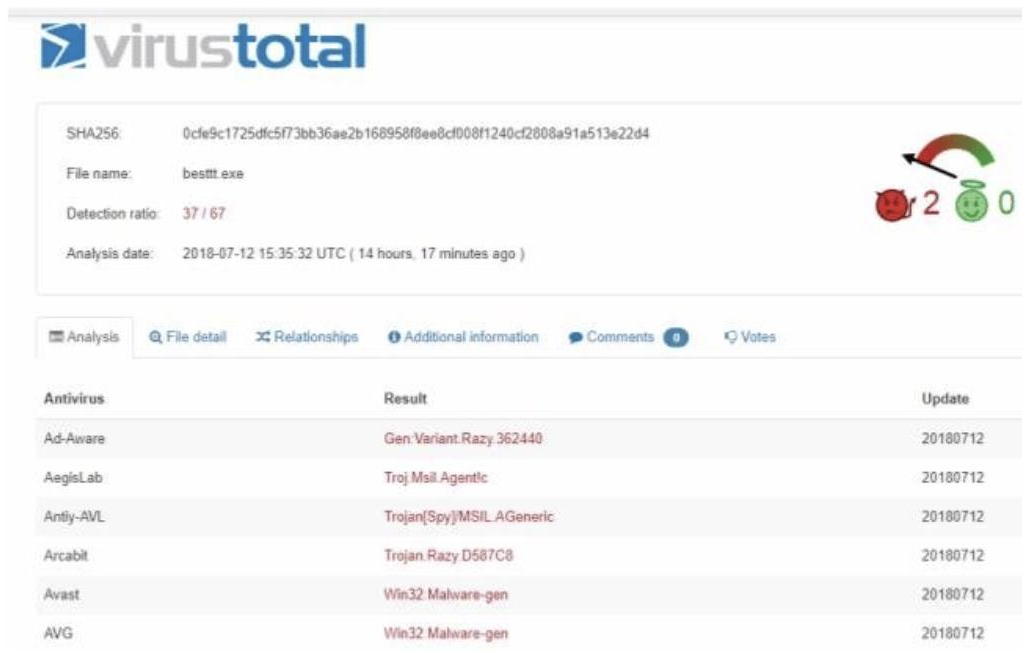
Smishing





- **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

- <https://virustotal.com>
- <https://haveibeenpwned.com/>



The screenshot shows the VirusTotal interface for a file analysis. At the top is the VirusTotal logo. Below it, the file's SHA256 hash is 0cfe9c1725dfc5f73bb36ae2b1689508ee8cf008f1240cf2808a91a513e22d4. The file name is 'besttt.exe'. The detection ratio is 37 / 67, and the analysis date is 2018-07-12 15:35:32 UTC (14 hours, 17 minutes ago). To the right of this information is a circular progress indicator with a red arrow pointing to the number 2, and a green circle with the number 0. Below this, there are tabs for Analysis, File detail, Relationships, Additional information, Comments (4), and Votes. The main section is a table with three columns: Antivirus, Result, and Update. The table lists several antivirus engines and their results for the file.

Antivirus	Result	Update
Ad-Aware	Gen.Variant.Razy.362440	20180712
AegisLab	Troj.Msil.Agentlc	20180712
Antiy-AVL	Trojan[Spy]MSIL.AGeneric	20180712
Arcabit	Trojan.Razy.D587C8	20180712
Avast	Win32.Malware-gen	20180712
AVG	Win32.Malware-gen	20180712

Bezpečné heslo



Otestujte bezpečnosť niektorých hesiel:

hesla.csirt.upjs.sk

1. heslo
2. 1234
3. mamRADcokoladu+čipsy
4. 0808200417
5. kybertímGKMKE
6. N1dT1trouS1Bl2sk1!



Bezpečné heslo obsahuje:

- **Minimálne 12 znakov**
- **Veľké aj malé písmená**
- **Čísla**
- **Špeciálne znaky**
- **Čím je heslo náhodnejšie, tým je bezpečnejšie!**

Heslo sa:

- **Neskladá z osobných údajov!**
- **S nikým nezdieľa!**

Zdroje:

<https://sk.wikipedia.org/wiki/Phishing>

<https://www.eset.com/sk/phishing/>

<https://www.eset.com/sk/malver/>

<https://www.slsp.sk/sk/ludia/otazky-a-odpovede/co-je-vishing>

<https://sk.wikipedia.org/wiki/Botnet>

Ďakujeme za pozornost'

