

BEZPEČNOSŤ NA INTERNETE

ŽIACI GYMNÁZIA, Ľ. ŠTÚRA 26,
MICHALOVCE



Sociálne inžinierstvo

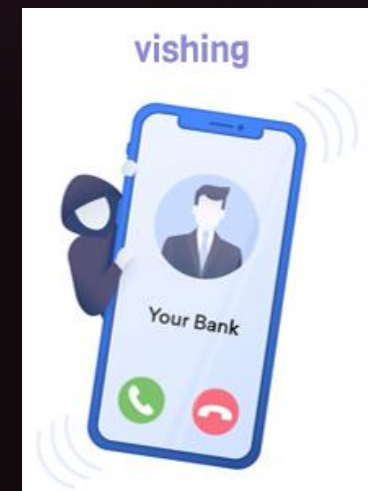
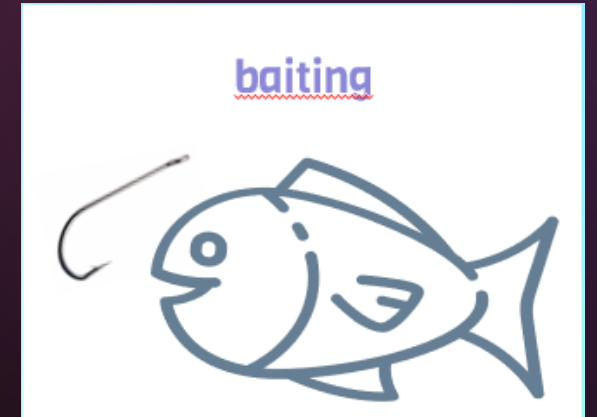
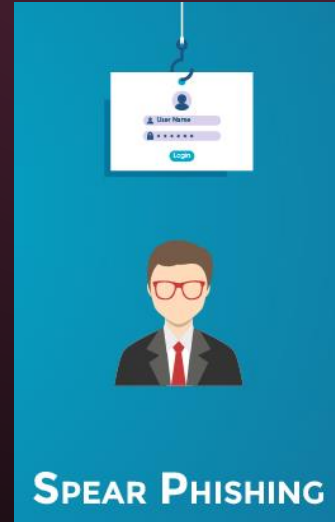


- Jeden z najefektívnejších nástrojov pre získavanie citlivých informácií zo zabezpečených systémov
- Útok založený na schopnosti ovplyvňovania a manipulácie ľudí
- Základným stavebným kameňom sociálneho inžinierstva je dôvera
- **Ciele:**
 1. získať citlivé osobné informácie
 2. získať prihlasovanie údaje
 3. spustiť škodlivý kód

Viete vymenovať
nejaké typy
útokov/príklady na
útoky?



Odpoved' 😊



Niečo o útokoch

- **Phishing**

- email je koncipovaný tak, aby pôsobil dôveryhodne

- **Spear phishing**

- **cielený útok** na osobu alebo organizáciu s cieľom získania dôverných informácií za účelom vykonania podvodu

- **Baiting**

- využitie nastrčených infikovaných návnad (dátových médií): USB, DVD
- z nosiča sa nainštaluje škodlivý kód

- **Vishing**

- podvodný postup s využitím telefonického rozhovoru, pomocou ktorého sa útočník snaží od obete získať citlivé údaje

- **SMiShing**

- podvodná správa realizovaná cez SMS
- SMS phishing môže byť podporovaný malvérom alebo webovými stránkami



Ochrana osobných údajov

- Osobné údaje sú citlivé informácie, ktoré slúžia k identifikácii osoby a spracovávať sa môžu len s jej súhlasom
- Každý má právo na ochranu pred neoprávneným zasahovaním do súkromného a rodinného života

Ktoré osobné
údaje si treba
chrániť na
internet?



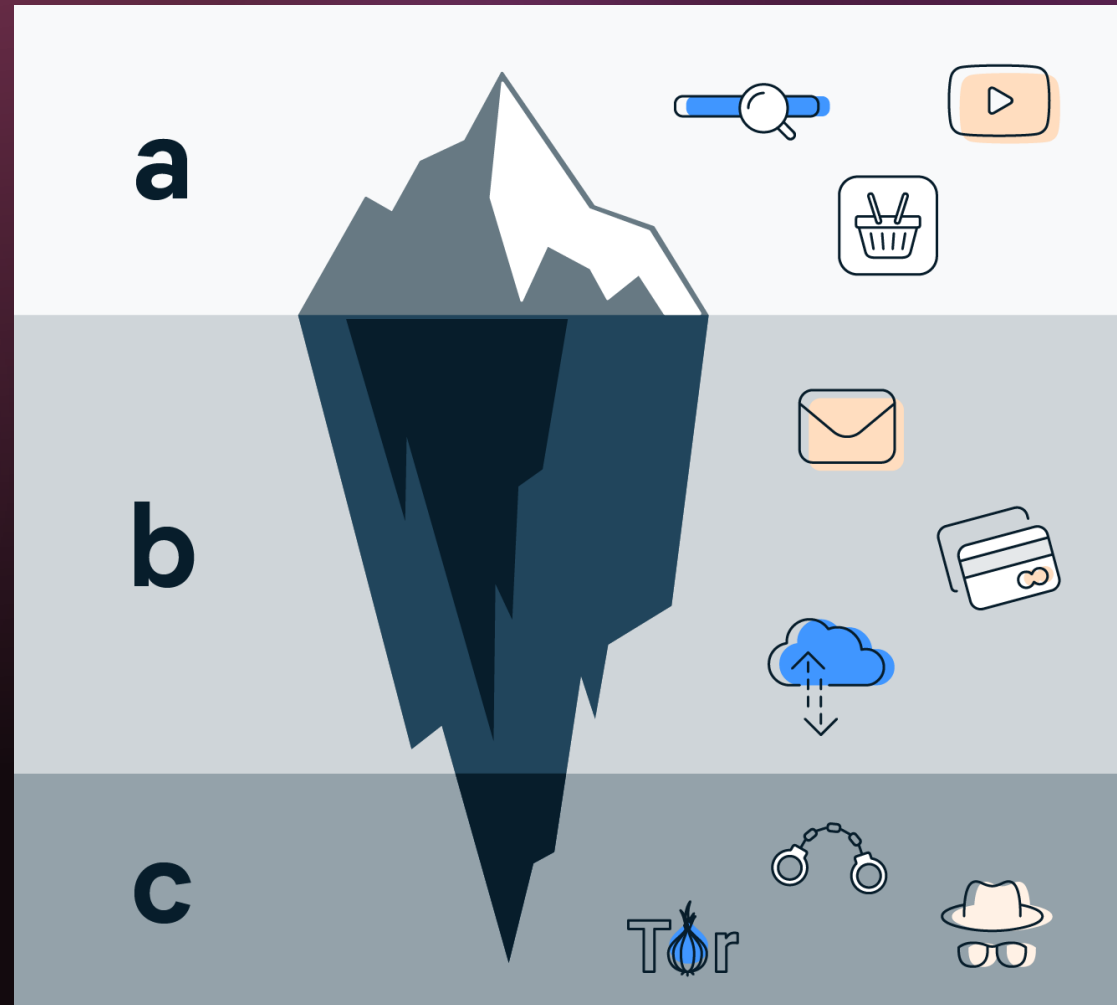
Akým spôsobom sa dostávajú údaje k „nechceným“ adresátom

- Prostredníctvom emailov, SMS správ, zverejnením na chatoch a internetových fórach, zadaním na webových stránkach, zverejnením v profiloch, na sociálnych sieťach, na stránkach na zverejňovanie fotografií a videí.
- Vaše údaje sa k nepovolaným ľuďom môžu dostať aj sprostredkovane, napr. vašu fotografiu uverejní váš kamarát, vašimi majetkovými pomermi sa pochváli cez internet vaše dieťa



Ako môžu byť údaje zneužit

- „Nabúranie“ do profilu, zneužitie profilu, emailovej schránky
- Krádeže
- Zneužitie fotografií
- Vydieranie, pomsta, šikanovanie
- Sexuálne obťažovanie, zneužitie



Viete ako si
najlepšie
chrániť
súkromie?

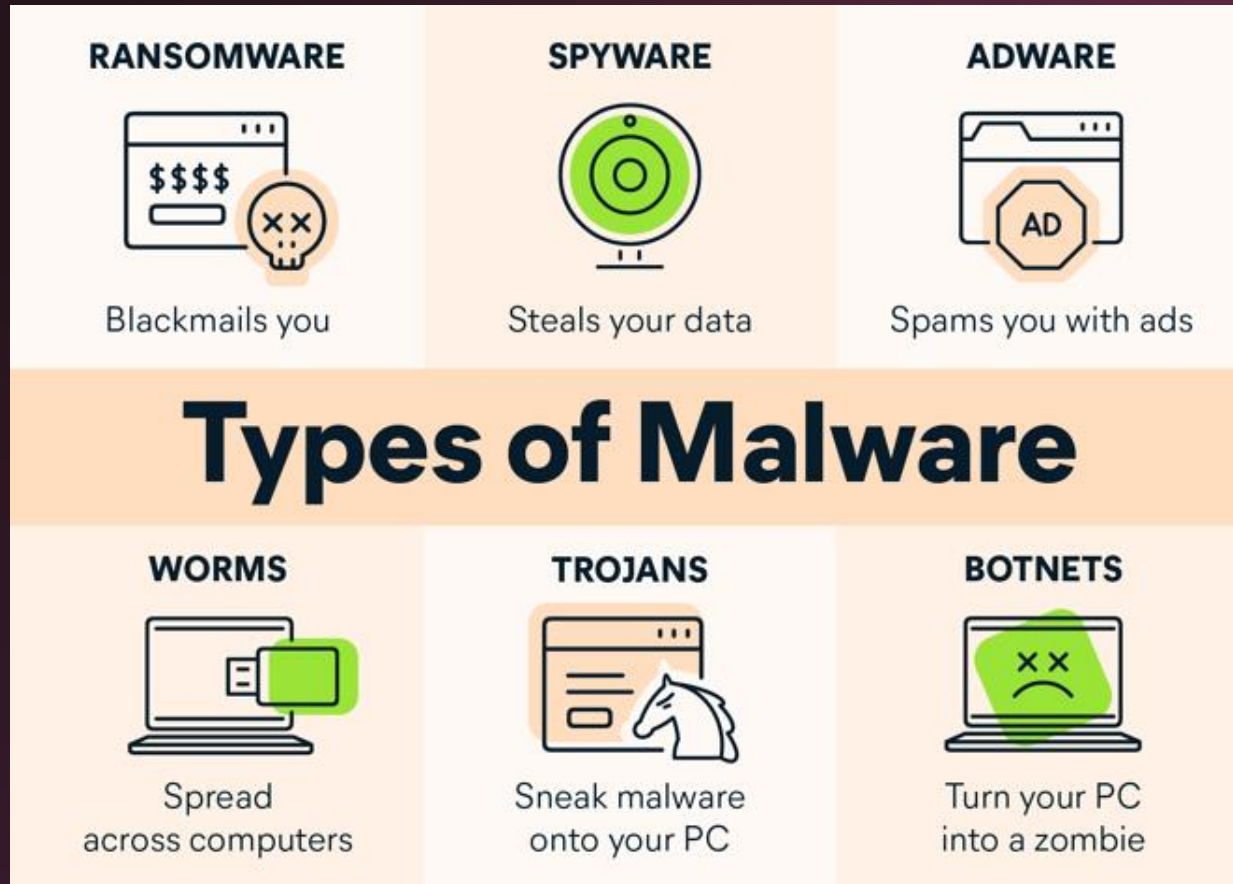




Odpoved' 😊

- Nezverejňovať adresu, kde bývate, mať silné hesla na sociálnych sieťach, nemať všade to isté heslo!
- Nezverejňuj na internet veci, ktoré môžeš o niekoľko rokov ľutovať!
- Zapamätaj si pravidlo internetu: čo tam raz zverejníš, to tam ostane navždy!

Malware (Malvér)



- Škodlivý softvér, ktorý obyčajne poškodí alebo zablokuje, zmocní sa alebo odcudzí informácie z počítačového systému
- Malware sa do počítača v dnešnej dobe dostáva zvyčajne cez Internet, hlavne pri prezeraní škodlivých stránok s nie dobre zabezpečeným systémom
- Napr: vírus, červ, trójsky kôň, logická bomba, rootkit, bootkit, backdoor, spyware atď...

Ako mať to najlepšie heslo

Heslo by nemalo obsahovať:

1. Mená domácich zvieratiek, kamarátov atď...
2. Čisto len dátum narodenia
3. Nemalo by byť zložené LEN z malých písmen

Ako vytvoriť to najbezpečnejšie heslo?

1. Malo by mať najmenej 8 znakov, ale čím viac tým lepšie
2. Ideálne je použiť aj veľké aj malé písmena, číslice a iné znaky
3. A najlepšie je použiť slová v nárečí 😊



Zaujímavosti

Linky na stránky

- Unikol môj email na internet? - <https://haveibeenpwned.com/>
- Test aké silné heslo máš - <https://www.passwordmonster.com/>
- Overovanie stránok - <https://transparencyreport.google.com/safe-browsing/search?url=https:%2F%2Fwww.zodpovedne.sk%2Findex.php%2Fsk%2Fohrozenia%2Fzneuzitie-osobnych-udajov&hl=sk>

Zdroje

- <https://www.zodpovedne.sk/index.php/sk/ohrozenia/zneuzitie-osobnych-udajov>
- <https://www.csirt.gov.sk/socialne-inzinierstvo.html>

Ďakujeme za pozornosť!

