

Dvakrát meraj a raz rež!

Hackeri maskujú phishingové odkazy a podvodné reklamy ako dôveryhodné zdroje, aby ťa oklamali.



Hackeri používajú zlé odkazy, aby sa dostali do tvojich zariadení, ako je...



Tablet



Mobil



Počítač

Keď sa dostanú dovnútra, môžu...

Špehovať ťa



Dostať sa k fotoaparátu



Poškodiť zariadenie



Ukradnúť informácie



... a viac

K zlým odkazom sa môžeš dostať cez



Webstránky



Vyhľadávače



Textové správy



E-maily



Príspevky na sociálnych sieťach



Súkromné správy (DMs)



Ochrániš sa tak, že si vybuduješ správne kyber-návyky.

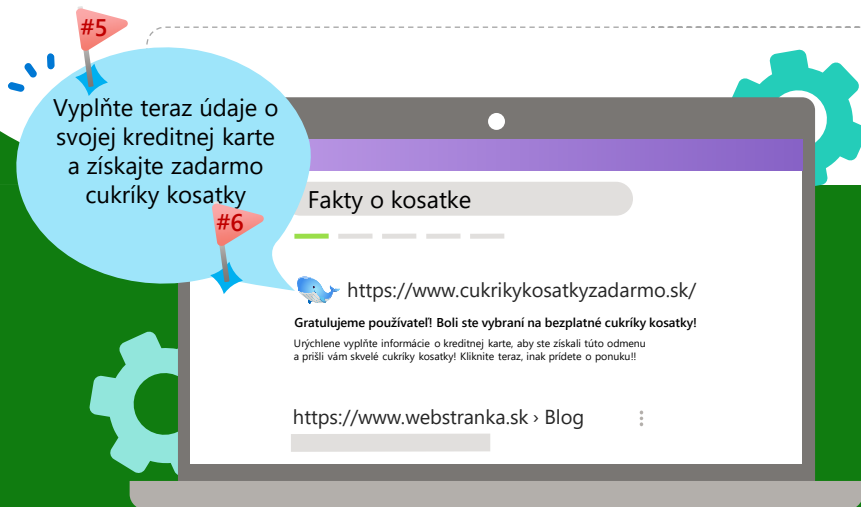
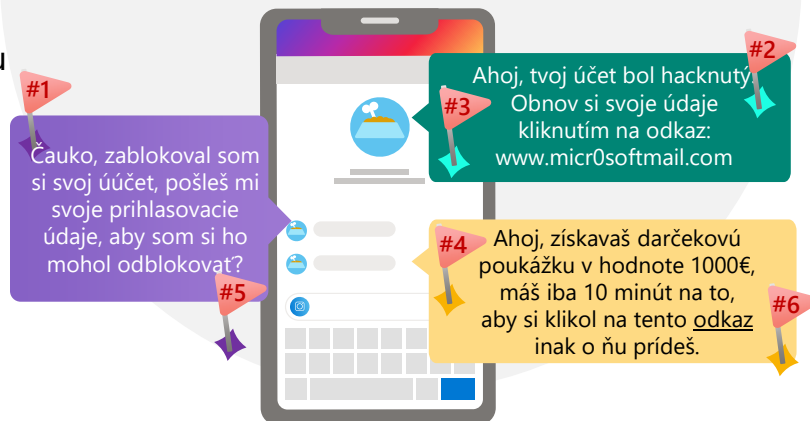


Pozri si najbežnejšie phishing taktiky

Čo je phishing? Použitie falošných správ alebo nebezpečných odkazov na pokus o krádež informácií o tebe!

- #1 Preklepy alebo chyby v texte správy
- #2 Nesprávne alebo podozrivé kontaktné informácie
- #3 Odkaz (alebo e-mail odosielateľa) naodkazuje na miesto, ktoré očakávaš

- #4 Správa vyjadruje hrozbu a naliehavosť
- #5 Žiada ťa o poskytnutie súkromných informácií
- #6 Výhodné ponuky a ponuky s nereálnymi odmenami



Nie všetky neznáme odkazy sú pokusmi o phishing...
Môžu to byť aj podvodné reklamy - **scam**.

Ako zistíš, že ide o scam?

- Podvodné reklamy môžu vyzerat' ako skutočné reklamy, preto nepredpokladajte, že sú legitímne len preto, že majú značku "Reklama" alebo "Sponzorované"
- Môžu mať podobné varovné signály ako phishingová správa, napríklad žiadosť o osobné údaje a ponúkание odmien výmenou za ne

Phishing odkazy ti priamo pošlú, naopak nebezpečné reklamy **scam** môžeš nájsť kdekoľvek.

Ak dostaneš alebo otvoríš zvláštny odkaz:



Nesnaž sa to opraviť bez pomoci!



Okamžite to oznám rodičovi, zákonnému zástupcovi alebo učiteľovi.