

PHISHING A SOCIÁLNÍ INŽENÝRSTVÍ



1. Co je podle prezentace "Phishing"?

- a. Technika pro zrychlení vašeho internetového připojení.
- b. Podvodná technika, která se tváří jako legitimní komunikace s cílem ulovit citlivé údaje.
- c. Nová sociální síť pro rybáře.
- d. Bezpečnostní software, který chrání váš počítač.

2. Jak se nazývá podvodný útok využívající SMS zprávy nebo chatovací aplikace?

- a. Vishing
- b. Smishing
- c. E-mailový phishing
- d. Tailgating

3. Který z následujících bodů není podle prezentace typickým znakem phishingového e-mailu?

- a. Vytváření pocitu naléhavosti nebo strachu.
- b. Nabídka podezřele výhodné výhry.
- c. Dokonalá gramatika a stylistika bez jakýchkoliv chyb (díky AI to ale již nemusí platit).
- d. Oficiálně vypadající adresa odesílatele, která je ale ve skutečnosti odlišná od pravé domény (např. @ceska-sporitelna-admin.xyz).

4. Jak se nazývá technika sociálního inženýrství, kdy útočník vytvoří propracovaný příběh (legendu) a vydává se za autoritu, např. IT oddělení?

- a. Baiting
- b. Pretexting
- c. Tailgating
- d. Quid Pro Quo

5. Nalezení USB disku s nápisem "Mzdy učitelů_2025" na chodbě školy a jeho připojení do počítače ze zvědavosti je příkladem útoku:

- a. Baiting (návnada)
- b. Vishing
- c. Typosquatting
- d. Pretexting

