HESLA A AUTENTIZACE

1. **Jaká je podle prezentace doporučená minimální bezpečná délka hesla v dnešní době?**
   a. 8 znaků
   b. 10 znaků
   c. 12-15 znaků
   d. 6 znaků, pokud obsahují speciální symbol

2. **Která metoda dvoufaktorové autentizace (2FA) je považována za nejméně bezpečnou kvůli riziku tzv. "SIM swappingu"?**
   a. Autentizační aplikace (např. Google Authenticator)
   b. Hardwarové bezpečnostní klíče (např. YubiKey)
   c. SMS kódy
   d. Biometrika (otisk prstu)

3. **Jak primárně správce hesel chrání uživatele před phishingem?**
   a. Skenuje příchozí e-maily a maže podvodné zprávy.
   b. Automaticky vyplní heslo pouze na správné a dříve uložené webové adrese (URL).
   c. Upozorní uživatele, pokud webová stránka vypadá podezřele.
   d. Vyžaduje otisk prstu pro každé jednotlivé přihlášení.

Pravda / Nepravda

1. Hlavní nevýhodou správce hesel je, že pokud útočník získá vaše jedno "hlavní heslo", získá přístup ke všem ostatním heslům v trezoru. ***(Pravda / Nepravda)***
2. Prezentace doporučuje jako moderní přístup tvorbu "heslových frází", což je například kombinace 4-5 náhodných slov. ***(Pravda / Nepravda)***
3. "Adaptivní autentizace" znamená, že systém vyžaduje 2FA při každém přihlášení, bez ohledu na to, odkud se přihlašujete. ***(Pravda / Nepravda)***

Doplňování

1. Jediné, extrémně silné heslo, které si musíte pamatovat pro odemčení vašeho digitálního trezoru (správce hesel), se nazývá _____ _____.
2. "Zlaté pravidlo bezpečnosti", které shrnuje celou lekci, je kombinace tří prvků: Silné heslo + Správce hesel + _____.