KVÍZ O KYBERNETICKEJ BEZPEČNOSTI

1. **Heslo123** je silné heslo.

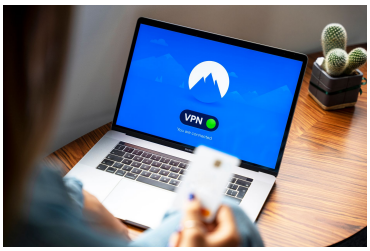
   - [ ] PRAVDA
   - [ ] NEPRAVDA

2. Čo znamená pojem 'Phishing' v kybernetickej bezpečnosti?

   - [ ] Hackovanie do počítačových sietí
   - [ ] Oklamanie ľudí, aby odhalili osobné informácie
   - [ ] Posielanie vírusov cez emailové prílohy
   - [ ] Fyzické kradnutie zariadení

3. Aký je hlavný účel VPN?

   - [ ] Zvýšiť rýchlosť internetu
   - [ ] Zabezpečiť a šifrovať dáta prenášané cez internet
   - [ ] Blokovať malware a vírusy
   - [ ] Spravovať a kontrolovať sieťovú prevádzku



4. Ktorý protokol zabezpečuje bezpečný prenos dát cez internet?

   - [ ] HTTP
   - [ ] FTP
   - [ ] SSL/TLS
   - [ ] SSH

5. Ktorá z nasledujúcich vlastností NIE JE bežnou charakteristikou bezpečného hesla?

- [ ] Obsahuje osobné informácie
- [ ] Obsahuje kombináciu písmen, čísiel a symbolov
- [ ] Je dlhšie ako osem znakov
- [ ] Neobsahuje bežné slová

6. Aký je hlavný účel firewallu?

- [ ] Monitorovanie odchádzajúcej internetovej prevádzky
- [ ] Zrýchlenie internetového pripojenia
- [ ] Zabránenie neoprávnenému prístupu do alebo z privátnej siete
- [ ] Šifrovanie emailov

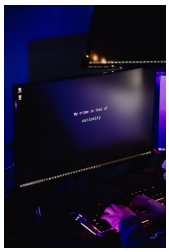
7. Aký je hlavný účel dvojfaktorovej autentifikácie (2FA)?

- [ ] Zdvojnásobiť silu firewallu
- [ ] Vyžadovať dve heslá na prihlásenie
- [ ] Pridať druhú vrstvu zabezpečenia k prihláseniam do účtov
- [ ] Vytvárať zálohy používateľských dát

8. Čo je 'Ransomware'?

- [ ] Softvér, ktorý posilňuje bezpečnosť
- [ ] Malware, ktorý šifruje súbory a požaduje výkupné
- [ ] Program, ktorý monitoruje stlačenia kláves
- [ ] Balík aktualizácií antivírusu

9. Čo znamená 'DoS' v kybernetickej bezpečnosti?



- [ ] Data over Security
- [ ] Disk on Standby
- [ ] Denial of Service
- [ ] Document of Safety

10. Čo znamená princíp minimálnych právomocí v kybernetickej bezpečnosti?

- [ ] Používatelia majú neobmedzený prístup ku všetkým systémovým zdrojom
- [ ] Používatelia sú povinní často meniť svoje heslá
- [ ] Používatelia majú pridelené minimálne úrovne prístupu potrebné na vykonávanie svojich pracovných úloh
- [ ] Používatelia môžu zdieľať svoje prihlasovacie údaje s niekoľkými ďalšími ľuďmi

11. Čo je trójsky kôň v kybernetickej bezpečnosti?

- [ ] Metóda šifrovania dát
- [ ] Škodlivý softvér maskovaný ako legitímny softvér
- [ ] Typ firewallu
- [ ] Bezpečná kódovacia prax

12. Čo znamená pojem "zero-day exploit"?

- [ ] Zastaralá softvérová chyba
- [ ] Typ antivírusového softvéru
- [ ] Zraniteľnosť v softvéri, ktorá nie je známa dodávateľovi
- [ ] Softvérová chyba s dostupnou záplatou

13. Čo je spyware?

- [ ] Softvér, ktorý spomaľuje výkon počítača
- [ ] Softvér, ktorý odstraňuje vírusy
- [ ] Softvér, ktorý šifruje súbory
- [ ] Softvér, ktorý tajne zhromažďuje informácie o aktivitách používateľa

14. Hlavným účelom bezpečnostnej záplaty je opraviť zraniteľnosti v softvéri a zlepšiť bezpečnosť.

- [ ] PRAVDA
- [ ] NEPRAVDA