

Digitális biztonság

1.

Ha egy weboldal címe https:// kezdetű, akkor biztosan nem lehet adathalász oldal.

Hamis

Magyarázat: A https titkosítást jelent, de **csaló oldalak is használhatják.**

2.

Egy 12 karakteres jelszó, amely szavakból áll, biztonságosabb lehet, mint egy rövid, bonyolult jelszó.

Igaz

Magyarázat: A hosszú jelszómondatok nehezebben feltörhetők.

3.

Ha egy üzenet sürgős cselekvést kér (pl. „azonnal kattints”), akkor nagy eséllyel csalásról van szó.

Igaz

Magyarázat: A csalók sürgetéssel próbálnak döntésre kényszeríteni.

4.

Nyilvános Wi-Fi használatakor biztonságos belépni banki fiókba, ha a kapcsolat erős.

Hamis

Magyarázat: Nyilvános hálózaton lehallgatható az adatforgalom.

5.

Ha egy alkalmazás sok engedélyt kér, az mindig azt jelenti, hogy kártékony.

Hamis

Magyarázat: Nem mindig rosszindulatú, de gyanús lehet → ellenőrizni kell.

6.

Egy profilkép és néhány fotó alapján is létrehozható hamis közösségi profil.

Igaz

Magyarázat: A csalók gyakran mások képeit használják.

7.

Ha letöltünk egy játékot hivatalos alkalmazásboltból, akkor az teljesen biztonságos.

Hamis

Magyarázat: Ritkán ugyan, de rosszindulatú appok átcsúszhatnak.

8.

A „jelszó visszaállítása” e-mailek is lehetnek adathalász támadások.

Igaz

Magyarázat: A hamis linkek ellophatják az adatokat.

9.

Ha valaki ismeri a felhasználónevünket, már könnyebben feltörheti a fiókunkat.

Igaz

Magyarázat: Ez az első lépés a támadók számára.

10.

Egy vírus csak akkor kerülhet a gépre, ha fájlt töltünk le.

Hamis

Magyarázat: Fertőzés történhet fertőzött weboldalon keresztül is.

11.

A digitális lábnyom azt jelenti, hogy minden online tevékenységünk nyomtalanul eltűnik.

Hamis

Magyarázat: Az interneten hagyott nyomok sokáig megmaradnak.

12.

Egy ismeretlen személy által küldött fájl megnyitása kockázatos lehet, még ha ismerős nevében érkezik is.

Igaz

Magyarázat: Feltört fiókokról is küldhetnek fertőzött fájlokat.

13.

Ha egy e-mail cím ismerősnek tűnik, biztosan attól a személytől érkezett.

Hamis

Magyarázat: A feladó neve hamisítható, az e-mail cím apró eltérést tartalmazhat.

14.

A böngésző által felkínált automatikus jelszómentés biztonságosabb lehet, mint ha ugyanazt a jelszót több helyen használjuk.

Igaz

Magyarázat: Az egyedi jelszavak biztonságosabbak; a jelszókezelés csökkenti az újrahazsnálat kockázatát.

15.

Egy vírusirtó program meglepte teljes védelmet nyújt minden internetes veszéllyel szemben.

Hamis

Magyarázat: Nem véd az adathalászat, gyenge jelszó vagy felhasználói hibák ellen.

16.

A túl sok személyes adat megosztása a közösségi médiában segítheti a csalókat a jelszó kitalálásában.

Igaz

Magyarázat: Születési dátum, kedvenc állat, iskola → gyakori jelszóelemek.

17.

Ha egy weboldal helyesen van megírva magyarul és nincs benne hiba, akkor megbízható.

Hamis

Magyarázat: A csalók is készíthetnek hibátlan szövegű oldalakat.

18.

Egy „nyereményt nyertél” üzenet akkor is gyanús lehet, ha korábban részt vettünk egy játékban.

Igaz

Magyarázat: A csalók kihasználják az ilyen helyzeteket.

19.

Ha kilépünk egy fiókból, más már nem férhet hozzá az eszközön.

Hamis

Magyarázat: Mentett jelszavak vagy automatikus bejelentkezés visszaengedhet.

20.

A képernyőzár használata védi adatainkat akkor is, ha elveszítjük a telefonunkat.

Igaz

Magyarázat: Megakadályozza az azonnali hozzáférést.

21.

Egy QR-kód beolvasása mindig biztonságos, mert csak információt tartalmaz.

Hamis

Magyarázat: Veszélyes weboldalra is irányíthat.

22.

Ha egy barátunk furcsa üzenetet küld, érdemes más módon is megkérdezni, valóban ő írta-e.

Igaz

Magyarázat: Feltört fiókokról gyakran küldenek csaló üzeneteket.

23.

Az online játékokban idegenekkel megosztott személyes adatok visszaélésre adhatnak lehetőséget.

Igaz

Magyarázat: Az online térben nem tudjuk, ki van a profil mögött.

24.

Ha egy alkalmazás ingyenes, akkor biztosan nem gyűjt adatokat a felhasználóról.

Hamis

Magyarázat: Sok ingyenes app adatgyűjtésből szerez bevételt.

25.

Ha egy jelszó tartalmaz speciális karaktereket (!, #, %), akkor feltörhetetlen.

Hamis

Magyarázat: A hosszúság és az egyediség fontosabb, mint néhány speciális karakter.

26.

Az „Elfelejtett jelszó” funkció biztonsági kérdései gyengíthetik a fiók védelmét, ha a válaszok könnyen kitalálhatók.

Igaz

Magyarázat: A „kedvenc tanár” vagy „születési város” könnyen kideríthető.

27.

Ha egy weboldal felugró ablaka azt írja, hogy vírus van a gépeden, akkor biztosan fertőzött a számítógép.

Hamis

Magyarázat: Ez gyakran csaló reklám.

28.

A digitális lábnyom nemcsak azt tartalmazza, amit mi teszünk közzé, hanem azt is, amit mások osztanak meg rólunk.

Igaz

Magyarázat: Mások által feltöltött képek és megjelölések is ide tartoznak.

29.

Ha törölünk egy bejegyzést a közösségi médiából, az biztosan végleg eltűnik az internetről.

Hamis

Magyarázat: Mások lementhették, archiválhatták.

30.

A kétlépcsős azonosítás csökkenti annak esélyét, hogy ellopott jelszóval belépjenek a fiókunkba.

Igaz

31.

Az ismeretlen USB-meghajtók használata kockázatos lehet még akkor is, ha ajándékba kaptuk.

Igaz

Magyarázat: Kártékony programot tartalmazhat.

32.

Egy profil beállítása „privátra” teljes védelmet jelent az online visszaélések ellen.

Hamis

Magyarázat: A tartalmak továbbküldhetők, lementhetők.

33.

Ha ugyanazt a jelszót használjuk több helyen, egy feltörés több fiókot is veszélybe sodorhat.

Igaz

34.

Az interneten megosztott vicces tesztek („Melyik állat lennél?”) nem jelentenek adatvédelmi kockázatot.

Hamis

Magyarázat: Személyes adatokat és preferenciákat gyűjthetnek.

35.

Egy online barát valódi személyazonossága nem mindig ellenőrizhető.

Igaz

36.

Ha egy alkalmazás frissítést kér, jobb soha nem frissíteni, mert az új verziók veszélyesebbek lehetnek.

Hamis

Magyarázat: A frissítések gyakran biztonsági hibákat javítanak.

37.

A jelszavak megadásakor az a legfontosabb, hogy könnyen megjegyezhetők legyenek.

Hamis

Magyarázat: A legfontosabb szempont a **biztonság**, nem az egyszerű megjegyezhetőség.

A túl egyszerű jelszavakat (pl. 123456, jelszo, születési dátum) könnyű feltörni.

- Jó jelszó: hosszú, bonyolult, kis- és nagybetűket, számokat, jeleket tartalmaz.

- Megjegyzéshez használható jelszókezelő vagy mondat alapú jelszó.

38.

A többfaktoros hitelesítés biztonságosabb, mint kizárólag jelszót használni.”

Igaz

Magyarázat: A többfaktoros azonosítás (MFA) több lépcsőben azonosít:

- jelszó
- SMS-kód vagy alkalmazás
- biometrikus azonosítás (ujjlenyomat)

- Ha valaki megszerzi a jelszót, még akkor sem tud belépni a kód nélkül.

39.

Nem biztonságos, ha szöveges formában tárolja jelszavait az eszközein.

Igaz

Magyarázat: Ha a jelszavak jegyzetben, dokumentumban vagy telefon jegyzetekben vannak:

- vírus vagy hacker megszerezheti
- mások hozzáférhetnek a készülékhez

- Biztonságosabb: jelszókezelő alkalmazás használata.

40.

Biztonságos Csilla számára, ha megosztja a jelszavát közeli ismerőseivel, barátaival.

Hamis

Magyarázat: A jelszó **személyes adat**, nem szabad megosztani.

Veszélyek:

- visszaélhetnek a fiókkal
- adatlopás történhet
- felelősség a tulajdonost terheli

- Még a legjobb baráttal sem szabad megosztani.