Teszt – Védekezés a digitális világ veszélyei ellen

1. Egyszeres választás
Mi a legfontosabb lépés, ha egy hihetetlennek tűnő hírt olvasol?
A) Azonnal megosztani másokkal, hogy mindenki tudja.
B) Megnézni, hogy ki osztotta meg a hírt a közösségi médiában.
C) Ellenőrizni a hír forrását és hitelességét.
D) Kommentszekcióban megkérdezni, hogy mások mit gondolnak.

2. Egyszeres választás
Milyen tényezőre kell különösen figyelni egy online hír esetében?
A) A hír frissességére és a közzététel időpontjára.
B) A hír olvasottságára és népszerűségére.
C) Arra, hogy mennyi kommentet kapott a bejegyzés.
D) Arra, hogy hány ismerősöd osztotta meg.

3. Igaz-hamis
A legtöbb álhírt egyszerű felismerni, mert mindig tartalmaz helyesírási hibákat.

4. Többszörös választás
Melyik módszerek segíthetnek az álhírek kiszűrésében?
A) Több forrásból is ellenőrizni a hírt.
B) Kizárólag a közösségi médiában terjedő hírekre hagyatkozni.
C) Megnézni, hogy van-e logikai ellentmondás a cikkben.
D) Figyelni, hogy a hír hatni próbál-e az érzelmekre.

5. Egyszeres választás
Mi lehet egy álhír rejtett célja?
A) Csak szórakoztatni szeretné az embereket.
B) Rejtett reklámként egy termék népszerűsítése.
C) Tudományos felfedezések hiteles bemutatása.
D) Az olvasók kritikai gondolkodásának fejlesztése.

6. Igaz-hamis
A digitális világban mindig megbízhatsz azokon a híroldalakon, amelyeket a közösségi médiában sokan megosztanak.

7. Egyszeres választás
Mi jellemzi a jó jelszót?
A) Minél rövidebb és könnyebben megjegyezhető legyen.
B) Csak számokat tartalmazzon.
C) Tartalmazzon kis- és nagybetűket, számokat és speciális karaktereket.
D) Legyen azonos a felhasználó nevével.

8. Többszörös választás
Milyen információkat nem érdemes használni jelszóként?
A) Születési dátumot.
B) Kisállat nevét.
C) Egy véletlenszerű szót, amelyet csak te ismersz.
D) A lakcímedet.

9. Egyszeres választás
Mit tegyél, ha egy e-mailben egy ismeretlen személy ajándékot vagy nyereményt ígér neked?
A) Azonnal kattints a linkre és add meg az adataidat.
B) Ellenőrizd az e-mail feladóját és gyanús esetben ne kattints a linkekre.
C) Küldd tovább minél több barátodnak, hogy ők is nyerjenek.
D) Válaszolj az e-mailre és kérdezd meg a részleteket.

10. Igaz-hamis
Az online csalók gyakran érzelmi manipulációval próbálnak pénzt kicsalni az emberektől.

11. Egyszeres választás
Hogyan lehet a legjobban elkerülni a levélszemetet (spam)?
A) Ne adjuk meg az e-mail címünket mindenféle oldalon.
B) Küldjük tovább másoknak a spam üzeneteket.
C) Regisztráljunk minél több hírlevélre.
D) Minden levélszemetet olvassunk el figyelmesen.

12. Többszörös választás
Milyen jelek utalhatnak arra, hogy egy online hír rejtett reklám?
A) Egy adott termék túlzott dicsérete.
B) Az, hogy több forrásból is megerősítik a hírt.
C) Az, hogy csak egyetlen márkát említ és pozitív színben tünteti fel.
D) A hír végén egy vásárlásra ösztönző link szerepel.

13. Igaz-hamis
A hackelés minden esetben törvénysértő cselekedet.

14. Egyszeres választás
Miért veszélyes, ha más személy jelszavát megszerezzük és használjuk?
A) Mert ezzel segítünk neki jobban megvédeni a fiókját.
B) Mert ezzel megmutathatjuk neki, hogy nem jó jelszót választott.
C) Mert jogsértést követünk el, és akár büntethető is lehet.
D) Mert ettől népszerűbbek leszünk az iskolában.

15. Többszörös választás
Mit tehetsz, ha úgy érzed, hogy feltörték a fiókodat?
A) Azonnal változtasd meg a jelszavadat.
B) Értesítsd a szolgáltatót és kérj segítséget.
C) Írd ki egy közösségi médiás posztban, hogy feltörtek.
D) Beszélj egy felnőttel vagy szakértővel a problémáról.

Teszt – Védekezés a digitális világ veszélyei ellen (2. rész)

1. Egyszeres választás
Mit jelent az adathalászat (phishing)?
A) Egy adathordozó gyorsabb olvasását jelenti.
B) Olyan módszer, amely során csalók hamis weboldalakkal vagy e-mailekkel próbálnak személyes adatokat megszerezni.
C) Egy titkosított internetkapcsolat típusa.
D) A számítógépes adatmentés egyik eljárása.

2. Többszörös választás
Milyen módon próbálhatják a csalók megszerezni az adataidat online?
A) Hamis banki e-mailek küldésével.
B) Egy közösségi médiás játék vagy nyereményjáték álcájában.
C) Egy hiteles kormányzati weboldalon keresztül.
D) Telefonhívással, amelyben sürgős intézkedésre kérnek.

3. Igaz-hamis
A biztonsági kérdések használata növeli a fiókok védelmét, de nem ajánlott könnyen kitalálható válaszokat adni (pl. anyukád neve).

4. Egyszeres választás
Mit kell tenni, ha gyanús üzenetet kapsz egy barátod fiókjából?
A) Azonnal válaszolni, hogy kiderüljön, tényleg ő írta-e.
B) Rákattintani a benne lévő linkre, hogy ellenőrizd, miről van szó.
C) Figyelmeztetni a barátodat és nem kattintani a linkekre.
D) Figyelmen kívül hagyni, hiszen nincs jelentősége.

5. Igaz-hamis
A nyilvános Wi-Fi hálózatok mindig biztonságosak, ezért nyugodtan bejelentkezhetsz a banki fiókodba, ha szükséges.

6. Egyszeres választás
Milyen hosszú jelszó ajánlott egy biztonságos fiókhoz?
A) Legalább 8 karakter
B) Legalább 6 karakter
C) Legalább 12 karakter, kis- és nagybetűkkel, számokkal és speciális karakterekkel.
D) Bármilyen hosszú, ha könnyen megjegyezhető

7. Többszörös választás
Milyen veszélyekkel járhat, ha egy nyilvános helyen elérhető számítógépen (pl. internetkávézóban) jelentkezel be egy fiókodba?
A) Egy kémprogram rögzítheti a jelszavaidat.
B) Valaki megfigyelheti, mit gépelsz be.
C) A böngésző elmentheti az adataidat, ha nem lépsz ki megfelelően.
D) A gép gyorsabban elromlik tőle.

8. Egyszeres választás
Melyik jelszó a legbiztonságosabb az alábbiak közül?
A) jelszo123
B) Kutyus2008
C) P@ssW0rd!#78
D) 12345678

9. Igaz-hamis
Ha egy alkalmazás vagy weboldal kéri a személyes adataidat, mindig meg kell adnod, mert biztosan megbízható.

10. Egyszeres választás
Mi történhet, ha egy közösségi média oldalra túl sok személyes információt töltesz fel?
A) Nem történik semmi, hiszen ezeket az oldalakat mindenki biztonságosan használhatja.
B) A csalók és hackerek könnyebben visszaélhetnek az adataiddal.
C) Csak a barátaid látják, így semmilyen kockázat nincs.
D) Növeli az oldal látogatottságát.

11. Többszörös választás
Milyen technikákkal próbálhatják a csalók rávenni az embereket arra, hogy megosszák a jelszavukat?
A) Hamis üzenetek küldése, amelyben banki vagy biztonsági figyelmeztetés szerepel.
B) Egy nyereményjátékban való részvétel lehetősége.
C) Egy ismerős nevében küldött üzenet, amelyben segítséget kérnek.
D) Egy kormányzati üzenet, amelyben mindenki számára ingyenes pénzt ígérnek.

12. Igaz-hamis
A kétlépcsős azonosítás (pl. SMS-kód vagy hitelesítő alkalmazás) növeli az online fiókjaid védelmét.

13. Egyszeres választás
Mit tehetsz, ha egy weboldal azt állítja, hogy vírus van a számítógépeden, és azonnali letöltést ajánl a probléma megoldására?
A) Azonnal letöltöm, hogy megvédjem a gépemet.
B) Ellenőrzöm egy megbízható víruskeresővel, mielőtt bármit tennék.
C) Keresek egy másik ingyenes vírusirtót az interneten.
D) Újraindítom a számítógépemet, és remélem, hogy eltűnik a figyelmeztetés.

14. Többszörös választás
Milyen jelek utalhatnak arra, hogy egy e-mail csalás lehet?
A) Az üzenet sürget, hogy azonnal cselekedj.
B) Az e-mailben szereplő link gyanús vagy ismeretlen oldalra mutat.
C) Az e-mail nyelvezete és helyesírása hibás.
D) Az üzenetben arra kérnek, hogy add meg a jelszavadat vagy banki adataidat.

15. Igaz-hamis
A közösségi médiában megosztott fotóid és információid mindig törölhetők, így nem kell aggódnod a digitális nyomaid miatt.

Teszt – Védekezés a digitális világ veszélyei ellen (3. rész)

1. Egyszeres választás

Milyen adatokat NEM szabad megosztani egy közösségi média profilban?

A) A kedvenc hobbid

B) Az iskolád neve és címe

C) A kedvenc filmed

D) A háziállatod neve

2. Igaz-hamis

Ha egy weboldal címe „https" előtaggal kezdődik, az azt jelenti, hogy az oldal 100%-ban biztonságos, és minden ott megadott adat védett.

3. Többszörös választás

Milyen módszerekkel próbálnak online csalók rávenni a felhasználókat, hogy kattintsanak egy veszélyes linkre?

A) Valamilyen sürgető üzenetet küldenek, például „Ha nem kattintasz, töröljük a fiókodat!"

B) Egy barátod nevében küldenek üzenetet, amelyben segítséget kérnek.

C) Egy hamis nyereményjátékot hirdetnek, ahol csak kattintani kell a részvételhez.

D) Egy ismert weboldal valós ügyfélszolgálati e-mailjét másolják le.

4. Egyszeres választás

Mit tehetsz, ha egy idegen személy privát üzenetben pénzt kér tőled egy közösségi oldalon?

A) Megkérdezem tőle, mire kell a pénz.

B) Jelentem és letiltom az illetőt.

C) Elküldöm neki a pénzt, mert biztosan szüksége van rá.

D) Megosztom az esetet az ismerőseimmel, hátha segítenek.

5. Igaz-hamis

A hackerek mindig rossz szándékú emberek, akik törvénytelen dolgokat tesznek.

6. Egyszeres választás

Miért érdemes rendszeresen frissíteni a számítógép és a mobiltelefon operációs rendszerét?

A) Mert a frissítések gyorsabbá teszik a készüléket.

B) Mert a frissítések új biztonsági javításokat tartalmaznak, amelyek védelmet nyújtanak a hackerek ellen.

C) Mert a régebbi verziók nem működnek megfelelően internetkapcsolat nélkül.

D) Mert így több reklámot láthatunk az új funkciókról.

7. Többszörös választás

Milyen lépésekkel védheted meg a személyes adataidat online?

A) Csak erős jelszavakat használok.

B) Nem adom meg a telefonszámomat és a lakcímemet ismeretlen weboldalakon.

C) Csak nyilvános Wi-Fi hálózatokon keresztül intézem az online banki ügyeimet.

D) Bekapcsolom a kétlépcsős azonosítást, ahol csak lehet.

8. Igaz-hamis

Ha egy ismerősöd megkér, hogy ossz meg egy gyanús linket, akkor is meg kell tenned, mert megbízol benne.

9. Egyszeres választás

Miért veszélyes, ha ugyanazt a jelszót használod több weboldalon is?

A) Mert könnyebb megjegyezni.

B) Mert ha egy oldalról kiszivárog a jelszavad, a hackerek más fiókjaidba is bejuthatnak vele.

C) Mert a jelszavakat időnként lecserélik automatikusan.

D) Mert ez az internetes szabályzatba ütközik.

10. Többszörös választás
Milyen veszélyeket jelenthet egy túl könnyű jelszó?
A) A hackerek könnyebben feltörhetik a fiókot.
B) A személyes adatok és üzenetek kiszivároghatnak.
C) A fiók elveszhet, és nem lehet többé visszaszerezni.
D) A jelszó gyorsabban elfelejtődik.

11. Igaz-hamis
Azért érdemes azonos jelszót használni mindenhol, mert így kevésbé valószínű, hogy elfelejted.

12. Egyszeres választás
Mi a legbiztosabb módja annak, hogy felismerd a hamisított weboldalakat?
A) Megnézem a weboldal kinézetét.
B) Ellenőrzöm a webcím (URL) helyesírását és megbízhatóságát.
C) Csak akkor kattintok, ha sok ember osztotta meg a linket.
D) Ha az oldal felajánl egy ingyenes ajándékot, akkor biztosan megbízható.

13. Többszörös választás
Hogyan lehet megvédeni egy online fiókot attól, hogy feltörjék?
A) Rendszeresen változtatom a jelszavam.
B) Kétlépcsős azonosítást használok.
C) Nem kattintok ismeretlen linkekre vagy gyanús e-mailekre.
D) A jelszavamat egy cetlire írom, és a számítógép mellé ragasztom.

14. Igaz-hamis
Ha egy ismeretlen ember kedves üzenetet küld neked egy közösségi oldalon, akkor biztosan nincs semmilyen hátsó szándéka, és nyugodtan válaszolhatsz neki.

15. Egyszeres választás
Miért érdemes a közösségi média fiókok adatvédelmi beállításait ellenőrizni?
A) Mert így eldöntheted, hogy kik láthatják a bejegyzéseidet és adataidat.
B) Mert így az ismerőseid könnyebben megtalálnak.
C) Mert így mindenki láthatja a tartalmaidat, és több lájkot kapsz.
D) Mert ettől gyorsabb lesz a telefonod.

Teszt – Védekezés a digitális világ veszélyei ellen (4. rész)

1. Egyszeres választás

Miért veszélyes nyilvánosan megosztani a pontos tartózkodási helyedet az interneten?
A) Mert az ismerőseid így könnyebben megtalálnak.
B) Mert a csalók és betörők kihasználhatják ezt az információt.
C) Mert a közösségi média algoritmusai ezt nem szeretik.
D) Mert ettől gyorsabban merül a telefon akkumulátora.

2. Igaz-hamis

Ha egy weboldalon sok pozitív véleményt és értékelést látsz egy termékről, az mindig azt jelenti, hogy a termék megbízható.

3. Többszörös választás

Milyen jelei lehetnek annak, hogy egy közösségi oldalon egy profil hamis?
A) A felhasználónak nincs sok ismerőse, és a profilképe gyanús.
B) A profil hirtelen kezd el nagy mennyiségű üzenetet küldeni.
C) A személy kizárólag másoktól másolt bejegyzéseket oszt meg.
D) A felhasználó mindig a legfrissebb híreket osztja meg.

4. Egyszeres választás

Mit kell tenned, ha egy ismeretlen személy felveszi veled a kapcsolatot és személyes információkat kér?
A) Megadom neki az adatokat, hiszen biztosan jó szándékú.
B) Ellenőrzöm a személy profilját, és ha gyanús, nem válaszolok neki.
C) Rögtön megosztom az adatokat a közösségi médiában is.
D) Azonnal letiltom a telefonomon az internetet.

5. Igaz-hamis

Egy bank soha nem kér e-mailben vagy SMS-ben jelszót vagy banki adatokat.

6. Egyszeres választás

Milyen lépésekkel csökkentheted az online zaklatás kockázatát?
A) Privát adatvédelmi beállítások használata és csak ismerősök elfogadása.
B) Minél több személyes információ megosztása, hogy mindenki lásson.
C) Minél több barát kérése, függetlenül attól, hogy ismered-e őket.
D) Zaklatás esetén az üzenetek figyelmen kívül hagyása, de a zaklató tiltásának elkerülése.

7. Többszörös választás

Hogyan kerülheted el, hogy egy e-mailben található link veszélyes legyen?
A) Rákattintás előtt ellenőrzöm az e-mail feladóját.
B) Ha gyanús az e-mail, nem kattintok a linkre.
C) Ha banki e-mailnek tűnik, inkább közvetlenül a bank hivatalos oldalára lépek be.
D) Ha az e-mail sürget, azonnal megnyitom a linket, nehogy lemaradjak valamiről.

8. Igaz-hamis

Egy víruskereső program telepítése teljes védelmet nyújt a hackertámadások ellen.

9. Egyszeres választás

Mi az egyik legjobb módja annak, hogy elkerüld az online csalásokat?
A) Csak azokat az e-maileket nyitom meg, amelyeket egy nagy cég küldött.
B) Nem osztok meg túl sok személyes információt az interneten.
C) Nem zárom be a böngészőt, hogy folyamatosan figyeljem az új üzeneteket.
D) Minden gyanús üzenetet továbbítok a barátaimnak ellenőrzés nélkül.

10. Többszörös választás
Milyen lépések segítenek a digitális eszközeid védelmében?
A) Rendszeresen frissítem a szoftvereket.
B) Kétes forrásból származó alkalmazásokat nem telepítek.
C) Bekapcsolom az automatikus jelszómentést minden oldalon.
D) Nem csatlakozom nyilvános Wi-Fi hálózatokhoz biztonsági intézkedések nélkül.

11. Igaz-hamis
Ha egy ismerősöd profilja gyanúsan viselkedik (például pénzt kér tőled), érdemes gyanakodni, hogy feltörték a fiókját.

12. Egyszeres választás
Miért fontos, hogy erős jelszavakat használjunk?
A) Mert a könnyű jelszavak gyorsabban beírhatók.
B) Mert az erős jelszavak megnehezítik a fiók feltörését a hackerek számára.
C) Mert a hosszabb jelszavak jobban mutatnak a bejelentkezési képernyőn.
D) Mert így az internet gyorsabb lesz.

13. Többszörös választás
Milyen trükköket használhatnak az adathalász csalók?
A) Egy ismert cég hivatalos e-mailjére hasonlító üzenetet küldenek.
B) Egy hivatalos weboldal hamis másolatát hozzák létre, hogy ellopják a bejelentkezési adataidat.
C) Egy reklámot jelenítenek meg, amely azt állítja, hogy nyertél valamit, és kattintanod kell.
D) Egy barátod fiókját feltörik, és az ő nevében küldenek üzenetet neked.

14. Igaz-hamis
Ha egy üzenet azt állítja, hogy „sürgősen be kell jelentkezned, mert veszélyben van a fiókod”, mindig kattints a megadott linkre.

15. Egyszeres választás
Mit tehetsz, ha egy weboldal túl sok személyes információt kér tőled?
A) Azonnal megadom az adatokat, hiszen biztosan megbízható.
B) Utánanézek az oldal hitelességének, és ha gyanús, nem adok meg semmit.
C) Megosztom az oldalt a közösségi médiában, hogy mások is kitöltsék.
D) Egy másik weboldalon keresek hasonló tartalmat.

Teszt – Védekezés a digitális világ veszélyei ellen (5. rész)

1. Egyszeres választás

Miért veszélyes egy idegen USB-eszközt csatlakoztatni a számítógépedhez?

A) Mert az USB túlmelegedhet és károsíthatja a gépet.

B) Mert rossz minőségű fájlokat tartalmazhat.

C) Mert vírusokat és rosszindulatú szoftvereket terjeszthet.

D) Mert lelassíthatja az internetkapcsolatot.

2. Igaz-hamis

Ha egy weboldal ingyenes ajándékot kínál, akkor biztosan megbízható, hiszen nem kér érte pénzt.

3. Többszörös választás

Milyen intézkedéseket tehetsz, ha azt gyanítod, hogy feltörték a fiókodat?

A) Azonnal megváltoztatom a jelszavamat egy erősebbre.

B) Kapcsolatba lépek az adott szolgáltató ügyfélszolgálatával.

C) Figyelemmel kísérem a fiókomban történt változásokat.

D) Figyelmen kívül hagyom, mert biztosan nincs komoly probléma.

4. Egyszeres választás

Mit tehetsz, ha egy alkalmazás túl sok jogosultságot kér (pl. hozzáférést a kamerádhoz és a kontaktjaidhoz, pedig nincs rá szüksége)?

A) Minden jogosultságot megadok, mert biztosan szüksége van rá.

B) Letiltom a jogosultságokat és ellenőrzöm az alkalmazás megbízhatóságát.

C) Letöltöm az alkalmazást, de nem használom.

D) Letöltöm, majd törlöm, ha gyanússá válik.

5. Igaz-hamis

A hosszú, véletlenszerű karakterekből álló jelszavak biztonságosabbak, mint az egyszerű szavakból állók.

6. Egyszeres választás

Miért fontos az adatok rendszeres mentése?

A) Mert így több helyet foglalnak el a számítógépen.

B) Mert ha elveszíted az eszközödet, az adatok biztonságban maradnak.

C) Mert így könnyebb lesz internetkapcsolat nélkül dolgozni.

D) Mert ettől gyorsabb lesz a géped.

7. Többszörös választás

Milyen jelek utalhatnak arra, hogy egy e-mail gyanús és adathalász lehet?

A) Az e-mail cím eltér a hivatalos szolgáltatókétól.

B) Az e-mail nyelvezete szokatlan vagy tele van helyesírási hibákkal.

C) Az üzenet sürget, hogy azonnal kattints egy linkre vagy add meg az adataidat.

D) Az e-mail egy általános megszólítással kezdődik (pl. „Kedves felhasználó!”).

8. Igaz-hamis

Ha egy barátod online megoszt egy hírhedt személyes adatokat tartalmazó bejegyzést, akkor is tovább kell osztanod, mert biztosan igaz.

9. Egyszeres választás

Miért nem szabad ugyanazt a jelszót használni több különböző fiókhoz?

A) Mert így könnyebben elfelejtheted.

B) Mert ha egy fiókot feltörnek, a hackerek hozzáférhetnek az összes többihez is.

C) Mert a szolgáltatók ezt nem engedélyezik.

D) Mert így a rendszer gyakrabban kéri a jelszócserét.

10. Többszörös választás
Milyen veszélyekkel járhat, ha nyilvános Wi-Fi hálózathoz csatlakozol megfelelő biztonsági intézkedések nélkül?
A) A hackerek elfoghatják és ellophatják az adataidat.
B) A banki és egyéb személyes adataid kiszivároghatnak.
C) A nyilvános Wi-Fi lelassíthatja a készülékedet.
D) Valaki más hozzáférhet az online fiókjaidhoz és jelszavaidhoz.

11. Igaz-hamis
Egy jól beállított tűzfal segíthet megvédeni a számítógépedet a kártékony támadásoktól.

12. Egyszeres választás
Miért fontos a közösségi média adatvédelmi beállításainak ellenőrzése?
A) Mert így meghatározhatod, ki láthatja a személyes információidat.
B) Mert így több ember láthatja a bejegyzéseidet.
C) Mert ettől gyorsabbá válik az oldal betöltése.
D) Mert így több reklámot kapsz a kedvenc termékeidről.

13. Többszörös választás
Hogyan segíthetsz másoknak elkerülni az online csalásokat?
A) Megtanítod őket az adathalászat és az álhírek felismerésére.
B) Figyelmezteted őket, ha gyanús e-maileket vagy üzeneteket kapnak.
C) Továbbküldöd nekik a gyanús üzeneteket, hogy megnézzék, igazak-e.
D) Megmutatod nekik, hogyan állíthatják be a fiókjaik biztonságát.

14. Igaz-hamis
A közösségi médiában megosztott adatok és képek mindig törölhetők, ezért nem kell aggódni, ha valami érzékeny információt osztasz meg.

15. Egyszeres választás
Mi a teendő, ha egy online játékban egy ismeretlen személy pénzt vagy személyes adatokat kér tőled?
A) Küldök neki pénzt, mert biztosan szüksége van rá.
B) Azonnal jelentem és nem válaszolok az üzeneteire.
C) Kipróbálom, hogy tényleg küld-e valamit cserébe.
D) Megosztom másokkal az üzenetet, hogy ők is lássák.

Teszt – Védekezés a digitális világ veszélyei ellen (6. rész)

1. Egyszeres választás

Mit kell tenned, ha egy gyanús weboldal az e-mail címed és jelszavad megadására kér?
A) Megadom az adatokat, hogy kipróbáljam az oldalt.
B) Ellenőrzöm a weboldal címét és a hitelességét, mielőtt bármit is megadnék.
C) Rákattintok, mert egy ismerősöm is megosztotta.
D) Beírom a jelszót, és ha nem működik, akkor változtatok rajta.

2. Igaz-hamis

A közösségi média profilodon megadott személyes adataidat bárki láthatja, ha nem állítod be megfelelően az adatvédelmi beállításokat.

3. Többszörös választás

Milyen módon próbálhatják a csalók kideríteni a jelszavadat?
A) Telefonhívással, amelyben azt állítják, hogy a bankod képviselői.
B) Egy e-mailben, amelyben egy ismerősöd nevében kérik az adataidat.
C) Egy weboldalon keresztül, amely a bejelentkezési oldal másolatának tűnik.
D) Egy ajándékot ígérő hirdetésen keresztül, amelyhez regisztrálnod kell.

4. Egyszeres választás

Mit jelent a kétlépcsős hitelesítés (2FA)?
A) Két különböző jelszó megadása belépéskor.
B) Egy további biztonsági réteg, például egy SMS-ben kapott kód vagy hitelesítő alkalmazás használata a bejelentkezéshez.
C) Egy másik eszközről történő belépés engedélyezése.
D) Egy titkos kérdés megválaszolása.

5. Igaz-hamis

Ha egy alkalmazás túl sok engedélyt kér (például a kamerád, mikrofonod és helyzeted elérését), érdemes gyanakodni.

6. Egyszeres választás

Mit kell tenned, ha egy online ismerősöd hirtelen furcsán kezd viselkedni, például pénzt kér tőled?
A) Rákérdezek, hogy miért van szüksége pénzre.
B) Ellenőrzöm a profilját és megpróbálom más csatornán elérni, hogy valóban ő-e.
C) Azonnal elküldöm neki a pénzt.
D) Megosztom az esetet a közösségi médiában.

7. Többszörös választás

Milyen jelek utalhatnak arra, hogy egy weboldal hamis?
A) Az URL furcsa karaktereket vagy elírásokat tartalmaz.
B) A weboldal rossz minőségű grafikát és helyesírási hibákat tartalmaz.
C) A weboldal sürget, hogy gyorsan cselekedj, mert különben „elveszíted a lehetőséget”.
D) Az oldal HTTPS protokollt használ.

8. Igaz-hamis

Ha egy ismerősöd egy különleges ajánlatot vagy nyereményt küld neked egy gyanús linkkel, az biztosan megbízható, mert ismered őt.

9. Egyszeres választás

Mi a legbiztonságosabb módja egy erős jelszó létrehozásának?
A) A születési dátum és egy kisállat nevének kombinálása.
B) Véletlenszerű kis- és nagybetűk, számok és speciális karakterek keverése.
C) Egy egyszerű, de hosszú szó használata.
D) Az iskolai becenevem hozzáadása a jelszóhoz.

10. Többszörös választás
Milyen lépésekkel előzheted meg, hogy a közösségi média fiókodat feltörjék?
A) Erős jelszót használok és rendszeresen megváltoztatom.
B) Nem kattintok gyanús linkekre vagy ismeretlen üzenetekre.
C) Kétlépcsős hitelesítést használok, ha elérhető.
D) Nyilvánosan megosztom a bejelentkezési adataimat, hogy mások is segíthessenek visszaszerezni a fiókomat.

11. Igaz-hamis
Ha egy e-mail szerint „sürgős" cselekvésre van szükség, akkor azonnal kattintani kell a benne lévő linkre, hogy ne veszítsem el a fiókomat.

12. Egyszeres választás
Mit kell tenned, ha egy ismeretlen weboldal jelszavad megadását kéri, de nem emlékszel rá, hogy regisztráltál volna oda?
A) Megadom, mert lehet, hogy már regisztráltam régen.
B) Megpróbálok információt keresni az oldalról, és ha gyanús, nem adok meg semmit.
C) Beírom a jelszót, és ha nem működik, akkor módosítom.
D) Kérek egy új jelszót az e-mail címemre.

13. Többszörös választás
Milyen típusú támadásokkal próbálhatják a hackerek ellopni a személyes adataidat?
A) Adathalászat (phishing), amikor egy hamis e-mail vagy weboldal próbálja kicsalni az adataidat.
B) Kémprogramok telepítése, amelyek titokban figyelik a billentyűleütéseidet.
C) Vírusok terjesztése, amelyek ellophatják az adataidat vagy titkosíthatják a fájljaidat.
D) Reklámozás, amely csak arra ösztönöz, hogy vásárolj egy terméket.

14. Igaz-hamis
Ha egy e-mailben vagy üzenetben egy link rövidített formában (pl. bit.ly vagy goo.gl) szerepel, az mindig megbízható.

15. Egyszeres választás
Miért fontos, hogy rendszeresen frissítsd az alkalmazásokat és a szoftvereket az eszközeiden?
A) Mert így gyorsabbá válnak az eszközök.
B) Mert a frissítések gyakran tartalmaznak biztonsági javításokat, amelyek megvédenek a hackerektől.
C) Mert így több funkciót érhetek el.
D) Mert ettől kevésbé merül az akkumulátor.