

ONLINE BIZTONSÁG - TESZTELD MAGAD! (*MEGOLDÁS ☺)*

1. **Mi az a KiberPajzs?**
2. Virtuális játék.
3. **Védelem a netes csalók ellen, azaz edukációs és kommunikációs program a lakosság pénzügyi tudatosságának erősítése érdekében.**
4. Vírusirtó.
5. **Mit jelent az adathalászat (phishing) kifejezés?**
6. Online adatbank.
7. Speciális keresztrejtvény.
8. **Olyan adathalász csalási forma, amely bizalmas banki információk (személyes, pénzügyi, illetve biztonsági adatok) jogosulatlan megszerzésére irányul.**
9. **Honnan ismerhetjük fel az adathalász e-maileket, szöveges üzeneteket?**
10. Nem ismerjük a feladóját, hangneme behízelgő.
11. **Helyesírási hibákról, sürgető hangnemről, szokatlan formátumú csatolmányról, stb**.
12. Bizalmas információkat tartalmaz.
13. **Az elkövetők milyen módon próbálnak bizalmas pénzügyi információkhoz jutni?**
14. Közösségi oldalakon keresztül.
15. Telefonkönyvből.
16. **Általában telefonhívásokon, szöveges üzeneteken, valamint e-maileken keresztül**.
17. **Honnan lehet felismerni a hamis weboldalakat?**

1. Az eredetitől eltérő az arculata.
2. Túl sok fényképet tartalmaz.
3. **A weboldal domain neve kinézetre megtévesztésig hasonlít az ismert, megbízható**

 **oldaléhoz, azonban azzal könnyen összetéveszthető karaktereket (is) tartalmaz.**

1. **Mit tegyünk, ha idegen személy azt kéri, hogy számítógépünkre vagy telefonunkra olyan programot, alkalmazást (pl. Anydesk) telepítsünk, amelyet nem ismerünk?**
2. Nyugodtan megtehetjük, ebből még nem származhat kárunk.
3. **Soha ne tegyünk ilyet, mivel ezáltal hozzáférést biztosíthatunk (akár) banki adatainkhoz (is).**
4. Attól függ, hogy milyen programról van szó.
5. **Online vásárlás esetén milyen bankkártyát célszerű használni?**
6. Hitelkártyát.
7. **Virtuális bankkártyát.**
8. Online vásárlás esetén soha nem szabad bankkártyával fizetni.
9. **Mit célszerű tenni, ha a pénzintézet ügyintézője telefonon keresztül azt kéri, hogy lépjünk be internetbankunkba, illetve pénzintézetünk mobilalkalmazásába, módosítsuk banki limitbeállításunkat?**
10. Ha ezt pénzintézetre hivatkozva kérik, akkor nyugodtan megtehetjük.
11. **Telefonos kérésre sem szabad ezeket megtenni! Egy pénzintézet ügyintézője sosem kér ilyet az ügyféltől.**
12. Minden esetben meg kell tenni.
13. **Mi a teendő, ha az internetes hirdetésünkre jelentkező vásárló, azt kéri, hogy a tranzakciót egy ismert csomagküldő szolgáltatón (pl. FoxPost) keresztül bonyolítsuk le?**

1. A vásárló által küldött linkre rákattintok, mert ez a legbiztonságosabb és leggyorsabb megoldás.
2. A vásárló által küldött linkre csak abban az esetben kattintok rá, ha ismerem a csomagküldőt, és jó tapasztalataim vannak vele kapcsolatban.
3. **A vásárló által küldött linkre akkor sem kattintok rá, ha ismerem a csomagküldőt, és jó tapasztalataim vannak vele kapcsolatban.**
4. **Mi a teendő a szöveges üzenetben, e-mailben kapott hivatkozással, melléklettel?**
5. Nyugodtan meg lehet nyitni, rá lehet kattintani.
6. **Sohasem szabad ezeket megnyitni, illetve nem szabad ezekre rákattintani.**
7. Csak abban az esetben szabad megnyitni, illetve rákattintani, ha az üzenet küldőjét, illetve az e-mail feladóját ismerjük.
8. **Gyanakvással kell-e fogadni a banki adatokra vonatkozó hívást abban az esetben is, ha a hívószám valós pénzintézeti telefonszámnak tűnik?**
9. Nem, ebben az esetben nyugodtak lehetünk.
10. **Igen, a vonalat minden esetben meg kell szakítani (mert lehet, hogy hívószám-hamisítás, azaz spoofing, amivel dolgunk van) és bankunk központi telefonszámát kell felhívni.**
11. Ha pénzintézetre hivatkoznak és a telefonszámot is ismerjük, akkor nem kell gyanakodni.

*Bővebb információ: www.kiberpajzs.hu*

