

Gyakori online csalási kampányok az iskolakezdési időszakban

A nyár vége és a szeptember eleje sok családban egy **stresszes, sűrű időszak**, hiszen az iskolakezdés számos teendővel és ügyintézéssel jár. A tanszerek beszerzése mellett ilyenkor kerülhet sor például **ösztöndíjak és támogatások igénylésére**, az idősebb diákok esetében pedig akár **lakhatással kapcsolatos ügyek intézésére** is. Ezt az időszakot a **csalók is igyekeznek kihasználni különböző támadási módszerekkel**, ezért érdemes kellő óvatossággal eljárni az online ügyintézés során.

Tanszervásárlás és egyéb iskolakezdési akciók

Egy új tanév számos kiadással járhat. Be kell szerezni a tankönyveket, tanszereket, ruhákat, illetve egyéb, például sportfelszereléseket és digitális eszközöket. Amennyiben valaki ezek online megvásárlása mellett dönt, érdemes a **már jól ismert, megbízható webáruházaknál maradni**.

Sok áruházban érhetők el iskolakezdési kedvezmények, de **legyünk óvatosak a túlzó – sokszor 80%, 90%-os kedvezményt ígérő – kihagyhatatlan ajánlatokkal!** A csalók gyakran **sürgetik a vásárlókat** a gyors, meggondolatlan rendelések leadására, ezért nem érdemes kapkodni. Az alábbiak betartása jelentősen csökkenheti annak kockázatát, hogy online vásárlási csalás áldozatává váljunk.

- **Ha túl szép ahhoz, hogy igaz legyen, nagy valószínűséggel nem az!** Érdemes egy kis piackutatást végezni a keresett termék vonatkozásában, ugyanis a 80-90% árengedmény bizony gyanúra adhat okot.
- **Mindig ellenőrizzük az URL címeket**, kimondottan az ismeretlen feladóktól kapott linkeket (amelyek megnyitása egyáltalán nem javasolt)! A támadók gyakran használnak az eredetihez hasonló domaineket, mint például yOoutube.com, faceb00k.com, official-paypal.com.
- **Ellenőrizzük a https:// meglétét** azokon az oldalakon, ahol érzékeny adatokat kell megadnunk! Fontos, hogy ez önmagában nem elegendő művelet, ugyanis adathalász oldalakon is használhatnak ilyen protokollt.

- **Ne kattintsunk a hirdetésekre!** Helyette látogassunk el magára a webshopra és keressük meg az adott terméket!
- **Legyünk gyanakvók a kihagyhatatlan, sürgető ajánlatokkal!** A csalók gyakran hajszolják gyors, átgondolatlan lépésekre a felhasználókat ilyen módszerekkel.
- **Ismeretlen vagy korábban nem használt webáruház esetén részesítsük előnyben az alacsonyabb kockázatú fizetési megoldásokat!** Ha van rá lehetőség, az utánvétes fizetés csökkentheti annak kockázatát, hogy előre kifizetett összegért cserébe nem érkezik meg a megrendelt termék.

Diákmunka és albérletes csalások

Diákmunkát vagy albérletet keresők számára is mindenképp javasolt az óvatosság, ha **túl szépnek tűnik egy ajánlat**, de további figyelmeztető jelekre is – például, ha **sürgetnek vagy előre pénzt kérnek** – érdemes odafigyelni.

- Diákmunkára **kizárólag hivatalos szervezeten keresztül jelentkezzünk!** Az e-mailben, üzenetben vagy közösségi médiában kapott álláshirdetéseknél mindig ellenőrizzük a hirdető és a munkáltató valóságát, és **Ne kattintsunk** az e-mailben vagy közösségi oldalakon lévő álláshirdetésekre!
- **Kerüljük az érzékeny adatok megadását** (személyigazolványról, bankkártyáról stb. készült fotó) és **ne küldjünk pénzt előre** regisztrációs vagy képzési díj címszóval!
- **Ne telepítsünk ismeretlen programokat** vagy távoli hozzáférést biztosító alkalmazást egy „állásinterjú” vagy „munkafeladat” miatt!
- Albérlet keresés során **megtekintés nélkül ne utaljunk kauciót/óvadékot!** Különösen gyanús lehet, ha a hirdető arra hivatkozik, hogy külföldön tartózkodik, és a kulcsokat csak az előzetes utalást követően tudja átadni.
- **Ellenőrizzük a hirdetésben szereplő fényképeket!** Fordított képkereséssel kiderülhet, ha ugyanazokat a fotókat több, egymástól független lakáshirdetésben is felhasználták. Emellett érdemes számolni azzal is, hogy a csalók **mesterséges intelligenciával generált vagy manipulált képeket** is alkalmazhatnak, amelyek akár nem létező ingatlant is valónak tűntethetnek fel. Ezért a meggyőzőnek tűnő fotók önmagukban nem igazolják a hirdetés hitelességét; az ingatlant lehetőség szerint személyesen is tekintsük meg.
- Ragaszkodjunk az írásos bérlet szerződéshez! Mindenképp **kössünk szerződést**, amelyben szerepeljenek a felek adatai, a lakás címe, a bérleti díj és a kaució összege, valamint a fizetés és a bérleti jogviszony legfontosabb feltételei is!
- Az albérletes csalásokkal kapcsolatban további érdekességek és hasznos tudnivalók olvashatók egy korábbi tippünkben.

Ösztöndíjakkal kapcsolatos átverések

A tanévkezdési időszakban jellemzően megnő az e-mailben vagy közösségi oldalakon keresztül érkező **ösztöndíj témájú átverések**, amelyek általában **rövid jelentkezési**

határidővel sürgetik a felhasználókat a gyors, meggondolatlan interakcióra. A támadások során látszólag egy iskola nevében kérnek be **személyes adatokat vagy „adminisztrációs díjat” számítanak fel** az ügyintézés során.

- **Olvassuk át többször** az e-mailt, hátha találunk valami nem szokványosat az üzenetben (helyesírási hibát, megszólítás, tegeződés és magázódás váltakozása, stb)!
- Ne az üzenetben található hivatkozáson keresztül intézzük a jelentkezést! helyette inkább keressük fel az iskolai intézmény hivatalos weboldalát és ott tájékozódjunk az ösztöndíjprogramról!
- Bár az iskolai adminisztrációs teendők sokszor határidőhöz kötöttek, **ne engedjünk a sürgető, azonnali cselekvésre buzdító felszólításoknak!**

További hasznos tanácsok

Az iskolakezdés sok esetben jár együtt különböző felhasználói fiókok létrehozásával és kezelésével. Számos tanulást segítő alkalmazás és online szolgáltatás létezik, mint például a Google Classroom, a Doulingo, illetve ott vannak a teljeskörű online iskolai rendszerek is, mint a KRÉTA, amely számos különböző modullal támogatja a teljeskörű digitális oktatást és az ezzel kapcsolatos e-ügyintézés.

- Az alkalmazásokat **kizárólag megbízható forrásból** telepítsük! Soha ne töltsünk le alkalmazást hirdetésre vagy e-mailben érkező linken keresztül!
- Felhasználói fiókunk regisztrálásakor használjunk **hosszú, egyedi és erős jelszavakat**, amelyek legalább 12 karakter hosszúságúak, tartalmazzanak kis-és nagybetűt, illetve speciális karaktereket!
- Amennyiben módunkban áll, **állítsunk be kétfaktoros azonosítást (2FA)**!
- Soha **ne adjuk meg másnak** jelszavainkat, illetve biztonsági kódjainkat!
- Alkalmazzuk a **legkisebb jogosultság elvét**, vagyis minden rendszer, alkalmazás és személy csak azokhoz az adatokhoz férhessen hozzá, amelyekre ténylegesen szüksége van.