**„Zsebesek” az online térben**

A Magyar Nemzeti Bank adatai szerint 2023. II. negyedévében a kártyás vásárlások értékének 30 százalékát, azaz 1,3 ezer milliárd forintot online, különböző webshopokban költöttünk el. Szintén ebben a negyedévben a (bank)kártyás visszaélések száma jelentősen nőtt. Hogy mit jelent ez a gyakorlatban? Azt, hogy a kiberbűnözők kizárólag a figyelmetlenségünkre, a befolyásolhatóságunkra és a kapkodásunkra várnak – ami a karácsony közeledtével jellemzően egyre nő, ezzel együtt pedig az online csalások száma is.

**Adathalászat, pszichológiai manipuláció – üres bankszámla**

Egy riadalmat keltő telefonhívás, egy rémisztő kép és link a közösségi médiában, egy sürgető e-mail – néhány rossz kattintással máris vírust telepítettünk a számítógépünkre, kiadtuk személyes- vagy épp bankkártya adatainkat, másnap pedig arra ébredünk, hogy üres a bankszámlánk. Ez minden esetben dermesztő hír, de karácsony előtt még rosszabbul érinti az áldozatot. Épp ezért már a vásárlási hajrá előtt vértezzük fel magunkat a legfontosabb tudnivalókkal, hiszen az online csalók kizárólag a mi közreműködésünkkel férhetnek hozzá adatainkhoz. Nehezítsük meg a dolgukat!

**Mire figyeljünk?**

Sajnos a kiberbűnözők mindig egy lépéssel az áldozatok előtt járnak, azonban sikeresen megvédhetjük magunkat, ha odafigyelünk néhány apróságra, ha gyanakvóan kezelünk bizonyos helyzeteket, és annak megfelelő döntéseket hozunk.

- **Használjunk erős jelszót**! A 12 karakteres, kis- és nagybetűt, számot és speciális karaktert is tartalmazó jelszó megnehezíti a kiberbűnözők dolgát. Azonban a születési dátumokat, becenéveket, „123456” vagy „jelszó” típusú jelszavakat azonnal feltörik. A Nemzeti Kibervédelmi Intézet jelszó ellenőrző modulja segít a megfelelő erősségi védelmi vonal összeállításában.
- A megdöbbentően olcsó árakat kínáló oldalak, közösségi médiából érkező egyedi ajánlatok gyakran hamis weboldalra, webshopra irányítanak. Ezek **adathalász webhelyek, amelyeket kerüljünk el**!
- Amennyiben olyan webshopból rendelünk, ahonnan korábban még nem, **ellenőrizzük, hogy a cím „https”-sel kezdődjön**, valamint érdemes a **cégadatokat is áttekinteni**.
- Ha valahol **kizárólag külföldi értékeléseket** találunk, az **gyanúra ad okot**.
- **PIN kódot nem kérnek online vásárlás esetén**! Ha egy webshop ilyen adatot kér tőlünk, gyanakodjuk, és ne adjuk mega kódunkat!
- Mindig bizonyosodjunk meg róla, hogy **biztonságos fizetést garantáló oldalon tartózkodunk-e**! Ellenőrizzük, hogy helyesen szerepel az intézmény neve. Váljon gyanússá, ha „info”, „delivery” vagy „net” szerepel az url-ben!
- **Legyünk óvatosak a CVC-kóddal**! Soha ne adjuk ki személynek vagy gyanús oldalnak!
- **Kerüljük a nyilvános wifiket**! Ha online vásárolunk, azt otthonról tegyük meg!
- **Legyünk óvatosak a gyanús futárszolgálati, „vámfizetési” üzenetekkel**! Bevett csalási mód, hogy magukat futárküldő cégnek álcázva bírnak rá gyanútlan áldozatokat applikációk letöltésére a kiberbűnözők. Legyen körültekintő, csak megbízható forrású linkekre kattintson!

**Hová fordulhatok további információkért?**

A Pénzügyi Navigátor Digitális biztonság menüpontjára kattintva számos további hasznos információt talál, valamint érdemes felkeresni a KiberPajzs oldalt és Nemzeti Kibervédelmi Intézet honlapját.