

Karácsony előtti kapkodás, szuperakciók, vásárlások tömege – ez mind a kiberbűnözőknek kedvez

2023. 12. 14.



Az online vásárlás népszerűsége számos veszélyt is rejthet magában, különösen a karácsonyi időszakban, amikor a sok kedvezményes ajánlat között nehezebb kiszűrni az átveréseket. Néhány általános szabály betartásával azonban sokat tehetünk azért, hogy elkerüljük a csapdákat. Ebben segítünk most!

A karácsony előtti időszak a kiberbűnözők számára is aranybánya, hiszen rengeteget vásárolunk, sok az akció, ez kedvez az adathalászoknak és a kártyadatainkra áhítozóknak.

Biztos te is futottál már bele hamis ajánlatokba, visszautasíthatatlan akciót hirdető Instagram-posztokba vagy gyanús sms-be, ahol valaki megbízható futárcégnek adja ki magát, ezzel kérve további személyes adatokat. Ilyenkor hajlamosak vagyunk egyből rákattintani a szövegben található linkre, és másodpercek alatt egy olyan oldalra kerülünk, ahol személyes adatainkat és hitelkártya adatainkat kérik. Bármit is “vásárolunk meg”, vagy bármilyen további díjat fizettetek ki velünk azt sosem fogjuk megkapni, a befizetett pénz náluk landol és még a szenzitív adataink is idegenek kezébe kerülnek.

De hogyan lehet biztonságos a fizetés, hogyan ismerjük fel a biztonságos webáruházakat, hogyan lehetünk biztonságban az ünnepek előtt és alatt? Az [ESET biztonsági szoftverek](#) szakértői összegyűjtötték a legfontosabb tudnivalókat ahhoz, hogy a vásárlók biztonságban tudhassák pénzüket és adataikat.

1. Legyünk tisztában a kockázatokkal!

Legyünk elővigyázatosak a valószerűtlenül jó ajánlatokkal szemben, és legyünk tisztában azzal, hogy minél több eszközt használunk, és minél inkább függünk az online szolgáltatásoktól, annál nagyobb eséllyel esünk áldozatul.

2. Vásároljunk hivatalos webshopokból!

Hogy megbizonyosodjunk arról, egy weboldal megbízható, érdemes a kiskereskedő URL címét saját magunknak beírni ahelyett, hogy egy random linkre kattintunk. Figyeljünk a nyelvtani hibákra és más figyelmeztető jelekre, emellett ellenőrizzük, hogy az oldal HTTPS protokollt használ-e. Google keresést is lefolytathatunk egy adott kiskereskedővel és weboldallal kapcsolatban a fogyasztók véleményéről.

3. Óvakodjunk az átverésektől az online piactereken!

Mindig ellenőrizzük, hogy ki a hirdető, nézzük meg az előzményeket és a véleményeket, hogy megbizonyosodjunk a megbízhatóságról. Kerüljük a banki átutalást, és kérjük inkább más fizetési módok, például PayPal használatát, amely biztosítja a vevőt arról, hogy visszakapja a pénzét, ha nem kapja meg a megvásárolt terméket.

4. Válasszunk biztonságos fizetési módot!

Használjuk ki a modern technológiát a biztonságunk megóvása érdekében. Érdeklődjünk a bankunknál, hogy kaphatunk-e egyszer használatos virtuális kártyát egyedi vásárlásokhoz. Ezáltal, ha bedőlünk egy átverésnek, nem a valós számladatainkat adjuk meg, a virtuális kártya pedig nem használható újra. Igénybe vehetünk olyan biztonságos fizetési szolgáltatókat is, mint a PayPal, emellett előfizethetünk online vásárlási biztosításra is.

5. Használjunk olyan védelmi szoftvert, ami véd az online bankolás során, és jelzi, ha adathalász oldalra tévedünk.

6. Óvakodjunk azoktól az ajánlatoktól, amelyek valószínűtlenül jónak tűnnek!

Ez egy arany szabály az online átverések elkerülése érdekében. Ha egy ajánlat túl jó, akkor valószínűleg csalásról van szó.

7. Ne használjunk nyilvános Wi-Fi-t!

Komoly kockázatokat is rejtenek magukban, ezért soha ne használjuk őket például online vásárlásra vagy banki ügyintézésre. A támadók könnyen bejuthatnak egy rosszul védett hálózatba, hogy figyelemmel kísérjék potenciális áldozataik online tevékenységeit. A kiberbűnözők rögzíthetik a kapcsolaton keresztül továbbküldött adatokat – beleértve a jelszavakat és a banki adatokat -, és kártékony szoftverrel fertőzhetik meg az eszközt.

8. Használjunk VPN-t!

Amennyiben kénytelenek vagyunk nyilvános Wi-Fi hálózatot használni, a kockázatok minimalizálása érdekében használjunk virtuális magánhálózatot, vagyis VPN-t, amely titkosítja az adatokat a nyilvános hálózaton keresztül történő adatátvitel során.

9. Kétfaktoros hitelesítés (2FA) engedélyezése! A jelszavak vagy a jelmondatok (passphrase) használata kulcsfontosságú, ugyanakkor a 2FA, vagy a többtényezős hitelesítés (MFA) sokkal biztonságosabbá teszi a bejelentkezéseket fiókjainkba. Mindez történhet olyan egyszerű módon, mint az SMS-ben küldött számsor, amellyel bejelentkezhetünk, de ennél jobb megoldást jelent, ha a fiókunkkal párosított hitelesítő alkalmazáson vagy hardveres biztonsági kulcson keresztül érkezik az azonosító kód.

10. Tartsuk biztonságban eszközeinket!

Mindig frissítsük a legújabb operációs rendszert mobiltelefonunkra, laptopunkra vagy táblagépünkre, és tartsuk naprakészen az összes alkalmazást és egyéb szoftvert, amit használunk. Mindez nagyobb védelmet biztosít az ismert sebezhetőségekkel szemben, és megnehezíti a támadók számára, hogy feltörjék eszközeinket vagy ellopják adatainkat. Emellett fontos, hogy olyan digitális biztonsági megoldásokat használjunk, amelyek valós időben védenek a fenyegetésekkel szemben.

11. Vigyázzunk a sok személyes információt kérő oldalakkal!

Ha egy webáruház regisztrációjánál úgy érezzük, hogy túlságosan sok, és a vásárlás szempontjából nem releváns adatot is kérnek tőlünk, akkor azonnal fogjunk gyanút, és hagyjuk el az oldalt. Érdemes ilyenkor egy teljes vírus és kémprogram ellenőrzést is lefuttatni a gépünkön.

12. Ingyen kapott pénz még az interneten sem létezik!

Ha egy weboldal vagy még inkább, egy felugró pop-up ablak adatok, űrlapok kitöltögetése fejében értékes ajándékot, iPhone-t, iPad-et, "ingyen pénzt" vagy egyebeket ajánl, távozzunk.

13. Az ünnepek után is maradjunk figyelmesek!

Karácsony és Újév közti szünetben a hitelkártya egyenlegeket legtöbbször nem szívesen olvasgatják, talán mert nem szeretnének szembesülni azzal, hogy mennyit költöttek. Pedig az online vásárlás közbeni csalások, átverések során keletkezett kár a számlaegyenlegen mutatkozik meg először. Ha igénybe vesszük az SMS értesítési lehetőséget, percre készen láthatjuk a terheléseket a számlánkon. Minél előbb vesszük észre a gyanús tranzakciókat, és teszünk bejelentést, annál nagyobb az esély a szabálytalan ügyletek felderítésére, és ezzel együtt pénzünk esetleges visszaszerzésére.

További edukatív kiberbiztonsággal kapcsolatos információkért hallgass bele az [ESET Hackfelmetszők – Veled is megtörténhet!](#) c. podcastjébe!

Nem csak a felnőttekre leselkedik veszély az interneten, hanem a gyerekekre is. Azt gondolhatnánk, hogy a szülők ismerik ezeket a veszélyeket, de ez sajnos nem igaz.

Nem jellemző a szülőkre a tudatosság és a felkészülés, annak ellenére, hogy a kicsik egyre korábban kezdenek el okoseszközöket használni!



Egy európai felmérés szerint a 0-2 éves gyermekek 30%-a használ táblagépet. Egy 2012-es kutatás szerint 10%-uk első szava nem az anya vagy apa, hanem a tablet volt. Az [NMHH 2021-ben közzétett](#), 7-16 éves gyerekekkel és szüleikkel végzett kutatásából is az derült ki, hogy a gyerekek egyre hamarabb kezdenek netezni és közösségi oldalakat használni. A magyar tízévesek többségének már van mobiltelefonja, jellemzően okostelefon.

Ugyanakkor a szülők egy része sajnos nem tudja, sem azt, hogy milyen alkalmazásokat, játékokat, oldalakat használ a gyereke, sem azt, hogy mennyit használja. Sokan arra sem gondolnak, hogy az eszközöket használat előtt olyan modern biztonsági programmal kellene ellátni, ami a vírusok felismerése mellett védelmet nyújt a webkamerához történő hozzáférésekkel vagy az adathalászattal szemben is. De azt is érdemes tudatosítani, hogy ha megtörténik a baj – hackertámadás, adatlopás, zaklatás stb. – kihez fordulhatnak a gyerekek és a szülők.

„Ha megkérdezik a szülőket, mi a gyerekük kedvenc netes játéka, kik a kedvenc youtuberei, használ-e Twitchet, gyakran már a kérdést sem értik” – magyarázza **Csizmazia-Darab István, az ESET biztonsági szoftverek hazai forgalmazójának a Sicontact Kft.-nek az IT-biztonsági szakértője**. „Ezért kell sokat beszélgetni a gyerekekkel arról, hogy mit mivel szeretnek játszani, és megkérni őket, hogy mutassák meg ezeket”.

A szülők rendszerint az idegenektől, pedofiloktól féltik a gyermekeiket (pedig sokan maguk töltenek fel a gyerekeikről képeket a közösségi oldalakra), a gyerekek viszont a kiközösítéstől, a velük egykorúak zaklatásától és az online bántalmazástól tartanak.

Ezek a veszélyek fenyegetik a gyerekeket a digitális térben:

1. Életkoruknak nem megfelelő tartalmakat láthatnak; például nem nekik szóló filmeket, sorozatokat,

játékprogramokat, internetes tartalmakat.

2. Egy amerikai felmérés szerint a gyerekek negyede bármennyit netezhet, és naponta átlagosan 200 képet, valamint 10-20 videót lát.
3. A felvételeken a gyerekek akár erőszakos cselekményeket is láthatnak (például gyermekbántalmazást, állatkínzást, háborús sérüléseket), vagy törvénszegéssel kapcsolatos dicsekvést (például gyorsajtást).
4. Olyan életveszélyes netes „kihívások” terjednek időről időre, mint amilyen a vonat tetején utazás, az óvszer felszívása orron keresztül, mosószerkapszula nyelése, 48 órás eltűnés stb.
5. Webkamerás kukkolás.
6. Netre feltöltött fotókkal való visszaélés.
7. Álhírek, kamu videók: fake news, deepfake.
8. Pedofilok.

Az NMHH már idézett kutatásából az is kiderül, hogy a magyar szülők egy része egyáltalán nem figyeli, mivel foglalkozik a gyermeke a neten. Egyharmaduk passzív a gyermekük digitális életével kapcsolatban, vagyis nem tiltanak, nem korlátoznak, nem ellenőriznek semmit, és nem is beszélgetnek a netes tapasztalatokról. Pedig a kutatás szerint azoknak a szülőknek a gyerekei, akik odafigyelnek erre, jóval tudatosabbak a neten.

A kutatás egyértelmű eredménye, hogy a szülők bármilyen, a gyermek online jelenlétével kapcsolatos aktivitása, érdeklődése mérhetően csökkenti a gyerekekre leselkedő netes kockázatokat!

A megoldás viszont nem az, ha gyereket egy bizonyos életkorig eltiltjuk a digitális eszközöktől, az ugyanis nem fogja megóvni a veszélyektől, ráadásul emiatt ki is közhíthatik az osztálytársai.

Tiltás helyett a megoldás az, ha megtanítjuk a gyereket arra a nethasználatra, ami tanuláshoz, később a munkájához, boldogulásához kell, ha tudatosítjuk a kockázatokat, ha biztonságossá tesszük számukra a netezést, és ha mi magunk is követendő jó példát mutatunk: tudatos médiafogyasztással, tudatos eszközhasználattal és időbeosztással, „kütyümentes” időszakokkal.

„A tudatos szülői felügyelet valóban nehezebb a mai online világban, de közel sem lehetetlen” – mondja Csizmazia-Darab István IT-biztonsági szakértő. „De az őszinte kommunikáció és egyértelmű szabályok mellett már számos szoftveres megoldás is segíti a szülőket. Az ESET androidos telefonokra ingyenesen is letölthető szülői felügyelet alkalmazásával például szabályozható a gyermekek okostelefon és táblagép használata.”

Fontos, hogy már azelőtt védelemmel lássuk el az eszközöket, hogy azokat a gyerek kezébe adnánk.

Erre ügyelj, ha okoseszközt, kütyüt, videójátékot veszel karácsonyra a gyermekednek! Beüzemeléskor az eszköz valamilyen feloldó kód beállítását kéri. Válasszatok olyan kódot, ami nem köthető hozzátok, tehát nem a születési dátum vagy név kombinációja.

A gyerekekkel együtt nézd át, milyen alkalmazások kerülnek a telefonra vagy tabletre, és ellenőrizd, hogy

ezek mihez kérnek hozzáférést. Gyanús, ha egy app túl sok vagy furcsa hozzáférést kér.

Mindig a hivatalos áruházból töltsd le az appokat (Google Play, App Store), mert a nem ellenőrzött forrásokból beszerezhető appok kártevőket tartalmazhatnak, amelyek zárolhatják az eszközt, de kémkedhetnek is a gyerekek után.

Az okosórát is megbízható forrásból vásárold meg, vásárlás előtt ellenőrizd a modellt, és olvasd el róla a véleményeket. Keress rá az esetleges sebezhetőségre. Légy óvatos a kevésbé ismert vagy ellenőrizhetetlen márkákkal szemben.

A számítógépekhez és telefonokhoz hasonlóan, ha lehetséges, az eszközre telepítsd fel rendszeresen a biztonsági frissítéseket.

Amelyik eszközre telepíthető vírusirtó, ott gondoskodj erről: ne csak asztali gépen, laptopon, hanem okostelefonon és tableten is legyen vírusvédelem!

Az ESET Mobile Security Biztonsági audit funkciójával gyorsan át tudod tekinteni az alkalmazás engedélyeket, így meg tudod vonni azokat az engedélyeket az egyes alkalmazásoktól, amelyekre nincs szüksége a működéshez.

Az sem árt, ha felügyelni tudod a gyermeked online jelenlétét. Az ESET Parental Control for Android applikációja mobileszközökre telepíthető, és pár lépéssel beállítható rajta az alkalmazásfelügyelet, vagyis az, hogy milyen alkalmazást és mennyi ideig használhat a gyerek, de le is tilthatók az életkorának nem megfelelő alkalmazások.

Webfelügyelet és Biztonságos keresés segítségével korlátozható egyes weboldalak elérhetősége; külön kategóriák szerint tiltható le többek közt a szerencsejáték, a pornográfia vagy az alkohollal, droggal kapcsolatos tartalom. Így csak a gyerek életkorának megfelelő tartalmak jelennek meg.

A helymeghatározás azért lényeges, mert ellenőrizheted, éppen hol van a gyermeked. Beállíthatók a személyre szabott biztonsági zónák, például az iskola, az otthoni cím vagy mondjuk a barátok lakcíme, és értesítést lehet beállítani, ha a gyerek elhagy egy zónát vagy belép egy zónába.

A gyerek tevékenységéről az információkat az [ESET Home portálon](#) találod, ami számítógépről, mobiltelefonról és tabletről is elérhető.

Tanítsd meg azt is, mi a teendő, ha mégis megtörténik a baj, vagyis a gyereket zaklatják, káros vagy illegális tartalmat lát, ha szexuális céllal veszi fel vele valaki a kapcsolatot stb. Jelentse a kifogásolható tartalmat vagy zaklató üzeneteket, ezután kérjen segítséget egy megbízható felnőttől (szülőtől vagy tanártól). Ha szüksége van rá, forduljon az ingyenesen hívható anonim segélyvonalhoz, a Kék Vonalhoz. Ha zavaró, durva, illegális stb. tartalommal találkozik a gyerek, azt az NMHH-nak jelenthetitek. Ha pedig bármilyen abúzusról van szó, forduljatok a rendőrséghez.

A legfontosabb útravaló a biztonságos nethasználathoz és digitális jelenléthez:

- Legyetek biztonsággtudatosak és médiatudatosak.
- Használjatok vírusvédelmi és felügyeleti programot.

- Frissítések rendszeresen!
- Vigyázzatok az adataitokra beállításokkal és rendszeres mentésekkel.
- Használjatok a belépésekhez egyedi, erős jelszavakat és 2 faktoros hitelesítést.
- Óvjátok az eszközöket fizikailag is, például PIN-kóddal, képernyőzárral.
- Csak megbízható, legális forrásból töltsetek le alkalmazást!
- MerjeteK segítséget kérni a bajban.
- BeszéljeteK a gyereKkel rendszeresen az online térben történteKről.
- MutassateK jó példát.
- Legyen nálateK is egy digitális családfő, aki tud segíteni.



Digital Security
Progress. Protected.