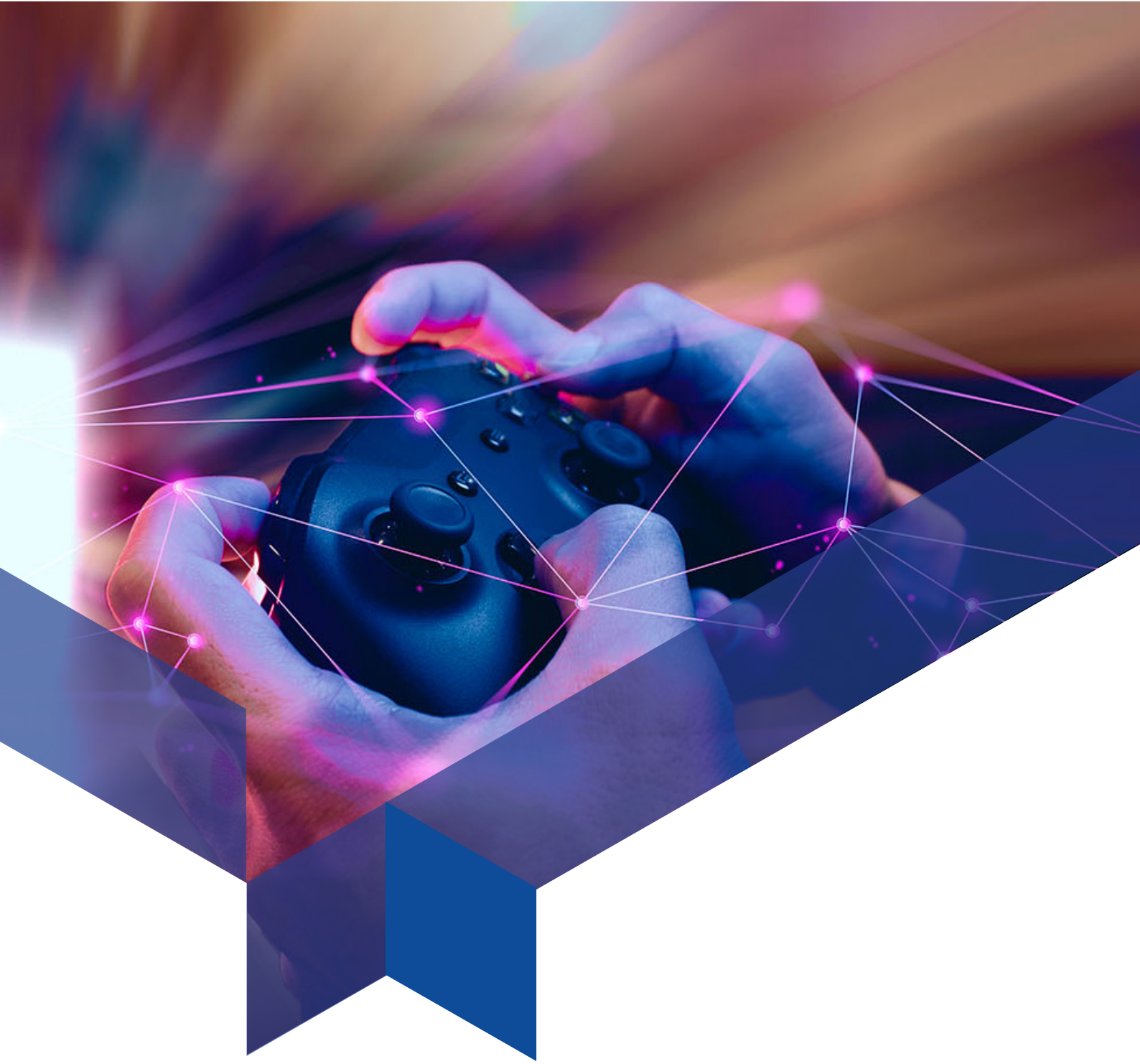
CTI Jelentés

Gamer platformok biztonsága és online tartalmak biztonságos vásárlása

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

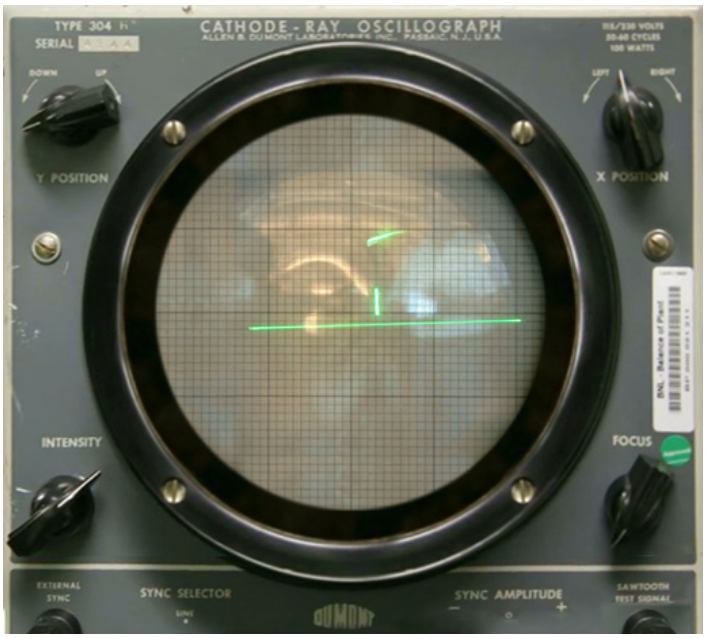
NEMZETI KIBERVÉDELMI INTÉZET

Tartalomjegyzék



Az Online gaming kialakulása, fejlődése és piaci részesedése

A fizikus William Higinbotham 1958-ban megalkotta a Tennis for Two-t, amely egy nagyon egyszerű videójáték volt, azonban hatalmas mérföldkőnek számít, ugyanis egy oszcilloszkóp segítségével ez lett az első olyan játék, amely grafikus kijelzőt használt.



A Tennis for Two játék egy oszcilloszkópon.
Forrás: commons.wikipedia.org

Ezt követően egyre több típusú játék készült, egyre szebb grafikával, amelyek fokozatosan a szórakoztatóipar egyre meghatározóbb tényezőjévé váltak.

Az 50'-es és a 60'-as években készültek olyan videójátékok, amelyeket egy számítógépen többen lehetett játszani. A különféle játékok gyártása és az Internet kialakulása majd fejlődése 1986-ban ért össze teljes mértékben,

amikor Gary Tarolli megalkotta az SGI Dogfight nevű játékot, amely először használt TCP/IP protokollt.

Jelen dokumentumban nem célunk a videójátékok evolúciójának részletes bemutatása, csupán rá szerettünk volna világítani arra, hogy közel 80 évvel ezelőtt kezdődött el ez az út, amely odáig vezetett, hogy a különféle játékok több milliárd ember szórakozását biztosítják nap mint nap. Bár ezek fő célja, hogy az emberek kikapcsolódhassanak, fontos megjegyezni, hogy az iparág napjainkra egy óriási méretű üzletté fejlődött. A GlobeNewswire szerint 2021-ben az online gaming – azaz az Interneten keresztül elérhető játékok – 56 milliárd dollár értékű volt, ami 2030-ra már valószínűleg a 132 milliárd dollárt is el fogja érni.

A fiatalok körében egyre népszerűbbek az egyes játékok, amelyekre sokan potenciális megélhetési forrásként is tekintenek. Ennek komolyságát mutatja, hogy a fogadóirodák már bevették a kínálatukba az egyes játékokat, és olyan versenyek lebonyolítására kerül sor minden évben, ahol az összdíjazások a több tíz millió dollárt is elérik.

A technológia egyre gyorsuló fejlődésével az egyes generációk más és más módon kötődnek az online gaminghez, hiszen van, aki anélkül nőtt fel, hogy valaha találkozott volna a kifejezéssel, mások pedig egy olyan világba csöppentek bele, ahol több száz millió 10 év alatti fiatal játszik internetes játékokkal napi rendszerességgel. Ezek a különbségek miatt teljesen máshogy viszonyulnak a mai kor fiataljai a játékokhoz és az Internethez, mint az idősebb korosztályok.

Amíg az Y generáció tagjai rendszerint 12-14 éves korukban kaptak először telefont, amely akkoriban még csak telefonálásra, SMS küldésre és zene hallgatásra volt alkalmas, addig az újabb generációk (Z és A) esetén jellemző, hogy már a kisiskolás gyermekek is rendelkeznek okostelefonnal, amely lényegesen több funkcióval rendelkezik.

Bár a telefonokon, tableteken, számítógépeken beállítható szülői felügyelet funkció sok esetben nagyon hasznos, fontos, hogy képesek legyünk átlátni, hogy pontosan mi az az online gaming, milyen jellemzői vannak, mire érdemes ügyelni és szülőként milyen szabályokat fontos betartatni a gyermekkel.

Mára mindez a gyermeknevelés szerves részévé vált. Előbb-utóbb minden gyerek találkozni fog az online játékokkal —ami ráadásul egyre fiatalabb korban következik be — és akkor lesz igazán fontos, hogy milyen nevelést, tanácsokat és információkat kapott a szüleitől. Egészségesen játszva a fejlődésüket és a szocializációjukat szolgálhatja, így érdemes fiatal koruktól kezdve biztonságos és egészséges szokásokra ösztönözni őket.

Mik azok az online gaming platformok?

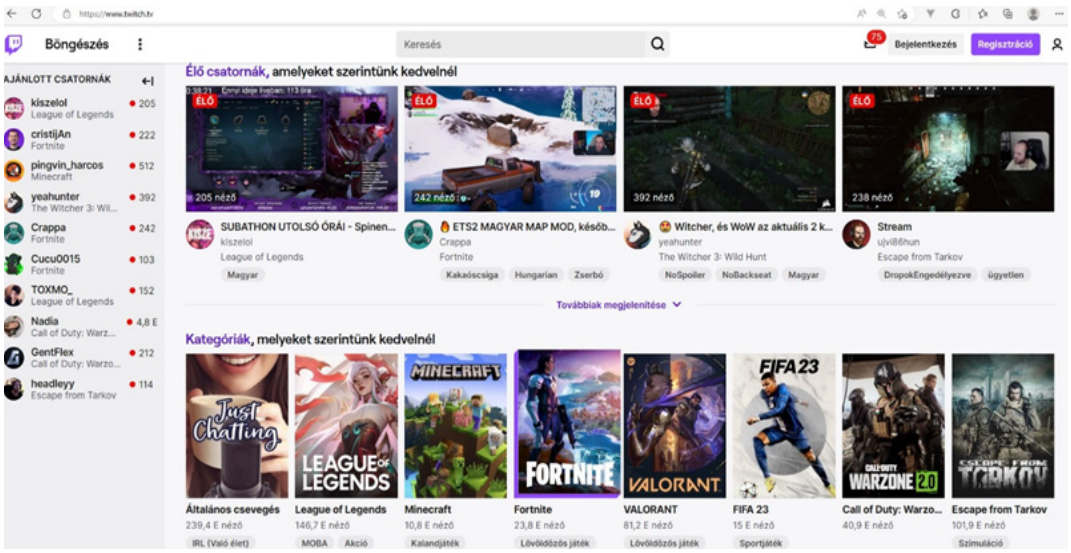
Online gamingről akkor beszélünk, ha egy videójátékban lehetőségünk van más játékosokkal az Interneten keresztül kapcsolatba lépni. Mértékét tekintve ez egészen eltérő lehet: egyes játékok esetében csupán egy közös ranglista mutatja, hogy nem egyedül játszunk és, hogy hol helyezkedünk el a rangsorban a többiekhez képest, más játékok esetén pedig láthatjuk a felhasználók avatárjait, és a játék a műfajától függően valamilyen interakcióba is léphetünk velük, például szöveges üzenetet válthatunk. Más szóval a felhasználó egy virtuális világban kapcsolatba tud lépni más emberekkel.

Eszközök széles választéka érhető el, amelyekkel az online térben tudunk játszani: számítógépek, laptopok, hordozható játékeszközök, telefonok, tabletek, konzolok és VR (virtual reality) eszközök

Játékra alkalmas eszközök

Az online gaming kapcsán fontos megemlíteni a hihetetlen népszerűségnek örvendő videostreaming platformokat, ahol lényegében azt nézhetjük, ahogy mások játszanak, vagy akármi is készíthetünk videófolyamot.

Elsősorban a 2010-es években robbant be a köztudatba a szórakozás ezen fajtája, és a hatalmas igények kielégítésére rengeteg féle streaming platform jött létre az elmúlt évtized során. A legnagyobb és legjelentősebb ezek közül a Twitch.tv, amelyet 2011-ben alapítottak. A felület olyannyira sikeresnek bizonyult, hogy a Google és az Amazon is versengett a felvásárlása miatt. Végül az utóbbi lett a befutó, a tranzakció pedig közel 1 milliárd dollárért valósult meg 2014-ben. A platform néhány kisebb visszaesést leszámítva folyamatos növekedésben van, és 2022 decemberére elérte a havi 140 millió egyedi látogatót. Bármelyik pillanatban egyidejűleg (átlagosan) 100 000 felhasználó streamel 2,5 milliós követőbázissal. A felhasználók 72%-a 16-34 év közöttiek, akik kétharmad részben férfiak



A twitch.tv weboldal

A Twitchhez hasonló online gaming platformok közé tartozik még a HitBox, Disco Melee, Gosu Gamers, Beam, Smashcast, Bigo Live, YouTube Gaming, Afreeca és az Azubu.

Az online gaminghez köthető veszélyek

A virtuális térben (és persze azon kívül is) minden olyan felület, közösség vagy csoport, ahol valamilyen célból jelentős tömegek gyűlnek össze nap mint nap, potenciális lehetőséget jelent az amatőr és profi csalók számára is. Kiváltképp igaz ez , ha emellé jelentős pénzforgalom is társul a platformon. Jó analógia lehet ennek megértéséhez, hogy például egy közönséges tolvaj milyen helyszíneket és célpontokat választ a profit maximalizálása érdekében: leginkább olyan színtereket, ahol rengeteg embert elérhet és ahol a potenciális áldozatok nem igazán figyelnek az értékeikre, vagyonukra. Nincs ez másképp az online térben sem, ahol rengeteg felhasználó érhető el, akik között jó eséllyel lesz olyan, aki figyelmetlen vagy gyanútlan. A következőkben áttekintjük azokat a leggyakoribb kiberfenyegetéseket, amelyek az online játékosokat érhetik.

Adathalászat

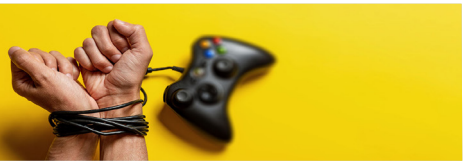
A jól ismert átverés azon változata, amely során a felhasználót arra próbálják rávenni, hogy adja meg személyes, például számlaadatait. A csalók a legtöbbször e-mailt küldenek a játékosoknak, amelyben közlik velük, hogy meg kell erősíteniük a bejelentkezési adataikat az egyes felületekhez.

Ha a játékosok rákattintanak az e-mail linkjére, egy hamis bejelentkezési oldalra kerülnek, ahol meg kell adniuk az aktuális jelszavukat és felhasználónevüket, amelyet a kiberbűnözők fel tudnak használni. A témában az NBSZ NKI korábban készített kiberbiztonsági elemzést, amely bemutatja az adathalászat legfőbb típusait és technikáit, és amiben olyan javaslatokat is teszünk, amellyel elkerülhetjük, hogy ilyen támadás áldozatává váljunk.

Cyberbullying

Az internetes zaklatás, avagy az úgynevezett cyberbullying alatt olyan cselekményt értünk, amelyben az áldozathoz elektronikus úton eljutó információk durvább csúfolódásokból, kárörvendésből és fenyegetésből állnak, melyet egy vagy több felhasználó végez ismétlődő alkalmanként. Ez történhet online többszereplős játékcsevegésekben is, ahol rendszerint teljesen ismeretlenek tanúsítanak ilyenféle viselkedést a fiatalokkal szemben. Sok szülő azért bagatellizálja el ezt a témát, mert úgy gondolják, hogy a gyermekük nem lép fizikai kapcsolatba ismeretlenekkel, így valós veszély nem is fenyegeti őket. A témával részletesebben az NBSZ NKI korábbi elemzése foglalkozik.

Függőség

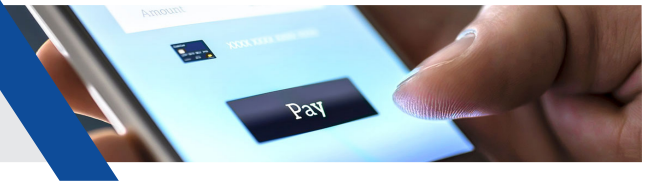


Nem megfelelő tudatossággal és a mértékletesség hiányával egyes játékok komoly addikciót válthatnak ki kortól függetlenül. Olyan pszichológiai hatásai lehetnek, amelyet nem, vagy később csak nagyon nehezen, komoly idő- és energiaráfordítással tudunk korrigálni. Ilyenkor az online játék már csak kis mértékben, vagy egyáltalán nem a szórakozásról szól, a játékos akár megszakítás nélkül teljes napszakokat tölthet el a virtuális térben, teljesen mellőzve a valós világot és környezetét. Ilyenkor az egyén teljesen megszállottá válik, sokszor akkor is a játékra gondol, amikor nincs gép közelben, és igyekszik minél hamarabb ismét játszani. Ez veszélyes lehet, mert nagy mennyiségű időt emészthet fel, a valós emberi kapcsolatok rovására is mehet és egészségkárosító hatása is lehet, például a mozgás hiányának kialakulása és a táplálkozási szokások negatív irányba történő változása miatt.

Rosszindulatú szoftverek

Előfordulhat, hogy a felhasználók olyan frissítéseket vagy akár komplett játékokat töltenek le (például egy torrent hálózatról), amelyekbe a kiberbűnözők káros kódokat rejtettek el. Fontos, hogy mindig csak jogtiszta, megbízható forrásból (gyártói alkalmazásboltok és játék platformok), töltsünk le játékokat!

Rejtett díjak

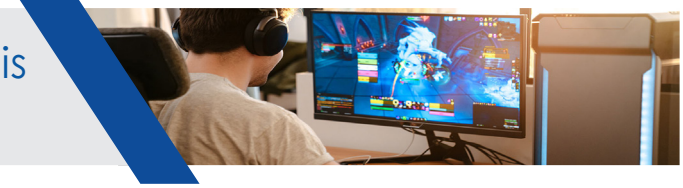


Egyre népszerűbb az úgynevezett **freemium modell**, amelyben a vállalat **ingyen** kínálja a szoftverét, azonban a **teljes funkcionalitáshoz már fizetni kell**. Egyes esetekben ezek a játékok megkövetelik, hogy a felhasználók hitelkártyát csatoljanak a játékprofiljukhoz, és a kártyát automatikusan megterhelik, amikor a felhasználók új elemeket vagy szolgáltatásokat vásárolnak.

Harmadik fél webhelyeire való átirányítás

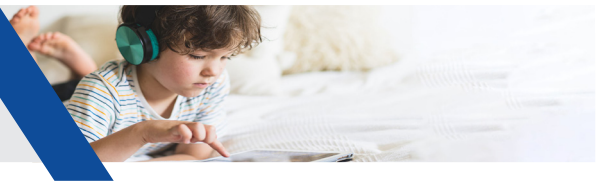
Ezek valódi weboldalaknak tűnnek, ahol a felhasználók bizonyos játékelemeket megvásárolhatnak, hogy előnyre tegyenek szert a játékostársaikkal szemben, de valójában **ezek az oldalak hamisak és becsapják a felhasználókat, hogy ellophassák a pénzüket**, rendszerint adathalász technikákkal.

Népszerű játékok hamis verziói



Letöltés után ezek az alkalmazások **rosszindulatú szoftvereket telepítenek** az áldozatok eszközeire, amelyek segítségével megszerezhetik a játékosok online fiókjainak adatait, hogy ellophatják a felhasználók érzékeny adatait, például hitelkártya adatokat, lakcímeket vagy telefonszámokat.

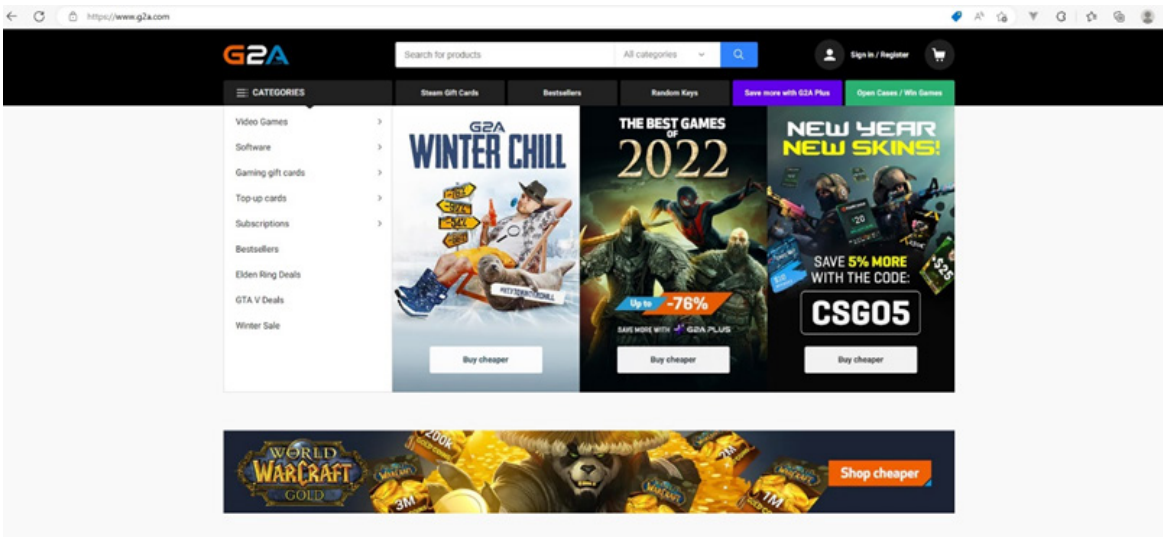
Gyermekek megcélzása



A kiberbűnözők rávehetnek kis- vagy fiatalkorú gyerekeket, hogy fizessenek helyettük a játékokban található virtuális tárgyakért a szüleik bankkártyájával. Ezek a csalók meggyőzik a gyerekeket, hogy adják meg nekik a bejelentkezési adataikat, vagy nyissanak meg egy általuk küldött linket, hogy hozzáférjenek a fiókjukhoz, így akár megszerezhetik a gyerek szüleinek bankkártya adatait is. Az ellopott adatokat ezután tovább értékesíthetik a darkweben.

G2A csalások

A G2A egy digitális piactér, amely a játéktermékek viszonteladására specializálódott. Az oldalon értékesített termékek között szoftverek, aktiváló kódok és elektronikai cikkek szerepelnek. A G2A-nak több mint 20 millió felhasználója van.



Az itt lebonyolított üzletek jellegéből fakadóan rengetegen vertek át másokat, például hamis telepítő kulcsok eladásával. Mivel ez a G2A rossz hírnevét keltette, lépéseket tettek a csalások megelőzésére. Az eladóknak ma már igazolniuk kell a személyes adataikat és a telefonszámukat, és 10 tranzakcióra korlátozódnak, mielőtt további igazolást kell benyújtaniuk. A cél egyértelműen az volt, hogy a kétes eladók ne tudják átverni nem működő játékkódokkal a vásárlókat, azonban a platform a pénzvisszatérítést 2 feltételhez köti: az áldozatnak rendőrségi feljelentést kell tennie és évente maximum 3 alkalommal jogosult a visszatérítésre. Ezzel a lépéssel a legtöbb kisértékű csalás következmény nélkül marad, mivel potenciálisan több időbe, energiába és pénzbe kerülne feltárni a bizonyítékokat és felelősségre vonni a csalókat.

A G2A alternatívái közé tartozik a Kinguin, Gamivo, AllKeyShop, CDKeys és az SCDKey.

Online tartalmak biztonságos vásárlása

A játékokon felül megannyi digitális termék létezik, amellyel nap mint nap találkozhat és megvásárolhat a felhasználó. Egy digitális terméket online értékesítenek és nincs fizikai formája vagy anyaga. Egyes digitális termékek fizikai termékekké alakíthatók, például egy e-book vagy recept PDF formátumban kinyomtatható, de a legtöbb termékre ez nem jellemző. Ilyen online tartalmak lehetnek a kurzusok, fotók, zenék, alkalmazások, különféle szoftverek, websablonok, oktatóanyagok, e-könyvek, podcastek stb.

A legtöbb esetben, ha szükségünk van valamilyen termékre, egy kereséssel fogjuk indítani a vásárlást: hol és mennyiért található meg egy adott produktum. A legfontosabb, hogy mindig jóhírű, ismert weboldalról vásároljunk, és soha ne a legolcsóbb ár legyen a legfontosabb szempont, ugyanis a csalók legtöbbször az akciós árakkal igyekeznek átverni minket. Ha például egy szoftvert mindenhol 10 vagy több dollárért árulnak, legyen gyanús, ha valahol már 1-2 dollárért hozzájuthatunk! Ha találunk egy legitimnek tűnő oldalt, érdemes felhasználói véleményekre keresni, hogy meggyőződhessünk, hogy valóban legitim-e.

Amennyiben eladni szeretnénk digitális tartalmakat, számos lehetőség tárul elénk. A legismertebb oldalak a Sellfy, Podia, Payhip, SendOwl, BigCommerce, Squarespace, DPD, Gumroad, Thinkfic, MemberPress, Easy Digital Downloads. Attól függően, hogy mit szeretnénk értékesíteni, járjuk körbe a témát és győződjünk meg, hogy melyik a profilunknak leginkább megfelelő!

Az NBSZ NKI javaslatai a biztonságos online gaminghez

- Amennyiben megtehetjük, használjunk VPN szolgáltatást! A VPN-ek a személyes internetkapcsolatot priváttá teszik, így anonim módon tudunk jelen lenni a virtuális térben. Az ingyenes szolgáltatások a kipróbálás erejéig jó megoldások lehetnek, azonban ezek rendszerint korlátozott adatmennyiségig elérhetők, így javasoljuk egy megbízható fizetős VPN beszerzését. Fontos, hogy ha elérhető, aktiváljuk az automatikus frissítést, hogy a szoftveres sebezhetőségek javításai minél előbb települjenek.

- Mielőtt VPN terméket választunk, olvassuk el a szolgáltatás feltételeit és az adatvédelmi irányelveket is! Bár egyes VPN szolgáltatók azt állítják, hogy védelmet nyújtanak a rosszindulatú programok és az adathalász oldalak ellen, érdemes ezt önálló vírusirtó szoftverekkel együtt használni a legmagasabb védelmi szint elérése érdekében!

  Csak hivatalos weboldalakat használjunk a játékkal kapcsolatos vásárlásokhoz. Ne kattintsunk olyan linkekre, amelyek harmadik fél webhelyeire irányítanak át!

- Használjunk olyan megbízható forrásokat, mint a Google Play Store, Apple App Store vagy az Amazon Appstore!

- Ne válaszoljunk a banki, pénzügyi vagy személyes adatainkat kérő e-mailekre vagy a platformokon belüli közvetlen üzenetekre, még akkor sem, ha úgy tűnik, hogy az üzenet a játék fejlesztőjétől érkezik, mivel ők soha nem kérnek személyes adatokat üzenetváltás útján!

- Ne osszunk meg online személyes adatokat, azonosító adatokat vagy számlainformációkat!
- A bejelentkezési adatainkat ne osszuk meg senkivel, beleértve a barátainkat is!
- Használjunk kétfaktoros hitelesítést!
- Soha ne kattintsunk olyan linkekre, amelyek a jelszó megerősítését kérik!
- Ha G2A-n keresztül vásárolnánk termékeket, győződjünk meg arról, hogy olyan eladótól vásárolunk, akinek sok pozitív értékelése van (ideális esetben magasabb, mint 90%)!
- A G2A-n fokozottan ügyeljünk arra, hogy kitől vásárolunk, ugyanis a vásárlók csak negatívról pozitívra változtathatják az értékelésüket, fordítva nem, így a későbbiekben kiderült problémák nem feltétlenül látszódnak az értékelésekben!
- A megbízható online áruházak közé tartozik a Steam, Humble Bundle, Fanatical, Epic Games Store, GameFly, itch.io, Xbox PC app, GreenManGaming, IndieGala, GoG, de ide tartozik az IsThereAnyDeal nevű weboldal, amely segítségével több mint 30 legális online áruház kedvezményeit, csomagjait és ajánlatait követheti nyomon. Az oldalon importálható a Steam kívánságlista, és e-mailben értesítenek, ha valamelyik játék akcióssá válik.
- Mobileszközeinkkel, laptopokkal mindig kerüljük el a nyilvános Wi-Fi hálózatokat, használjunk helyettük mobilinternetet!

Hogyan tartsuk biztonságban a gyermekeket?

- Ha a fiatalkorú gyermekünk rendszeresen jelen van a virtuális térben, fontoljuk meg a szülői felügyelet beállítását! Függetlenül attól, hogy milyen eszközt használ a gyermek, ezzel mi határozhatjuk meg, hogy hogyan léphet kapcsolatba más játékosokkal, például csak a meglévő barátokkal! A szülői felügyelet segítségével azt is korlátozhatjuk, hogy mennyi ideig tudjon játszani gyermek.

- Ellenőrizzük mindig a játék tartalmát! A legtöbb játéknak van korhatár besorolása, így például az erőszakos vagy szexuális tartalmú játékok magasabb besorolást kapnak. Az Entertainment Software Rating Board oldalon ezt ellenőrizhetjük.

- Győződjünk meg róla, hogy a gyermek olyan felhasználónevet választ, amely nem árul el személyes adatokat! Ha a játék lehetőséget ad személyes profil létrehozására, győződjünk meg róla, hogy gyermek nem ad ki semmilyen személyes adatot, például nevet, életkort, lakóhelyet, iskolát, pénzügyi információkat vagy fiókjelszavakat!

- Győződjünk meg arról, hogy a gyermek a játék engedélyezett, törvényes forrásból származó verzióját futtatja! Világosítsuk fel az illegális letöltések, a fájlcserélő oldalak és a játékok kalózmásolatainak kockázatáról, mivel ezekben nagy a rosszindulatú programok kockázata!

- Mutassuk meg a gyermeknek, hogyan jelenthet vagy blokkolhat más felhasználókat a választott platformokon!
- Olvassuk el a játék feltételeit és ellenőrizzük, hogy nincsenek-e rejtett díjak!
- Szerezzünk információt arról, hogy hogyan kezeli a játék fejlesztője az elfogadhatatlan viselkedéseket és tartalmakat!
- Győződjünk meg róla, hogy frissített vírusirtó szoftver fut a gyermek az eszközökön!
- Mint az élet legtöbb területén, a kommunikáció a legfontosabb, ezért beszélgessünk az alábbi témákról a gyermekkel! Főbb és releváns témák lehetnek:

  - a biztonságos online tartózkodás,
  - milyen típusú játékokkal kellene játszania,
  - mások miért nem feltétlen azok, akiknek kiadják magukat,
  - mit illik és mit nem illik mondani online játék közben,
  - biztosítsuk, hogy nyugodtan megoszthatja velünk, ha inzultus éri, vagy ha úgy érzi, hogy folyamatosan zaklatják!

Teendő, ha online játékkal kapcsolatos átverés áldozatává válnánk:

- Küldjünk részletes jelentést a játék support felületén!
- Amennyiben anyagi kárt szenvedtünk el, vegyük fel a kapcsolatot a bankunkkal! Amennyiben lehetséges, az eseteket kivizsgálják és visszatérítést is kaphatunk tőlük.
- Ha személyes adatokat adtunk meg a csalóknak, tanácsos minden jelszót megváltoztatni (netbank, közösségi média, e-mail fiók, stb)!
- Ha egy csaló megfenyegeti bennünket, jó ha tudjuk, hogy lehetőségünk van rendőrségi feljelentést tenni!

Milyen szempontokat érdemes figyelembe venni jelszóválasztásnál?

- Ne legyen ránk jellemző, mert kevés információ birtokában is könnyen kitalálható (pl.: családtag neve + születési dátum egy rövid kereséssel a közösségi oldalakon kideríthető).
- Nem szerencsés, ha a jelszó csak egy szóból áll (például az „almafa" szó biztosan szerepel egy támadó által kipróbálandó jelszavak listájában).
- Jó, ha a jelszó hosszú és többféle karaktert (kisbetű, nagybetű, szám, írásjel) tartalmaz, mert ezzel megnehezíti a brute force technikával való feltörést.
- A legjobb, ha néhány szóból álló jelmondatot választunk, amelyben van kisbetű, nagybetű, szám és írásjel is. Ezt könnyű megjegyezni, azonban nehéz kitalálni, brute force technikával feltörni pedig szinte lehetetlen.

Hogyan kezeljük a jelszavainkat?

- Fontos, hogy ne adjuk „kölcsön" a jelszavunkat, hiszen nem tudhatjuk, hogy az adott személy körültekintően fogja-e kezelni.
- Ne írjuk fel a jelszavunkat, mert ez könnyen illetéktelen kezekbe kerülhet.
- Ne használjuk mindenhol ugyanazt a jelszót, ha a támadók egyet feltörnek, minden más rendszerünkhöz is hozzáférhetnek.
- Rendszeresen változtassuk meg a jelszavainkat, a támadónak minél több ideje van próbálkozni, annál nagyobb valószínűséggel tudja megszerezni a hozzáférésünket.
- Használjunk valamilyen jelszókezelő rendszert! Ezek olyan szoftverek, amelyek titkosított formában tárolják jelszavainkat, így azokhoz illetéktelenek (ideális esetben) nem — vagy csak irreálisan nagy erőforrás ráfordításával — férhetnek hozzá. A megoldás előnye, hogy ehhez csupán egyetlen, ún. mesterjelszót kell fejben tartanunk, azt, amellyel hozzáférhetünk az elmentett jelszavakhoz. A jelszókezelőkről bővebben az NBSZ NKI weboldalán itt írtunk.

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2023