Biztonságban a neten –

kiberbiztonsági tippek diákoknak az ESET-től

www.eset.com/hu/digitalis-biztonsag/fiataloknak/

ESET®

Digital Security

Progress. Protected.

Te is a neten tartod a kapcsolatot a barátaiddal, vásárolsz, olvasod a híreket és osztod meg az élményeidet?

És hallottál már a cyberbullyingról, az adathalászatról vagy a személyazonosság-lopásról?

Európa egyik vezető kiberbiztonsági vállalatánál, az ESET-nél és hazai forgalmazójánál, a Sicontact Kft.-nél szívügyünk az internetes biztonság, különösen, ha Rólad, Rólatok, azaz diákokról van szó.

Legfrissebb felmérésünk[1] szerint a diákok harmada úgy gondolja, hogy kifejezetten tájékozott a kiberbiztonságot érintő kérdésekben, kétharmaduk pedig ismerni véli a főbb veszélyeket és védekezési módokat.

Mégis, csak minden ötödik diák érzi magát teljesen biztonságban neten. A legtöbben (78%) az adathalászattól, személyazonosság-lopástól és profil feltöréstől tartanak. A diákok többsége (54%) fél a kártevő programoktól, kéretlen levelektől és rosszindulatú appoktól, és minden második diák tart attól, hogy online vásárlás miatt kerül bajba. A felmérésben résztvevő diákok amiatt is aggódnak, hogy információk, képek szivárognak ki róluk a közösségi médiában (43%), cyberbullying, azaz online zaklatás és gyűlöletkeltés áldozatává válnak (35%), vagy online ragadozók környékezik meg őket (28%).

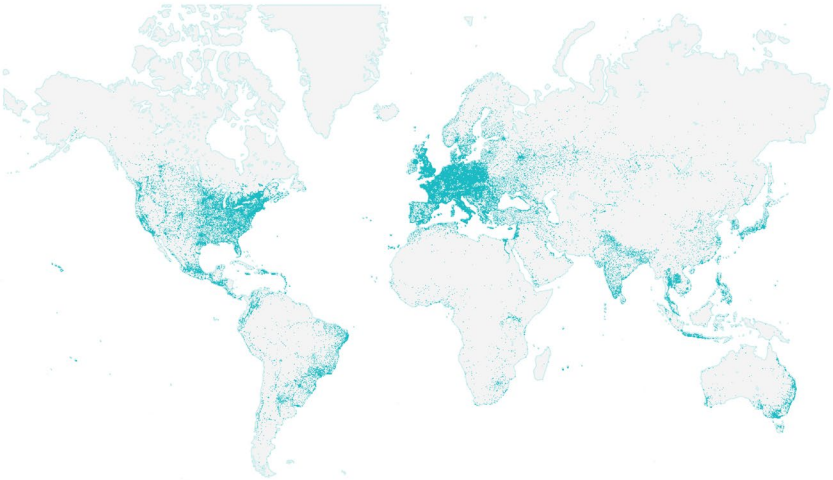
Ezekről a veszélyekről már biztos Te is hallottál, de talán még nem ismered az összes trükköt, amivel túljárhatsz az online csalók eszén.

Ebben a rövid kisokosban szeretnénk veled együtt körbejárni az internetes veszélyforrásokat, és egyszerű, hasznos tippeket is adunk, amelyek segítségével biztonságban lehetsz, és a netezés minden előnyét élvezheted!

1 2022 májusában 200 diák bevonásával készítettünk felmérést kiberbiztonság témában.

KIK VAGYUNK MI?

Az **ESET** internetbiztonsági megoldásai világszerte 202 országban több mint 110 millió otthoni felhasználó és vállalkozás védelmét biztosítják az online térben. Küldetésük, hogy a digitális tér mindenki számára biztonságos hely lehessen. Ennek érdekében számos hasznos tanáccsal látják el a felhasználókat, melyeket a több mint 30 éves tapasztalatuk mellett IT biztonsági szakértők és kártevőkutatók segítségével állítottak össze.



A **Sicontact Kft.** az egyik legjelentősebb, IT biztonsággal foglalkozó hazai szoftverdisztribútor, az ESET termékek kizárólagos forgalmazója Magyarországon. Célunk, hogy felhívjuk a figyelmet az online világ kockázataira, és hasznos tudnivalókkal, egyszerűen alkalmazható tippekkel segítsük a diákokat, a szülőket és a tanárokat. Szakértőnk, Csizmazia-Darab István jó tanácsaival és elemzéseivel rendszeresen találkozhatsz a sajtóban és az **Antivírus blogon**, de hallhattad már őt a rádióban, televízióban és rendezvényeken is.

MIK IS AZOK A NETES (DIGITÁLIS) ESZKÖZÖK?

Számítógép, laptop, mobil. Egyértelmű, igaz? De gondoltál már arra, hogy valójában az okosórád is egy internetes eszköz? Fontos, hogy minden olyan „hardware-t", amely a netre tud csatlakozni, körültekintően használj.

Ezek a digitális eszközök a következők lehetnek:

- számítógép és laptop
- okostelefon
- tablet
- okostévé
- okosóra és egyéb „okoskütyük"
- játékkonzolok

Melyek a leggyakoribb netes veszélyek? És hogyan járhatsz túl az online csalók eszén?

1) Adathalászat, személyazonosságlopás, profil feltörés

Mindhárom veszély a személyes adataiddal való visszaélésről szól. A bűnözők gyakran a közösségi média profilokon nyilvánosan elérhető adatok segítségével férkőznek az áldozatok bizalmába, illetve adathalász e-mailekkel jutnak bizalmas információkhoz.

Ezek az adatok lehetnek jelszavak, azonosító számok, hitelkártya-, vagy társadalombiztosítási adatok, amelyeket aztán a csalók a legkülönbözőbb **törvénytelen célokra** használhatnak: igényelhetnek például a nevedben hitelt, letilthatják a SIM kártyádat, vagy nagyobb értékben is vásárolhatnak a pénzedből a neten.

Sőt, középtávon akár Te is felelősségre vonható lehetsz a nevedben elkövetett cselekményekért, és egy esetleges nyomozás során jogi költségekkel, vagy a jó híred sérülésével is szembe kell nézned.

A profilfeltörés ellen legegyszerűbben erős, egyedi jelszavakkal és kétfényezős hitelesítéssel védekezhetsz. Biztos neked is van jónéhány online fiókod, amelyeken személyes és pénzügyi adatokat is tárolsz. Sajnos sokan használnak mindenhol teljesen egyező rövid és gyenge, vagy egymáshoz nagyon hasonló jelszavakat, hogy könnyebb legyen megjegyezni őket. Ráadásul a jelszó frissítés is el szokott maradni, pedig fél-egy évente érdemes lecserélni minden jelszavadat.

A legfontosabb: a biztonságos internet kapcsolat

✔ Használj otthoni vagy iskolai hálózatot, vagy mobilnetet, kerüld a jelszóval nem védett nyilvános Wi-Fi kapcsolatokat.

✔ Ha ezek közül egyik sem elérhető, használj virtuális magán hálózatot (VPN), ami titkosítani fogja az összes adatot, és megvéd téged, illetve az adataidat.

Ne tedd nyilvánosan elérhetővé a saját és az ismerőseid személyes adatait

Akár egy egyszerű szülinapi fotó nyilvános megosztásával is rengeteg személyes adatot tehetsz közzé. Például kiposztolsz egy csoportképet „Boldog szülinapot, Anna!" szöveggel. Máris közzétetted a barátnőd fotóját, nevét, születési dátumát, és akár a földrajzi elérhetőségét is. Az adatok könnyen felhasználhatók személyazonosság-lopáshoz, és segítségükkel bárki rossz szándékkal a Te, vagy barátaid bizalmába férkőzhet.

✔ Ne ossz meg magadról vagy a barátaidról publikusan személyes adatot (név, lakcím, születési idő, stb.) és hiányos öltözetű képet

✔ A fotózáskor kapcsold ki a helymeghatározást

✔ Mindig ellenőrizd az adatvédelmi szűrőket és a bejegyzés célközönségét

Használj erős jelszavakat és többfaktoros hitelesítést

A profilod feltörése ellen legegyszerűbben erős, egyedi jelszavakkal védekezhetsz. Biztos neked is van jónéhány online fiókod, amelyeken személyes és pénzügyi adatokat is tárolsz.

✔ Kerüld a könnyen feltörhető, primitív (pl. qwerty, 12345, abc, stb.), illetve a hozzád személyesen köthető szavakat, neveket és évszámokat. Ha ebben segítségre van szükséged, használd az **ESET ingyenes jelszógenerátorát**!

✔ Extra biztonságot jelent a több faktoros hitelesítés is. Ilyenkor a jelszó megadása mellett leggyakrabban egy SMS-ben vagy e-mailben kapott kódot kell megadni. Ennél is biztonságosabb választás a dedikált hitelesítő alkalmazás vagy hardveres megoldás, például hitelesítési tokenek használata. Ha több faktoros hitelesítést használsz, akkor arról is értesülsz, ha illetéktelenek próbálnak hozzájutni a fiókodhoz.

✔ A jelszavaidat ne oszd meg senkivel! A szolgáltatók, bankok, hivatalos szervek sosem kérik emailben a jelszavad megadását, ezért ha ilyen levelet kapsz, az valószínűleg átverés.

Ismerd fel az adathalász e-maileket

Az alábbi esetekben jó eséllyel adathalász e-maillel van dolgod:

✔ Túl általános a megszólítás, például: Tisztelt Ügyfelünk

✔ A feladó személyes információkat kér, pedig a bankok, szolgáltatók nem szoktak ilyen adatokat kérni e-mailben

✔ Rossz a levél helyesírása, nyelvtanilag hibás mondatok szerepelnek benne

✔ Váratlanul megkeresnek egy olyan szolgáltatótól, amellyel nem is álltál kapcsolatban

✔ Sürgetnek, amellyel meggondolatlan döntésre ösztönöznek

✔ Visszautasíthatatlan ajánlatot kapsz, amely túl szép ahhoz, hogy igaz legyen

✔ Gyanús címről, Kínából, Indiából, egy afrikai országból, vagy esetleg egy celeb, influencer nevében keresnek meg

Védd az eszközeidet szoftver szinten

✔ Használj olyan internetbiztonsági megoldást, amely szoftveres szinten képes védeni az eszközeidet, ilyen például az **ESET Internet Security**, amelyet ingyenesen is ki tudsz próbáni.

✔ A számítógéped, laptopod mellett az okostelefonodra és tabletedre is telepíts megbízható biztonsági alkalmazást.

✔ Válassz olyan szoftvert, amely a hagyományos vírusvédelem mellett biztonságot nyújt az online vásárlás, netbankolás és a webkamera használat során, illetve tartalmaz adathalászat elleni védelmet is.

2) Kártevő programok, rosszindulatú appok és kéretlen levelek

Az interneten számos vírussal, kártevővel találkozhatsz, amelyek különböző módszerekkel fertőzik meg az eszközeidet. A zsarolóvírusok például olyan kártevő programok, melyek segítségével a bűnözők zárolhatják az eszközödet vagy titkosíthatják az eszközödön lévő adatokat. Ezt követően a képernyődön megjelenő ablakban, vagy egy dokumentumban azzal zsarolhatnak meg, hogy egy bizonyos összegért cserébe visszaállítják a hozzáférésedet a gépedhez és az adataidhoz.

✔ Ismerd fel az adathalász e-maileket (lásd fent), hiszen gyakran olyan mellékleteket vagy linkeket is tartalmaznak, melyekre kattintva az eszközt megfertőzik a kártevő programok.

✔ Ismerd fel a híres márkának vagy szervezetnek álcázott, hamis weboldalakat, és véletlenül se kattints az ezeken szereplő linkekre. A domain név árulkodó lehet: csupán egyetlen betű vagy karakter is gyanús, ha eltér a valódi márka, vagy szervezet nevétől. Keress rá a hivatalos domainre egy keresőmotor segítségével is.

✔ A kéretlen levelek, reklámok nem csak bevételt generálnak a weboldal üzemeltetőjének, hanem gyakran tele vannak kártevőkkel is. Használj reklámblokkoló bővítményt a böngésződben!

✔ Használj naprakész biztonsági megoldást, vírusirtót az eszközeiden. Az **ESET Internet Security** ebben az esetben is megvéd, mivel a vírus- és kémprogramvédelmen kívül levélszemétszűrőt is tartalmaz.

3) Online vásárlás

Online vásárlás esetén is jobb, ha körültekintő vagy. Ha például márkás, vagy luxuscikkekre vágysz, Te is biztos tudod, hogy mélyen a (virtuális) pénztárcádba kell nyúlnod ahhoz, hogy tiéd lehessen a kiszemelt kincs. Sajnos a csalók is jól tudják, mik a divatos trendek, ezért gyakran kínálnak a közösségi médiában népszerű termékeket nevetségesen alacsony áron, hogy aztán egy hamis webáruházban való vásárlás után ne kapj semmit, vagy a legrosszabb esetben még a bankszámládat is lenullázzák.

Vigyázz az ajándékkártyás és kuponos akciókkal is, hiszen a csalók ezekkel is megpróbálhatnak rábírni a kattintásra, amivel aztán adathalász oldalra kerülhetsz, de akár banki trójai vagy billentyűzetfigyelő vírust is letöltődhet a gépedre.

✔ Biztos Te is tudod, mennyibe kerül valójában a kiszemelt termék, ne dőlj be az irreálisan alacsony ár ígéretének.

✔ Ismerd fel a hamis weboldalakat, webshopokat! (lásd fent)

✔ Ne chatelj olyan idegenekkel (sem), akik valamit el próbálnak adni neked.

✔ Mielőtt bármilyen adatot megadnál a rendelés során, ellenőrizd, hogy HTTPS titkosítást használ-e az oldal, azaz a böngésző címsorában megjelenik-e egy kis lakat ikon. Ez azonban csak azt jelenti, hogy a kapcsolat biztonságos, de nem garantálja, hogy maga a webáruház is megbízható.

✔ Használj virtuális bankkártyát, amelyre csak a vásárlás előtti pillanatban utald át a szükséges összeget.

✔ Az online vásárlás esetében is nagyon jól jön a kétfaktoros azonosítás, élj a lehetőséggel!

✔ Mindig telepíts az eszközeidre olyan megbízható, folyamatosan frissülő biztonsági programot, amely netbank- és tranzakcióvédelemmel is rendelkezik. Rendszeresen frissítsd az operációs rendszert és a telepített programokat is.

4) Cyberbullying

Az online zaklatás, azaz a cyberbulling az egyik, pszichésen legnehezebben kezelhető netes veszély, hiszen a zaklatók gyakran „elbújnak" a neten, és persze könnyű bántani valakit, aki azt sem tudja, kitől kellene megvédenie magát. Ilyenkor jellemzően rosszindulatú, sértő üzeneteket osztanak meg valakiről a közösségi oldalakon, chat alkalmazásokban, fórumokon, vagy akár online játékok csevegőiben. Mit tehetsz, ha Te váltál valaki céltáblájává?

✔ Bármennyire is nehéz megállni, ne reagálj! Ezzel csak olajat öntesz a tűzre.

✔ Készíts mentéseket, képernyőképeket a bántó üzenetekről, hogy a későbbiekben bizonyítani tudd az online zaklatás tényét.

✔ Ha egy iskolatársad a zaklató, azonnal a tanárokhoz kell fordulnod, ha pedig egy ismeretlen, akkor a szolgáltató ügyfélszolgálatán kell jelezned a problémát, és ők le tudják tiltani a felhasználót.

✔ Érdemes bejelentést tenned a Nemzeti Média- és Hírközlési Hatóság oldalán is.

5) Online ragadozók

Az ismerkedés még az offline világban sem mindig egyszerű, hát még a neten, amikor csak a kijelződön szereplő információk alapján tudsz megítélni valakit. A „szerelmi csalók" és „bizalmas barátok" gyakran a közösségi médiában, vagy akár online játékok közben adják ki magukat olyan személynek, aki a kiszemelt áldozatnak – a róla elérhető információk alapján – valószínűleg tetszeni fog. Ha sikerül a kapcsolatfelvétel, privát üzenetekben igyekeznek bizalmas viszonyba kerülni, hogy pénzt csaljanak ki, vagy ami még veszélyesebb, személyes találkozókra vegyék rá őket.

✔ Ha egy idegen chatüzenetekben próbál kapcsolatba lépni veled és rövid időn belül szerelmet is vall, vagy mély barátságról számol be, akkor itt valami nagyon gyanús, légy óvatos!

✔ Akár egy gyors, kép alapján történő kereséssel is kiderülhet, hogy valós, vagy esetleg veszélyes személlyel van-e dolgod.

✔ Gondold meg, kivel osztod meg a webkamerád képét, és ha nem használod, mindenképp takard le és kapcsold ki.

✔ Ne küldj üzenetben intim fotót, és a bankkártyádról, okmányaidról készült képet sem.

Az ESET felmérése szerint a diákok többsége a fenti veszélyektől tart leginkább, de bizony van még néhány olyan téma, amire talán nem is gondoltál!

Egy szuper ösztöndíj, amiért szinte semmit se kell tenni? Gyorsan jutnál több pénzhez egy váratlan állásajánlatnak köszönhetően?

Olvass tovább, mert a netes csalók kreativitása szinte határtalan!

6) Ösztöndíjas csalások

A bűnözők sajnos még az anyagi támogatást kereső diákokat sem kímélik, különféle hamis ösztöndíjakat ajánlanak, elsősorban angol nyelvterületen. Az ösztöndíj természetesen ez esetben sem létezik, ám a csalók zsebre teszik a jelentkezéshez állítólagosan szükséges „regisztrációs díjat". Sőt, az „ösztöndíj-tombolás csalás" esetében gyakran adóköltségekre hivatkozva követelnek a résztvevőktől egy előre fizetendő „kezelési költséget" vagy „kifizetési díjat".

✔ Nézz utána más forrásból is a kínált ösztöndíjnak, és a szervezetnek, akár hívd is fel őket.

✔ Gyanakodj, ha regisztrációs, vagy kifizetési díjat kérnek tőled előre!

7) Hamis munkaajánlatok

Biztos te is sokat költesz a tanulmányaid mellett utazásokra, bulira, ruhákra – és mindezt sokszor nem fedezi a zsebpénz. A részmunkaidős állás szuper megoldás lehet, de csak akkor, ha az az állás valóban létezik is. A csalók sokszor hiteles állásajánlat-gyűjtő helyeken posztolnak hamis munkalehetőségeket, hogy aztán így csaljanak ki személyes adatokat, melyek segítségével például bankszámlát is nyithatnak, vagy okiratot hamisíthatnak.

✔ Ez esetben is igaz az alapszabály: ha az ajánlat túl szép ahhoz, hogy igaz legyen, akkor gyakran nem is valódi.

✔ Gyanakodj, ha otthoni könnyű online munkavégzésért kiemelkedő fizetéssel járó pozíciót ígérnek.

8) Okosórák

Az okosóra lassan olyan „alapeszközzé" válik, mint a mobiltelefon. Ne feledd, hogy ez is egy netes eszköz, és ennek megfelelően körültekintően kell választanod, ha Te is be szeretnél szerezni egyet.

✔ Olvass teszteket, felhasználói véleményeket, mielőtt okosórát vennél. Keress rá a termékre a hírekben is. Volt gond az adatvédelemmel a termék kapcsán? Komolyan vette a cég a problémákat, átláthatóan kommunikált, fejlesztésekkel és hibajavításokkal küszöbölte ki a hibát?

✔ Az okosórák is össze vannak kötve egy szerverrel, az eszköz akkor biztonságos, ha a szerverrel való kommunikáció titkosított. Járj utána, hogy a gyártó garantálja-e a titkosított kommunikációt!

✔ Az okosórán nem érdemes nagyon spórolni, válassz ismert, biztonságos márkát. Az olcsó okosórák gyakran gyenge minőségűek, és komoly adatvédelmi aggályok is felmerülnek velük szemben, például, hogy titkosítatlan, bárki által olvasható „clear textben" utaznak a bizalmas információid, jelszavaid a neten, ismeretlen szerverekre továbbítják az adatokat, és sosem jelennek meg hibajavító frissítések.

9) Fake news

Végül, de nem utolsó sorban nem maradhat ki az összeállításunkból a sokat emlegetett „fake news", azaz az álhírek. Mert a csalók nem csak a pénzedre és az adataidra utaznak, hanem bizony szeretnének befolyásolni is téged – természetesen a saját érdekeiknek megfelelően.

A neten elérhető híráradatban pedig nem könnyű eligazodni, és kiszűrni a hamis híreket.

Az alábbiakon mindenképp érdemes elgondolkodnod, ha híreket olvasol:

✔ Hihetőnek tűnik a hír? Hol jelent meg?

✔ Kerek egésznek tűnik a hír? Kimaradt esetleg belőle valami, ami fontos lehet?

✔ Van a hírnek egy beazonosítható szerzője? Megbízható a szerző és az oldal is, ahol a hír megjelent?

✔ Más ismert, hiteles hírportálok mit írnak a témáról?

✔ Ki fizethetett azért, hogy az adott hír megjelenjen? Ki kaphat azért pénzt, ha rákattintunk?

Reméljük, hogy hasznát veszed az ESET tippjeinek, és a jövőben még nagyobb biztonságban netezel!

További hasznos tanácsokért látogasd meg fiataloknak szóló oldalunkat:

https://www.eset.com/hu/digitalis-biztonsag/fiataloknak/

Ha kérdésed merült fel, fordulj hozzánk bizalommal alábbi elérhetőségeinken:

https://www.eset.com/hu/rolunk/kapcsolat/

Digital Security
Progress. Protected.