HÍRLEVÉL 2

Milyen veszélyeket rejt az internet, amelyeket ismernie kell, és melyektől kell óvakodnia?

Az internet veszélyei, amelyekről tudnunk kell, amelyekkel óvakodnunk kell, és amelyekkel szükség esetén foglalkoznunk kell, 9 nagy kategóriában foglalhatók össze.

1) **Rosszindulatú szoftverekkel és vírusokkal teli oldalak, amelyek készen állnak arra, hogy megfertőzzék a számítógépét.**

Internetezés közben nagyon könnyű rossz linkre kattintani, és olyan webhelyet megnyitni, amely rosszindulatú szoftvereket tölt be a számítógépre. Szerencsére, ha naprakész vírusirtó van telepítve a számítógépére, ez a vírus szinte mindig megállítható, mielőtt kárt tehetne. A legnagyobb veszélyt - a vírusirtó által véletlenül átengedett vírus veszélye mellett - az jelenti, ha nem veszi észre, hogy olyan fertőzést kockáztat, amely veszélyeztetheti a számítógép működését vagy az adatok sértetlenségét. Éppen a sok ember figyelmetlensége miatt az elmúlt évben széles körben elterjedtek az olyan zsarolóvírusok, mint a Cryptlocker, amely személyes fájlokat titkosít és váltságdíjat követel.

Tudjuk, hogy melyek a veszélyes oldalak, általában azok, amelyek kalózkodással, streaming oldalakkal, felnőtt tartalmakkal, társkereső és illegális anyagokkal foglalkoznak. Ha nem tudja elkerülni az ilyen típusú oldalak meglátogatását, legyen nagyon óvatos, hova kattint, mivel a vírusok bárhol elrejtőzhetnek. Elég csak a rossz "Letöltés" gombra kattintani, és máris rosszindulatú szoftverek települnek. És ne feledkezzünk meg azokról a reklámbannerekről sem, amelyek azt mondják, hogy a számítógéped fertőzött, pedig valójában nem az.

Ha kétségei vannak, vannak olyan eszközök, amelyek segítenek felismerni és elkerülni a veszélyes linkeket és gyanús oldalakat.

A vírusos oldalak felismerésének és elkerülésének egyik legfontosabb tényezője, hogy olyan naprakész böngészőt használjon, amely az összes eddig felfedezett vírus ellen védett.

A legveszélyesebb oldalak, amelyek rosszindulatú programokat tartalmazhatnak, minden bizonnyal a felnőtt oldalak, a kalózkodó oldalak, szinte minden torrent oldal (szintén kalózkodással), illegális letöltő oldalak (például filmek és zenék) és a crack oldalak.

Ideális esetben, ha feltétlenül meg kell látogatnia egy ilyen webhelyet, a legjobb, ha egy homokozóban böngészik. Mind a Windows 10-ben, mind a Windows 11-ben használhat egy virtuális

asztal funkciót, amely nemcsak biztonsági eszköz, hanem remek lehetőség arra is, hogy a számítógépen úgy végezzen el dolgokat, hogy azokat ne rögzítsék és ne jegyezzék meg, kicsit hasonlóan a webböngészők inkognitó üzemmódjához. Ezt az eszközt Sandboxnak hívják, és úgy tervezték, hogy a számítógép egy olyan területe legyen, ahol minden, amit teszel, nincs hatással a rendszerre, és a rendszer kikapcsolása után azonnal törlődik. A SandBox egy eldobható virtuális gépként működik, ahol biztonságosan futtathat bármit, amit csak akar; akár vírusos vagy rosszindulatú programot is megnyithat anélkül, hogy attól kellene tartania, hogy az kárt tesz a számítógépében, vagy adatokat lop el a számítógépéről.

2) **Az online adatvédelem mindig veszélyben van**

Elég nyilvánvaló, hogy ha az internetet részvételi módon akarjuk használni, azaz fórumokhoz, közösségi hálózatokhoz és csevegőszobákhoz csatlakozni, akkor fel kell áldoznunk némi magánéletet. Az olyan oldalakon, mint például a Facebook, kötelező megadni a valódi nevet, míg más oldalakon továbbra is szükséges megadni egy e-mail címet, amelyen keresztül, ha akarja, felkutathatja a tulajdonost. Alapvetően a normális internethasználat során az anonimitás nem létezhet, és ha valakit érdekelne, hogy megtudja, kik vagyunk, és rendelkezne a megfelelő hackerképességgel és tehetséggel, elméletileg mindent megtudhatna rólunk.

Az online adatvédelem azonban nem arról szól, hogy megakadályozzuk, hogy egy hacker kémkedjen az életünk után, mert hacsak nem követ minket egy zaklató, vagy nem teszünk olyan dolgokat, amelyek illegálisak és rejtegetni kell őket, akkor mondjuk úgy, hogy valószínűleg senki sem pazarolja az idejét arra, hogy az életünkbe betörjön. Az online adatvédelem viszont azt jelenti, hogy az érzékeny információkat, például a hitelkártyaszámunkat, a jelszavainkat, azt, hogy éppen hol vagyunk, mit keresünk az interneten, és így tovább, titokban tartjuk.

3) **Nem védett weboldalak**

Ez egy olyan veszélytényező, amelyet a legtöbb ember még mindig figyelmen kívül hagy.

A webhelyek nem mind egyformák, és biztonságos webhelyekre oszthatók, ahol az Ön által továbbított információkat titkosítják, és nem lehet kívülről lehallgatni, valamint normál webhelyekre, amelyek tisztán továbbítják az adatokat. A Navigaweb.net jelenleg egy titkosítatlan webhely, ami nem jelenti azt, hogy nem biztonságos, de mivel a bejelentkezéshez nem szükséges jelszó, nem kell védenie az Ön adatait. Minden olyan webhelyet, ahol jelszót kell megadnia, titkosítani kell, és ezt a védelmet a webcímen található lakatról és a http helyett a https előtagról lehet felismerni. Ha egy webhely HTTPS protokollal működik, és nincs tanúsítványhiba, akkor az összes általunk küldött információ, beleértve a jelszavakat, hitelkártya- vagy bankszámlaszámokat, nem látható az interneten senki számára, még az oldal üzemeltetője sem, akinek ezeket az információkat küldjük. Magától értetődik, hogy ne osszon meg személyes adatokat semmilyen webhelyen, akár van https, akár nincs.

Ha még mindig https nélküli e-mail szolgáltatást vagy ilyen sekélyes online banki szolgáltatást használ, azonnal váltson.

4) Adathalászat

Az általánosan veszélyes weboldalak között külön kategóriát képeznek a csalóoldalak, például az ismeretlen és nem ajánlott vásárlási oldalak, vagy ami még rosszabb, a híres oldalakkal azonosnak tűnő hamis oldalak, amelyek célja a fiókjelszavak ellopása.

A hamis weboldalak, banki vagy vásárlási oldalak másolatainak készítése az egyik leggyakoribb technika, amelyet a hackerek a webes fiókok jelszavainak ellopására használnak, és amelyet adathalászatnak neveznek. Az adathalászat mindig úgy működik, hogy üzenetet küldenek e-mailben, Facebookon, SMS-ben, Whatsappon stb. A legjobb módja annak, hogy elkerüljük, hogy bedőljünk ennek a technikának, ha a jelszavak ellopására használjuk. A legjobb módja annak, hogy ne essünk ilyen csapdába, hogy soha ne írjuk meg jelszavainkat és fontos adatainkat (még e-mailben sem), kivéve a hivatalos fiókoldalakon, amelyek felismerhetők a böngésző tetejére írt címről és a zöld lakattal ellátott HTTPS-ről.

Ideális esetben jobb lenne egy e-mail klienst, például a Microsoft Outlookot használni, és egy spamszűrővel blokkolni ezeket az üzeneteket.

5) Spam

A spamek veszélye ma sokkal kisebb, mint néhány évvel ezelőtt.

A spam a nem kívánt üzenetek, reklámok, adathalászat, vírusok vagy felesleges kommunikáció teljes kategóriája. Szerencsére a mai legjobb e-mail szolgáltatások, mint például a Gmail és az Outlook.com, hatékony spamszűrővel rendelkeznek, amely szabályozza a bejövő e-maileket.

6) Téves információk

Bár a spam kategóriájába tartozhat, az elmúlt évben az interneten terjedő félretájékoztatás valódi veszélyt jelentett a hoax oldalakról származó álhírek terjedése miatt, amelyeket meg kell tanulnunk felismerni, hogy ne nézzünk ki úgy, mint azok a hülyék, akik mindent elhisznek, amit az interneten vagy a Facebookon olvasnak.

7) Online társkereső

Ez az internet egyik legnagyobb veszélye a fiatalok számára.

Csúnyán hangzik, de egy felelős szülőnek a körülményektől függetlenül ellenőriznie kell, hogy a gyermekei csevegnek-e idegenekkel az interneten. Cseveghetsz egy idegennel egy online játékban, egy alkalmi társkereső oldalon, egy közösségi oldalon, egy fórumon vagy bármely más csevegőszobában. Akár szexről, akár randizásról vagy pusztán szórakozásról van szó, fontos, hogy ne adj ki túl sok személyes információt: ne mondd meg a valódi életkorodat, ne mondd meg, hol laksz, ne mondd meg, milyen iskolába jársz, ne add meg a családtagjaid vagy barátaid valódi nevét, és ne add meg a telefonszámodat. Az online ragadozók nagyon jók abban, hogy normális gyerekeknek adják ki magukat, és úgy tudják kihasználni a tinédzserek gyengeségeit, ahogy még a legjobb pszichológusok sem, a legrosszabb esetben a pedofília szörnyű betegségétől vezérelve.

8) Cyberbullying

Az idegenekkel való beszélgetés veszélyes lehet, mert sosem tudhatod, ki van a billentyűzet mögött, de az ismerősökkel folytatott beszélgetések vagy üzenetek is veszélyesek lehetnek. A cyberbullying nagyjából így működik: ha az iskolában vagy a barátai csúfolnak, egyikük feltölthet egy videót vagy fotót a Facebookra vagy más közösségi médiára, amely kínos helyzetbe hozhatja az áldozatot.

A cyberbullying másik esete a névtelen üzenetekből eredhet, amelyek erősen sértik az áldozatot, akár fenyegetésekkel is.

A valódi zaklatóval szemben a cyberbullynak megvan az az előnye, hogy nincs kontroll, és azt mondhat, amit akar, anélkül, hogy az áldozat szemébe nézne, vagy akár névtelenül, a billentyűzet mögé bújva. Mindkét esetben nem lenne olyan nehéz, legalábbis technikailag. Sokkal bonyolultabb azonban a pszichológiai szintű védekezés, amihez szükség lehet egy szülő vagy szakértő segítségére.

Kezdetnek azonban kiváló első lépés lenne, ha törölnéd a fiókodat az Ask.fm-en, az egyik olyan oldalon, amely az online cyberbullyingra leginkább hajlamos.

9) Az informatikai biztonság teljes figyelmen kívül hagyása

Ez egy nyilvánvaló veszély, amely annyira elterjedt, hogy meglep minket.

Lehetséges, hogy még ma is a világon a legelterjedtebb jelszó az 123456?

Azt hiszik az emberek, hogy mivel nincs mit rejtegetniük, egy hacker sem fogja ellopni a fiókjukat?

Hogyan lehetséges, hogy az emberek még mindig ugyanazt a jelszót használják minden weboldalon?

És még mindig vannak olyanok, akik a jelszavaikat - talán mind különböző és nehezen megjegyezhető - egy bárki által olvasható papírra írják?

A projekt az Európai Bizottság támogatásával valósult meg. Ez a dokumentum kizárólag a projektpartnerek véleményét tükrözi, és a Bizottság nem tehető felelőssé a benne foglalt információk bármilyen felhasználásáért.

This work is licensed under CC BY-SA 4.0