

Zsaroló levelek...

Sokszor hallani manapság zsaroló levelekről, hogyan tudunk védekezni elleni?

Az okostelefonok és az internet térnyerésével egyrészt könnyebbé vált az életünk, másrészt sokkal hamarabb kerülhetnek veszélybe adataink kellemetlen percek, órákat okozva. A fiatalok (s felnőttek egyaránt) számtalan közösségi oldalnak tagjai, telefonjukon elképesztő mennyiségű applikációt működtetnek. A közösségi felületek, az életünk megkönnyítésére hivatott applikációk rengeteg információt gyűjtenek rólunk. Ha minden megosztásra, alkalmazásra, körlevélre reagálunk, email címünk könnyen kerülhet egy virtuális adatbankba, hozzáférést biztosítva spam, reklám vagy zsarolólevelek számára. A zsaroló levelek tartalmukban sokszor igazodnak trendekhez, szokásokhoz, aktualitásokhoz és érzelmileg is manipulálnak. Gyakran személyes szférát is érintő kényes témára utalnak.

Tudatos internethasználattal megelőzhetőek, hogy a hoaxok vagy annak alfajai, a ransomware, malware nevű zsaroló levelek anyagi vagy erkölcsi kárt okozzanak. De mi az a hoax és a ransomware és mi a céljuk?

Hoax: lánclevél (lehet víruslevél, vagy lánc/körlevél), mely hamis híreket, információkat tartalmaz. Rémhírterjesztés, adatgyűjtés, számítógépek vírussal történő fertőzése, rendszer vagy hálózat lassítása is lehet a hoax célja. Védekezni ellene kellő óvatossággal lehet. Ismeretlen helyről származó email-t nem szabad megnyitni, továbbküldeni, megosztani másokkal, hivatkozott tartalom esetén több hivatalos oldalon is ellenőrizni kell az információt, a forrást, a feladót (ha nem ismert, gyanús, törölöm), bizalommal lehet fordulni szakemberhez, valamint meg kell vizsgálni a megosztott hír tényleges időpontját (dátumot) és a célcsoportot, akire vonatkozik, vagy akiről/akikről szól. A levél formája, a helyesírás, szokatlan szó- és nyelvhasználat, nem adekvát stílus, írásképe is árulkodó lehet.

Ransomware: zsarolóvírus, zsarolólevél, program. Zárolja az adatokat. Melléklet tartalmazhat exe, doc, pdf, mp4 kiterjesztést. A linkek, fájlok káros kódokat is tartalmazhatnak. Ha a gyanútlan felhasználó megnyitja az ismeretlen forrásból származó elektronikus levelet, vagy rákattint a levélben lévő linkre, a személyes képei, dokumentumai, teljes számítógépe a zsarológ, adathalászok kezébe kerülhet.

Az álhírekkel kapcsolatos ismeretek sikeresen ellenőrizhetőek az <https://www.urbanlegends.hu/> címen elérhető oldalon. Az oldalon játékos tesztek is elérhetőek. Ez az oldal iskolák számára is javasolt.

Mit tehet, ha ilyen hírrel találkozik?

- Mérlegeli a forrást! Ellenőrzi az email-címet!
- Ismeretlen email címről nem nyitja meg a levelet!
- Olvas a sorok között!
- Ellenőrzi a helyesírást, a nyelvezetet!
- Ellenőrzi a dátumot!
- Megnéz a hírrel kapcsolatban meg több hivatalos internetes portált!
- Fékezi az előítéleteit! Az előítéletek többsége nem személyes tapasztalás útján alakul ki!
- Megkérdezi a szakértőket, szakembereket!
- Hivatalos levélben a közvetlen stílus, tegeződés, sürgetés is gyanús lehet!
- Ellenőrzi, ha túl szokatlan az információ!

Csak azt tegye meg az internetes felületen, amit a valóságban is megtenne. Úgy jelenjen meg a közösségi szférában, ahogy egy baráti körben is megjelenne. Az internet nem felejt, az internet nyomon követ, az internet figyeli szokásainkat, közzé tett adatainkat, így bánjunk csínján az applikációk fejetlen telepítésével és céltalan böngészéssel! Legnagyobb védettséget a fedhetetlen életmód, megfontolt telepítés, óvatos nethasználat, tudatos megosztások jelentik.

Technikai szinten pedig a rendszeresen frissített böngésző, operációs rendszer, végpontvédelmet is nyújtó védelem, különböző defender programok, valamint kamera- és bankszámlavédelmi opcióval is rendelkező vírusvédelem (heurisztikus védelemmel), többfaktoros hitelesítéssel rendelkező levelezőrendszer és netbank applikáció, adware blokkoló alkalmazások nyújthatnak alapvető védelmet.

Amennyiben károsult, forduljon bizalommal a 112-es központi segélyhívón keresztül a rendőrséghez, vagy a legközelebbi rendőri egységnél tegyen feljelentést.

Internetes gondok, internetes zsarolás esetén segíthetnek (bejelentés is, segítő applikációk is):

- <http://saferinternet.hu/>
- <https://biztonsagosinternet.hu/>
- <http://nmhh.hu/internethotline/>