CTI jelentés

Általános ismertető az e-könyvek és az e-könyv olvasók biztonsági kérdéseiről

1996
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT
fortes fortuna adiuvat

NEMZETI KIBERVÉDELMI INTÉZET

Bevezetés

Az e-book, másnéven e-könyv a könyv digitális, számítástechnikai eszközökön megjeleníthető formája. A legnépszerűbb e-book fájlformátumok a PDF, az AZW, az EPUB és a MOBI, amelyeket telefonon, számítógépen, tableten és specifikusan erre a célra kifejlesztett e-book readeren, másnéven e-könyv olvasón lehet megtekinteni. Az utóbbi évtizedben rendkívüli mértékben elterjedtek az okostelefonok és tabletek a világon, amelyek teljesen alkalmasak e-könyvek olvasására. Felmerülhet a kérdés: miért van szükség egy plusz eszközre, amely kis túlzással csak olyan formátumú fájlok olvasására alkalmas, amelyeket bárki megtud nyitni a zsebében lapuló okostelefonnal?

Az e-könyv olvasók megalkotásánál 2 fontos dolgot tartottak szem előtt a gyártók: legyen az eszköz **alacsony fogyasztású** és **kímélje a szemet**, azaz több órás folyamatos használat se okozzon problémát a vevőnek. Az e-könyv olvasók alapvetően monokróm e-ink (e-tinta) kijelzőt használnak, amelynek köszönhető, hogy akár egy **teljes napszakot használva se fogja a szemet úgy fárasztani**, mint egy hagyományos LCD vagy LED kijelző. További előnye, hogy több hetes aktív használat után szükséges csak az újratöltése.

Tartalomjegyzék

Veszélyforrások 3. oldal

Leggyakoribb átverési technikák 11. oldal

- A szemét újracsomagolása 11. oldal
- Plágium 14. oldal
- Versenynek hirdetett átverés 15. oldal
- Spammelés 16. oldal
- Megtévesztés 10. oldal

Összefoglalás 18. oldal

Védelmi megoldások, javaslatok 19. oldal

Veszélyforrások

Az e-könyv olvasók ugyanúgy telepíthetnek és futtathatnak alkalmazásokat, mint az Android és iOS. Az egyik tipikus veszélyforrás, amikor egy hacker egy **.pdf fájlba rejti el a káros kódjait**. Miután az áldozat letölti a könyvet, a háttérben rosszindulatú szoftverek települnek a készülékre, legtöbbször a felhasználó tudta nélkül. Ezt az Adobe Reader javascript támogatottsága miatt tudják végrehajtani a csalók. Emellett a legtöbb böngésző is tartalmaz **beépített PDF olvasó motort**, amely szintén célpont lehet a támadók számára. A támadók kihasználhatják az AcroForms vagy az XFA Forms, a PDF készítés során használt szkriptelési technológiákat, amelyek célja az, hogy hasznos, interaktív funkciókkal egészítsék ki a szabványos PDF dokumentumokat.

A **VirusTotal** egy olyan online szolgáltatás, amely vírusirtó motorok és weboldal scannerek segítségével **elemzi a fájlokat és URL címeket** vírusok, férgek, trójaiak és egyéb rosszindulatú tartalmak észlelése céljából.

Detection | Details | Community 1

AegisLab	Trojan.PDF.Credlik.4!c	AhnLab-V3	PDF/Exploit
ALYac	Exploit.CVE-2018-4993	ClamAV	Pdf.Exploit.CVE_2018_4993-6546349-0
Cyren	PDF/Trojan.BVCF-3	ESET-NOD32	PDF/Exploit.CVE-2018-4993.D
GData	PDF.Trojan.Agent.GA2LFS	Ikarus	Exploit.CVE-2018-4993
Kaspersky	HEUR:Trojan.PDF.Credlik.a	McAfee	RDN/Generic Exploit
McAfee-GW-Edition	BehavesLike.PDF.Suspicious.zn	Qihoo-360	Win32/Trojan.d05
SentinelOne	DFI - Malicious PDF	Sophos AV	Troj/PDFEx-JK
Symantec	Trojan.Pidief	ZoneAlarm	HEUR:Trojan.PDF.Credlik.a

1. ábra: CVE- 2018 - 4993 a VirusTotalon

Amint a VirusTotal képéből kiderül, az előbbiekben szemléltetett példa egy trójai. A CVE-2018-4993 kód leírása szerint az Adobe Acrobat Reader 2018.011.20038 és korábbi, 2017.011.30079 és korábbi, valamint 2015.006.30417 és korábbi verzióiban NTLM SSO hash sebezhetőség található. Sikeres kihasználása információ lopáshoz vezethet.

Az **Internet of Things (IoT)** olyan fizikai tárgyak hálózatát írja le, amelyek érzékelőkkel, szoftverekkel és egyéb technológiákkal vannak ellátva. Ezek az eszközök képesek az internetre csatlakozni és adatokat cserélni más eszközökkel és rendszerekkel. Ide tartoznak az olyan hétköznapi tárgyak, mint a számítógépek, tabletek, telefonok, konnektorok, hűtőszekrények, klímák, távvezérelt villanykapcsolók, csatlakoztatott termosztátok, CCTV kamerák, de lehetnek napelemek, autók vagy traktorok is. Léteznek már komplett okos házak (okos otthon), okos gyárak és okos sportpályák is. Ma már több mint 10 milliárd ilyen készülék vagy rendszer létezik és egyes szakértők szerint 2030-ra elérheti a 25 milliárdot is a számuk.

Minden olyan eszköz, amely csatlakoztatható az otthoni Wi-Fi hálózathoz, **potenciális támadási célpontot** kínál a kiberbűnözőknek. Bár ezek a támadások nem kimondottan az e-könyv olvasókat célozzák, azok is könnyen áldozatul tudnak esni, ha a támadó sikeresen betört a hálózatba.

Az **e-olvasók Wi-Fi-t** és a mobiltelefonok által használt **3G vezeték nélküli hálózatot**, valamint lecsupaszított **webböngészőket használnak** az interneten keresztül az e-könyv áruházakhoz való csatlakozáshoz.

Az Egyesült Államokban az AT&T vezeték nélküli hálózatát (3G), és több mint 100 országban pedig a partnerek szolgáltatásait használva bárhol lehet internetezni egy Kindle eszközzel, ahol van lefedettség. Bár ez a szolgáltatás ingyenesen jár az összes Kindle e-olvasóhoz, csak az Amazon és a Wikipédia honlapja érhető el ezen a hálózaton keresztül.

A beépített webböngésző lehetővé teszi, hogy az e-könyvekben, blogokban vagy más tartalmakban megadott linkekről azonnal a webhelyekre ugorjon.

Ezzel szemben a webböngésző kezdetleges jellegének van néhány hátránya is:

- A szürkeárnyalatos kijelző nem ideális a legtöbb oldal böngészéséhez.
- A webböngésző nem támogatja a Flash vagy Shockwave multimédiás effekteket.
- A Java appletek nem támogatottak. Egyes webhelyek Java appleteket használnak animációkhoz vagy összetett funkciók biztosításához.
- A videók nem játszhatók le a webböngészőn keresztül.

Egyes készülékek lehetővé teszik a laptophoz vagy asztali számítógéphez való csatlakozást is **fájlok le- és feltöltésére**. Ennek eredményeképpen elképzelhető, hogy egy e-olvasó elkap egy vírust vagy férget egy e-mail üzenetből, fájlból vagy weboldalról.

Egy ilyen esetet előzött meg az Amazon 2020-ban, amikor 18 000 dolláros jutalmat adott egy olyan exploit láncért, amely lehetővé tette volna, hogy egy támadó teljes mértékben **átvegye az irányítást egy Kindle e-olvasó felett**, egyszerűen a célzott felhasználó e-mail címének ismeretében. A **KindleDrip** nevű támadást 2020 októberében fedezte fel Yogev Bar-On, az izraeli székhelyű Realmode Labs kiberbiztonsági tanácsadó cég kutatója. A KindleDrip három különböző biztonsági rés kihasználásával járt, amelyek mindegyikét az Amazon orvosolta.

Az első sebezhetőség a kihasználási láncban a **„Send to Kindle" funkcióhoz** kapcsolódott, amely lehetővé teszi a felhasználók számára, hogy MOBI formátumú **e-könyvet küldjenek e-mailben csatolmányként** a Kindle készülékükre. Az Amazon generál egy @kindle.com e-mail címet, ahová a felhasználó által jóváhagyott e-mail címek listájából a felhasználó e-könyveket küldhet csatolmányként.

Bar-On felfedezte, hogy ezzel a funkcióval visszaélve **speciálisan kialakított e-könyvet** tud küldeni, amellyel **tetszőleges kódot tud végrehajtani** a célzott eszközön. A rosszindulatú e-könyv a kódfuttatást egy olyan sebezhetőség kihasználásával érte el, amely a Kindle által a JPEG XR képek elemzésére használt könyvtárhoz kapcsolódik. A kihasználáshoz a felhasználónak egy **rosszindulatú** JPEG XR képet tartalmazó e-könyvben található linkre kellett kattintania, ami a webböngésző megnyitásához és a támadó kódjának korlátozott jogosultságokkal történő végrehajtásához vezetett.

A kutató egy olyan **sebezhetőséget** is felfedezett, amely lehetővé tette számára a **jogosultságok kiterjesztését** és a kód root-ként történő végrehajtását, ami teljes hozzáférést biztosított a készülékhez.

A támadónak csak a célzott felhasználó e-mail címére lett volna szüksége, és arra, hogy meggyőzze az áldozatot, hogy **kattintson a rosszindulatú e-könyvben található linkre**. Bár a Send to Kindle funkció csak azt teszi lehetővé, hogy a felhasználók előre jóváhagyott e-mail címekről küldjenek e-könyveket, a kutató rámutatott, hogy a támadó egyszerűen használhatott volna egy e-mail hamisító szolgáltatást is. A célzott felhasználó @kindle.com e-mail címének előtagja sok esetben megegyezik a normál e-mail címével.

2. ábra: A KindleDrip támadás folyamata

A Kindle firmware módosítását igénylő **biztonsági réseket** - a kódfuttatási és a jogosultságok kiterjesztésével kapcsolatos problémákat – 2020 decemberében, az **5.13.4-es verzió kiadásával foltozták be**. Az Amazon onnantól a nem hitelesíthető e-mail címekre is küld egy ellenőrző linket. Továbbá néhány e-mail aliashoz néhány karaktert ad hozzá, hogy nehezebb legyen kitalálni őket, és az e-mail címek nyers kitalálását megakadályozó rendszerek is hatékonyabban működnek ezáltal. A Kindle felhasználóknak nem kell semmilyen intézkedést tenniük.
Az Amazon 2021. április elején kezelt egy **másik kritikus sebezhetőséget** is a Kindle e-könyv olvasó platformjában, amelyet potenciálisan ki tudtak volna használni a támadók arra, hogy **teljes irányítást szerezzenek** az áldozat készüléke felett, ami érzékeny információk ellopását eredményezhette volna az Amazon fiók hitelesítő adataitól kezdve a számlázási adatokig.

Miután az Amazon 2021 februárjában nyilvánosságra hozta a problémát, áprilisban a Kindle firmware 5.13.5 verziójának részeként **javítást tett közzé**.
A támadás egy rosszindulatú e-könyv elküldésével kezdődik, amelyet a felhasználó megnyit és elindít egy fertőzéssorozatot mindenféle interakció nélkül. Ez lehetővé teszi a csaló számára, hogy törölje az áldozat könyvtárát, teljes hozzáférést szerezzen az Amazon fiókja felett és további eszközöket fertőzzön meg a felhasználó hálózatán belül.

```
// CPDF_ModuleMgr::Get()->GetJbig2Module()
uint32_t* mgr = ((uint32_t* (*)())(base + 0x1f654))();
uint32_t* mdl = ((uint32_t* (*)(uint32_t*))(base + 0x1fb8c))(mgr);

// CreateJbig2Context
uint32_t* ctxt = ((uint32_t* (*)(uint32_t*))(base + 0x8e4d8))(mdl);

// new CFX_DIBitmap
uint8_t* bitmap = (uint8_t*)malloc(0x34);
((void (*)(uint8_t*))(base + 0xb28a0))(bitmap);

// CFX_DIBitmap::Create
((void (*)(uint8_t*, uint32_t, uint32_t, uint32_t, uint32_t, uint32_t,
    uint32_t, uint32_t))(base + 0xb2b64))(bitmap, width, height, 1, 0, 0, 0, 0);

uint32_t dest = *(uint32_t*)(bitmap + 0x28);
uint32_t pitch = *(uint32_t*)(bitmap + 0x18);

// CCodec_Jbig2Module::StartDecode
((int (*)(uint32_t*, uint32_t*, uint32_t, uint32_t, uint8_t*, uint32_t,
    uint8_t*, uint32_t, uint32_t, uint32_t, uint32_t))(base + 0x8e1e4))(
    mdl, ctxt, width, height, data, data_sz, data_gl, data_gl_sz, dest, pitch, 0);
```

3. ábra: Heap túlcsordulási sebezhetőség a JBIG2Globals dekódoló algoritmusban

A probléma a PDF dokumentumok megnyitásához kapcsolódó implementációban található, ami lehetővé teszi a támadó számára, hogy rosszindulatú kódot futtasson a készüléken.

A PDF renderelő funkcióban található heap **túlcsordulási sebezhetőség** (CVE-2021-30354) és a **Kindle alkalmazáskezelő** szolgáltatásban található **helyi jogosultságok kiterjesztésének hibája** (CVE-2021-30355) teszi lehetővé a fenyegető számára, hogy a két hibát együttesen kihasználva **root felhasználóként rosszindulatú kódot futtasson** a fertőzött eszközön.

A leggyakoribb átverési technikák

A szemét újracsomagolása

Léteznek úgynevezett hamis kiadók, amelyek megvásárolják a szövegeket a „tartalomfarmoktól", újracsomagolják ezeket és eladják néhány dollárért. Így készítenek **értéktelen és haszontalan információkkal teli e-könyveket**. Ezt a technikát alkalmazva gyakran újra és újra átírják a szöveget, néha egyszerűen megismételve az anyagot, de más cím és szerzői név alatt árulva azt. A **csaló célja** egyértelműen a **pénzszerzés**, nagy mennyiség-kis ár alapon.

2016-ban az Amazon háza tájékán nagy port kavart Valeriy Shershnyov esete, aki körülbelül 1500 könyvet adott ki és több mint 3 millió dollárt keresett ezzel a csalási technikával. Shershnyov kifinomult, úgynevezett „catfishing" rendszerében több száz álnevet használt, hogy az Amazon vásárlóit rávegye arra, hogy gyenge minőségű e-könyveket vásároljanak. Sokáig senki sem volt képes betekintést nyerni abba, hogyan működik egy ilyen csalás - különösen egy olyan, amelyik ennyire jövedelmező.

Shershnyov két évig tudott az Amazon árnyékában maradni. Végül nem a szerzők, vásárlói panaszok vagy az Amazon buktatta le. Óvatlan volt és elfelejtett jelszót tenni a szerverére. Két éven keresztül egy nagy és összetett adatbázist üzemeltetett, amelynek egy pédányát a Microsoft Azure szerverén tárolta.

Ezt a 18 táblából álló adatbázist a MacKeeper Security Research Center találta meg, amely végül Shershnyov tevékenységének a felgöngyölítéséhez vezetett. Az adatbázis az elmúlt két évben készült 1453 rossz minőségű e-könyv adatait tárolta, amelyek mindegyike kapkodva készült el és tele voltak helyesírási hibákkal. A könyvek egy-egy kiadói fiókhoz kapcsolódtak, amelyet a jogdíjak beszedésére használt Shershnyov. Minden fiók több száz e-könyv kiadásáért felelt, így, ha egy fiókot elkaptak volna, nem dőlt volna össze az egész rendszer. Ezek a fiókok együtt dolgoztak azon, hogy mesterségesen felfújják a letöltött e-könyvek számát, és így növeljék azok helyezését az Amazon listáin. Ez segítette a valódi olvasók bevonzását. Az adatbázis egyik, amazon_accounts nevű táblája közel 84000 hamis Amazon fiók adatait tárolta (az Amazon nem kért email-en keresztüli megerősítést a regisztráló személytől).

4. ábra: Shershnyov adatbázisa, bal oldalon a táblák, alul a kijelölt tábla (amazon_accounts) rekordjai száma

Ezek a fiókok több száz, a hozzákapcsolt fiókok által publikált e-könyvet töltenek le néhány órán belül. Ezeket a könyveket rövid ideig ingyenesen lehet felajánlani, így a letöltések további költségek nélkül futhatnak, így ezek nem termelnek jogdíjat, de segítenek növelni az e-könyv értékelését és láthatóságát az Amazon listáin.

A letöltések a Tor anonim hálózatán keresztül történtek, hogy fedve maradjon a szerver IP címe, így az Amazonnak nehezebb dolga volt felfedni ezeket az automatizált letöltéseket.

Plágium

Egy másik gyakori technika a csalók részéről a plagizálás. Ahogy már az ókorban is problémát jelentett mások tulajdonának, munkájának eltulajdonítása, ez a 21. században sincs másképpen. A modern kor technológiáit kihasználva új szintre emelkedett ez a csalástechnika. A **hamis szerzők ellopják mások szellemi tulajdonát** a weboldalaikról, blogjaikról, majd ezeket e-könyvbe foglalják és **eladják látszólag teljesen legálisan**. Néha átírásra, átfogalmazásra kerülnek, de sokszor egyszerűen csak lemásolják ezeket az anyagokat és úgy értékesítik tovább.

2019 legnagyobb botránya Cristiane Serruya esete, aki lemásolta Courtney Milan könyvének, A hercegnő háborújának egyes részeit. A tovább fokozódó **CopyPastCris botrány** (ahogyan elnevezték) nem kevesebb mint 43 szerző 95 könyvét, 6 weboldal cikkeit és egyéb tartalmát érintette. A reflektorfénybe került írót egyre többen kezdték perelni. Claire Ryan aki fantasy író és webfejlesztő is egyaránt, gondolkozni kezdett az eset hatására, hogyan tudna kiépíteni egy rendszert a plágiumok felderítésére. Egy olyan algoritmust írt, ami képes volt megtalálni a hasonló szövegeket 2 könyv között, még akkor is ha a szöveg egy részét átfogalmazták, vagy a neveket megváltoztatták. Ezután tesztelte néhány könyvön a programját, és megbízhatónak bizonyult. Míg a plágiumok egy része az olvasóknak és a szerzőknek szúrt szemet, a plágiumok dokumentálásával kapcsolatos munka nagy részét Ryan végezte. Ő írta az algoritmust, ő biztosította a futtatásához szükséges időt, és ő ellenőrizte az eredményeket.

Versenynek hirdetett átverés

A szervezők **versenyeket hirdetnek**, ahova rendszerint ingyenesen vagy minimális díj ellenében lehet regisztrálni és a nyerteseknek pénzjutalmat, valamint publikációt ajánlanak fel. Ilyen volt 2019 őszén a Pressfuls esete. Az írók részt vettek egy novellapályázaton, ahol annyi információt kaptak, hogy ingyenesen lehet regisztrálni, 50 dolláros jutalom jár a nyertesnek és a 20 legjobb könyvet publikálják. A verseny végeztével kihirdették a győztest és mindenki azt hitte, hogy itt le is zárult a történet. Néhány hónappal később minden pályázó kapott egy emailt, hogy **közzétették a szervező honlapján a művét** és hangoskönyvet is csináltak mindegyikből. Természetesen semmilyen szabály vagy **engedélykérés nem történt** a művek ilyennemű felhasználására. A legtöbb esetben a szerzők megkereséseire nem válaszoltak érdemben. Néhány író könyvét többszöri megkeresés után törölték, de vannak akiké még mindig fent van a honlapon.

Spammelés

A módszer lényege, hogy a csalók **reklámokkal teli művekkel** és olyan hivatkozásokkal spammelik az olvasókat, amelyek valamilyen **kereskedelmi vagy rosszindulatú kódot tartalmazó weboldalra mutatnak**. Ez egyre nagyobb gondot okoz az e-könyv értékesítőinek, bár ez inkább a számítógépeken, iPadeken és mobiltelefonokon használt e-könyv-alkalmazásaiknál jelent problémát, mint az olyan speciális eszközöknél, mint az Amazon Kindle vagy a Barnes & Noble Nook.

Ezekben az e-book csalásokban a szerzők könyveket készítenek (például esküvői etikettről szólót), amelyet néhány dollárért árulnak. A tartalomról kiderül, hogy semmilyen többlet információt nem tartalmaz, mint amit egyébként az ember józan paraszti ésszel ne tudna önmagától, de a **szövegben** olyan részek vannak **elrejtve**, amelyek bizonyos **kereskedelmi termékeket népszerűsítenek**. Olyan linkeket is tartalmaznak, amelyekre kattintva olyan weboldalakra juthatunk, ahol vagy olyan dolgokkal házalnak, mint például esküvői ajándéktárgyak (példánk esetében), vagy vírust töltenek fel a gépünkre. Az interneten már 25 dollár körüli összegért olyan tanfolyamokat árulnak, amelyekben elmagyarázzák, hogyan lehet az e-könyveket ilyen módon spammelésre használni.Ezeket a linkeket gyakran hamis captchák, kuponok, fájlmegosztási vagy lejátszás gombok mögé rejtik el. A felhasználó gyakran nem elég figyelmes, hogy elkerülje ezeket, valamint a furcsa webcímek, amelyek gyanúsak lehetnek, így elrejtésre kerülnek.

5. ábra

Teljesen normálisnak kinéző captcha, amely egy rosszindulatú oldalra irányít kattintás után.

6. ábra

Népszerű fájlmegosztó logóját használják, hogy egy rosszindulatú oldalra irányítson kattintás után.

7. ábra

Videónak álcázott kép, amelyre kattintva egy rosszindulatú oldalra irányít át.

8. ábra

Orosz nyelvű kupon, ami egyszerű hivatkozásként átirányít egy rosszindulatú oldalra.

Megtévesztés

A csalók az e-könyv vásárlásokat és eladásokat arra használják fel, hogy **tömegeket tévesszenek meg** és **magukat hitelesen tüntessék fel** mások szemében. Legtöbbször olyan akciós oldalakon használják ezt, mint például az eBay. Fillérekért vagy valamilyen névleges összegért gyakran több tucatot vásárolnak egyes e-könyvekből és mindegyikre pozitív értékelést kapnak, így keltve azt az érzést a gyanútlan felhasználóban, hogy egy **megbízható** személlyel van dolguk. Így jó helyzetbe került a tökéletes, vagy közel tökéletes értékelésű csaló, hogy később végrehajtson egy másfajta átverést. A fentebb említett esetben, Valeriy Shershnyov részben ezt a módszert alkalmazta. Önmagának generált keresztbe a hamis fiókjaival jó értékeléseket, hogy az igazi vásárlókat megtévessze és bedőljenek az átverésének.

Összefoglalás

Az Amazon és más e-könyv forgalmazók folyamatos harcban állnak az ilyen jellegű csalókkal. Bár az erőforrások nincsenek meg arra, hogy minden önkiadású mű elolvasásra kerüljön, léteznek már olyan szoftverek, amelyekkel megtudják vizsgálni a szövegek ismétlését, duplikálását, valamint automata ellenőrzések alá tudják vonni az olyan szerzőket, akik több tucat könyvet adnak ki.

Védelmi megoldások, javaslatok

Az e-könyveket és alkalmazásokat mindig **csak elismert, jó hírű áruházból érdemes beszerezni** (Amazon, Google Play, App Store). Ez nagyban csökkenti a fertőzött fájlok letöltésének kockázatát. Ha ezektől eltérő oldalon vásárol, győződjön meg arról, hogy a **kereskedő weboldala biztonságos és naprakész**.

Az e-könyv olvasó tudatos használata mellett érdemes valamely **biztonsági alkalmazás telepítése** az e-könyv olvasóra. Ez főleg az olyan eszközökön fontos, mint a Kindle Fire, mert ennek módosított Android operációs rendszere van. Ilyen eszközöket az Amazon Appstore-ból lehet letölteni, például Norton Mobile Security, az Avast! Mobile Security és az AVG AntiVirus.

Kerülje a nyilvános WiFi hálózatok használatát!

Ellenőrizze az alkalmazások által kért **hozzáférési engedélyeket** és gondolja át, hogy valóban szükség lehet-e az adott jogosultság megadására az alkalmazás számára!

Ha e-könyvet vásárol, maradjon olyan szerzőknél, **akiket már ismer**, vagy akiknek már van hírnevük! Ha úgy dönt, hogy olyan szerzőtől vásárol, akit nem ismer, először nézze meg, hogy **letölthet-e egy ingyenes mintát** (az Amazon lehetővé teszi ezt), hogy **tesztelje a minőséget**.

Ne dőljön be az olcsó e-könyveket kísérő **nagyszerű kritikáknak**! Lehet, hogy ezek valódiak, de az is hogy az írókat lefizették az elkészítésükért. **Keressen rá** a könyv nevére vagy a szerzőre, hogy megnézze, mások milyen véleménnyel vannak róla! Érdemes azt is ellenőrizni, hogy az adott szerző milyen egyéb könyvkiadásokkal rendelkezik.

Ne kattintson az e-könyvben található linkekre! Még abban az esetben is azt javasoljuk, hogy a link használata helyett inkább egy internetes böngészőn keresztül látogassa meg a weboldalukat, ha a könyv egy elismert, jó hírű szerzőtől származik.

Ha úgy véli, hogy átverték, **kérje vissza a pénzét**! Az Amazon biztosít erre felületet és visszatérítést adhat, ha a vásárlástól számított 7 napon belül panaszt nyújt be. Panaszát az eladó ügyfélszolgálatán is regisztrálnia kell.

Ha csalás áldozatává vált, **segítse a többi olvasót** azzal, hogy ír egy rossz (de őszinte!) kritikát a könyvről.

Mindig használjon jelszavas védelmet az eszköz zárolására! A jelszavak optimális esetben **minél hosszabbak** és **alfanumerikusak**, vagyis tartalmaznak **kis- és nagybetűket** és speciális karaktereket. Ezeknek a kombinációja, esetleg mondatként vagy kifejezésként való használata megfelelő védelmet nyújt a felhasználónak.

Ha Ön blogger, szerző vagy író, **futtasson rendszeres kereséseket** (vagy állítson be Google-riasztást) **a nevére**, a könyv vagy cikk címére és a műveiből származó kifejezésekre! Ha a szerzői joggal védett művével kapcsolatban **jogsértést észlel**, **lépjen kapcsolatba az illetővel** és tájékoztassa, hogy Ön a szerzői jogok tulajdonosa! Súlyosabb és költségesebb esetekben fontolja meg a **jogi tanácsadás igénybevételét**, a jogsértés megszüntetésére vonatkozó felszólítást, sőt, akár az elmaradt jogdíjak visszaszerzése érdekében is lépéseket tehet.

Egyes hitelkártya-társaságok lehetővé teszik a kártyabirtokosok számára egy olyan alkalmazás használatát, amely egy **ideiglenes, egyszeri hitelkártyaszámot** generál. Érdemes lehet megfontolni ezek használatát, ugyanis, ha el is lopják, az értéktelen a csaló számára.

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36(1)325 7672

Nemzeti Kibervédelmi Intézet

@nki.gov.hu

Kibertámadás!
podcast

2022