NEMZETBIZTONSÁGI SZAKSZOLGÁLAT 1996
Fortes fortuna adiuvat

NEMZETI KIBERVÉDELMI INTÉZET

Az NBSZ NKI arra hívja fel a figyelmet, hogy az elmúlt hetek során ugrásszerűen megemelkedett az alábbi témakörökhöz kapcsolódó csaló üzenetek száma.

CSALÓ ÜZENETEK

Az adóbevallási időszakra hivatkozó, NAV nevével visszaélő csaló üzenetek

ADATHALÁSZAT

Bankokat megszemélyesítő adathalász üzenetek

ZSAROLÓ ÜZENETEK

Sextortion zsaroló üzenetek

További információkért látogasson el az nki.gov.hu weboldalra

e-mail cím: CSIRT@nki.gov.hu

Telefon: +36 (1) 3257672

Az adóbevallási időszakra hivatkozó, NAV nevével visszaélő csaló üzenetek

Az ilyen jellegű támadások ellen megfelelő védekezési módszer lehet egy jó gyakorlat kialakítása: bármilyen forrásból érkezzen is egy szolgáltatással kapcsolatos hír vagy üzenet, legelőször javasolt minden esetben felkeresni az adott szervezet hivatalos tájékoztatási csatornáját, és ott ellenőrizni az üzenetben szereplő információkat!

Ezeket a címeket első lépésben a böngésző címsorába kézzel begépelve érjük el, jó gyakorlat azonban, ha ezt követően a fontos webhelyek címeit elmentjük a könyvjelzők közé.

A NAV - más hivatalos szervezetekhez hasonlóan - soha nem kéri a bankkártya adatok megadását!

A kiberbűnözők módszerei között évről-évre megfigyelhető az adóbevallási időszakhoz köthető fokozott adathalász tevékenység. Az adózási és adójóváírási időszak során küldött megtévesztő üzenetek célja: érzékeny, személyes adatok (pl. adószám, bankkártya, vagy kapcsolati adatok) megszerzése, illetve pénz kicsalása az áldozattól.

Az ilyen csaló, hamis oldalak megtévesztésig hasonlítanak az eredeti honlapokra, azonban kellő elővigyázatossággal és óvatossággal megtalálhatjuk azokat a gyanús elemeket, amelyek segíthetnek eldönteni, hogy az oldal valódi, vagy hamis (lásd a fenti képen). Ilyenek például:

- a weboldal címe (URL);
- nyelvhelyességi és helyesírási hibák;
- pontatlan és szakmaiatlan megfogalmazás.

FONTOS ÜZENET

EN **Erste NetBank <sinicalizy@pakuki.sk>** 2020. április 13., hétfő 9:36

Kedves Erste NetBank ügyfél!

A minőségi és biztonságos szolgáltatás biztosítása érdekében adatbázisunkban rendszeres karbantartást végezünk. Őszintén kérjük, hogy ellenőrizze és frissítse fiókját, hogy elkerülje bármiféle laxitást vagy a szolgáltatás megszakítását.

KATTINTSON IDE:https: //netbank.erstebank.hu
személyazonosságának megerősítése érdekében.

https://southernlites.net/Erste NetBank.html

Ezt az utasítást az Erste NetBank összes ügyfele elküldte, és be kell tartani.

Kösz.
Erste NetBank Zrt.

A pénzintézetek nevében elkövetett csaló kampányok folyamatosan jelen vannak az online térben.

Az ilyen témakörben küldött csaló üzeneteknél a gyanús jellegzetességekre ugyanúgy felfigyelhetünk, a korábban említett javaslat pedig szintén érvényes: ne a levél linkjén keresztül érjük el az adott pénzintézet weboldalát, hanem a böngészőből mi magunk keressünk rá a hivatalos weboldalra és ellenőrizzük le, hogy az üzenetben közölt információk valósak-e.

Tipp: vigyük az egér kurzorját a levélben szereplő linkre, és így megláthatjuk az eredeti linket.

Néhány bank és a Magyar Bankszövetség hivatalos webes elérhetősége:

Budapest Bank: https://www.budapestbank.hu/
CIB Bank: https://www.cib.hu/
ERSTE Bank: https://www.erstebank.hu
K&H Bank: https://www.kh.hu/bank
Magyar Bankszövetség: http://www.bankszovetseg.hu/
MKB Bank: https://www.mkb.hu/
OTP Bank: https://www.otpbank.hu/
Raiffeisen Bank: https://www.raiffeisen.hu/
Takarék Bank: https://www.takarekbank.hu/

Tárgy: [SPAM] Magas veszély. Fiókját feltörték. Kérjük, azonnal változtassa meg jelszavát.
Date: Mon, 20 Apr 2020 15:48:57 +0200
From: cert@govcert.hu
To: cert@govcert.hu

Hello!
Nagyon rossz hírem van neked.
05.02.2020 - Ezen a napon csapkodtam az operációs rendszerre és hozzáférést kapott fiókjához: cert@govcert.hu

Igen, megváltoztathatja a jelszavát ... De a rosszindulatú programom minden alkalommal frissíti.

Hogyan csináltam:
Az útválasztó szoftverében, amelyet az internethez használt volt egy sebezhetőség.
Felcsaptam ezt az útválasztót, és rátelepítettem a rosszindulatú kódomat.
Miután csatlakozik az internethez, a vírusomat telepítették az eszköz operációs rendszerére.

Ezután teljes másolatot készítettem az Ön adataiból (a böngésző előzményei, az összes fájl, telefonszám és minden kapcsolattartó cím).

Egy hónappal ezelőtt le akartam zárni a készüléket és pénzt kértem a feloldó kódért.
De megnéztem azokat a webhelyeket, amelyeket rendszeresen meglátogatott, és megdöbbent az, amit láttak!
Úgy értem, felnőtt oldalak!

Úgy értem - te nagy perverz vagy. Képzeleted távol áll a normális ember szexuális felfogásától.

És jól gondoltam ...
Készítettem egy képernyőképet webhelyekről, ahol jól érezted magad (tudod, miről beszélek, ugye?).
Aztán fényképeztem a maszturbációdat a készülék webkamerajának használatával.
Csodálatosnak bizonyult! Olyan látványos vagy!

Biztos vagyok abban, hogy nem akarja megjeleníteni ezeket a képernyőképeket a barátok, rokonok vagy kollégák számára.
Úgy gondolom, hogy az 1250€ nagyon kis összeg a csendért.
Ráadásul sokáig kémtelek téged, miután sok időt töltöttem!

Csak a Bitcoins-ban fizet!
BTC-tárcám: 125iYH3kh9y4EoEs1YNcAywY3aeAqqvUuo

Nem tudod, hogyan küldhetek nekem Bitcoinekat?
Írjon be egy lekérdezést bármelyik keresőmotorba: "Hogyan vásároljunk bitcoineket".
Rendkívül egyszerű.

Két napot kapok neked a fizetéshez (48 óra).
Amint ez a levél megnyílik, az időzítő működni fog.

Fizetés után a vírusok és piszkos videók automatikusan megsemmisülnek.
Ha nem kapom meg a megadott összeget: az eszköz le lesz zárva, és az összes barátod vagy rokonod, talán egy kolléga kap egy fényképet az Ön "öröméről".

Remélem megértette a helyzetét.
- Ne próbálj megtalálni és megsemmisíteni a vírusomat! (Az összes adat, fájl és képernyőkép már fel van töltve egy távoli szerverre);
- Ne próbáljon kapcsolatba lépni velem (ez lehetetlen, ezt az e-mailt hoztam létre a fiókodból.);
- Különböző biztonsági szolgáltatások nem fognak segíteni: A lemez formázása vagy az eszköz megsemmisítése nem segít, mivel az adatok már egy távoli szerveren vannak

Egy jelenleg terjedő Sextortion zsaroló levél

A sextortion zsaroló üzenetek igyekeznek ráijeszteni az áldozatukra és bűntudatot kelteni bennük, azzal a hamis állítással, hogy szexuális tartalmú kompromittáló felvételekkel rendelkeznek az áldozatról.

Ne higgyünk az ilyen üzeneteknek! Ha a kiberbűnözők valóban rendelkeznének kompromittálásra alkalmas tartalommal, logikus lenne ezt bebizonyítaniuk egy példa bemutatásával, ehelyett csupán az áldozat e-mail címét és/vagy jelszavát jelenítik meg, amelyet több forrásból is megszerezhetnek.

További hasznos információkért látogasson el Intézetünk weboldalára (https://nki.gov.hu) és kövessen minket Facebookon (@Nemzeti Kibervédelmi Intézet), valamint Instagramon (@nki.gov.hu).