TLP: WHITE
Szabadon terjeszthető!

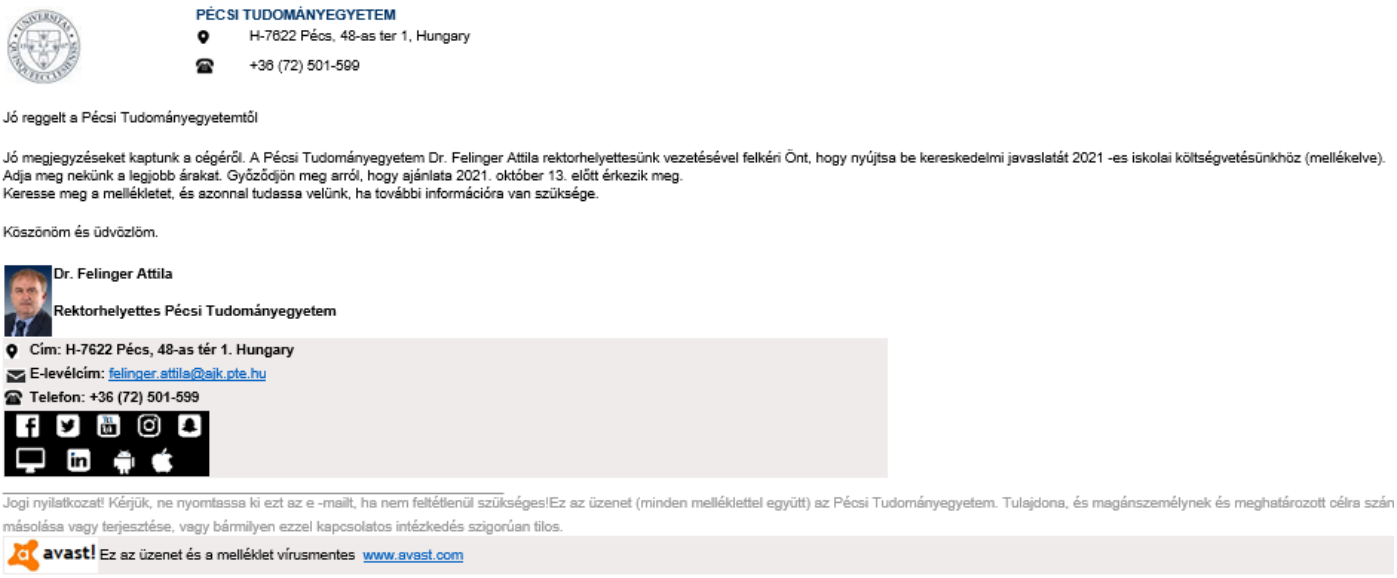
Tájékoztatás
A Pécsi Tudományegyetem nevével visszaélő, káros csatolmányt tartalmazó levelekkel kapcsolatban

(2021. október 8.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) tájékoztatást ad ki a Pécsi Tudományegyetem nevével visszaélő, káros csatolmányt tartalmazó levelekkel kapcsolatban.

Intézetünk számos bejelentést kapott a Pécsi Tudományegyetem nevében kiküldött, káros csatolmányt tartalmazó levelekkel kapcsolatban. A levél csatolmányában egy excel fájl (**Ajánlatkérés 2021.xlsm**) található, amely egy trójai típusú malware-t, a **Lokibot** egyik variánsát tartalmazza.



PÉCSI TUDOMÁNYEGYETEM
H-7622 Pécs, 48-as ter 1, Hungary
+36 (72) 501-599

Jó reggelt a Pécsi Tudományegyetemtől

Jó megjegyzéseket kaptunk a cégéről. A Pécsi Tudományegyetem Dr. Felinger Attila rektorhelyettesünk vezetésével felkéri Önt, hogy nyújtsa be kereskedelmi javaslatát 2021 -es iskolai költségvetésünkhöz (mellékelve).
Adja meg nekünk a legjobb árakat. Győződjön meg arról, hogy ajánlata 2021. október 13. előtt érkezik meg.
Keresse meg a mellékletet, és azonnal tudassa velünk, ha további információra van szüksége.

Köszönöm és üdvözlöm.

Dr. Felinger Attila
Rektorhelyettes Pécsi Tudományegyetem
Cím: H-7622 Pécs, 48-as tér 1. Hungary
E-levélcím: felinger.attila@ajk.pte.hu
Telefon: +36 (72) 501-599

Jogi nyilatkozat! Kérjük, ne nyomtassa ki ezt az e -mailt, ha nem feltétlenül szükséges!Ez az üzenet (minden melléklettel együtt) az Pécsi Tudományegyetem. Tulajdona, és magánszemélynek és meghatározott célra szán másolása vagy terjesztése, vagy bármilyen ezzel kapcsolatos intézkedés szigorúan tilos.

avast! Ez az üzenet és a melléklet vírusmentes www.avast.com

A káros csatolmányú levelek kiszűrése érdekében a Nemzeti Kibervédelmi Intézet az alább indikátorok tiltását / szűrését javasolja:

Ip: 136[.]243[.]159[.]53

Url: hxxp://136[.]243[.]159[.]53/~element/page[.]php?id=172

Beérkezett excel állomány: "Ajánlatkérés 2021.xlsm"

md5: c905b387d8889b669fbed95a6a252d30

sha256: 995e9fafe57d7228634d9acd7035bb4f3462dfff4d2061f78552869952523324

Futtatható fájl: Jtcrizlraiobuopr[.]exe

sha256: d51f9cd3b67f68e9df9af50fd1bf3b4f5676ac55f352ae0d44fc431f5e7986df

A fenti indikátorok szűrésén túl javasolt a fogadó oldalon az SPF rekordok ellenőrzésének kikényszerítése. Az SPF beállítások megfelelő alkalmazásával biztosítható, hogy ha olyan szervezet nevében érkezik levél, akinek van beállított SPF rekordja, akkor a fogadó oldali levelezőrendszer azt visszaellenőrizve meg tudja állapítani a feladó valódiságát. További, SPF rekorddal kapcsolatos információk a https://nki.gov.hu/it-biztonsag/tartalom/eszkoztar/spf/ oldalon érhetőek el. Az elektronikus levelezés biztonsági beállításaival kapcsolatban további javaslatok a Közigazgatási Kibervédelmi Eszköztárban találhatóak.

További hivatkozások:

- https://nki.gov.hu/wp-content/uploads/2019/03/NKI_White_Paper.pdf

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Fax: +36-1-336-4886
Incidensbejelentés: csirt@nki.gov.hu