



EIVOK-1 3. INFORMÁCIÓBIZTONSÁGI SZAKMAI FÓRUM

CYBER- MESÉK

AZ ELŐADÁS MÓDJA:

A

B

MIRE SZÁMÍTHATUNK MA?



THINK OUT OF THE BOX



WHOAMI

- Computer Security Incident Response Team (CSIRT)
- Azért nem CERT, mert az fizetős 😊
- Azért sem, mert EU
- Lényegében CSIRT=CERT, nincs számottevő különbség

IRÁNYTŰ



CYBERSPACE

JOG

- 2013. évi L. (Ibtv.) - számítógépes eseménykezelő központ 10. fejezet, 20. § - Feladatok
- 271/2018. (XII. 20.) Korm. rendelet - az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól.
- AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/1148 IRÁNYELVE a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (NIS irányelv)
- A Bizottság C(2017) 6100 számú ajánlása a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról (BluePrint)
- stb.

ÜGYFELEK



Megfelelőség (hatóság)



Incidenskezelés



Sérülékenységvizsgálat

MESÉK



INCIDENS BEJELENTÉSE #1

- Lövik az R6 szervert
- Hogyan változtassam meg a jelszavam, nem tudok belépni?
- Mondják meg, ki volt, odamegyek!
- „Exem mesztelen hamis fotókat töltött fel rólam”
- Ki a Facbook profil tulajdonosa, beszélgetnék vele...

INCIDENS BEJELENTÉSE #2

Zsarolólevelet kaptam!

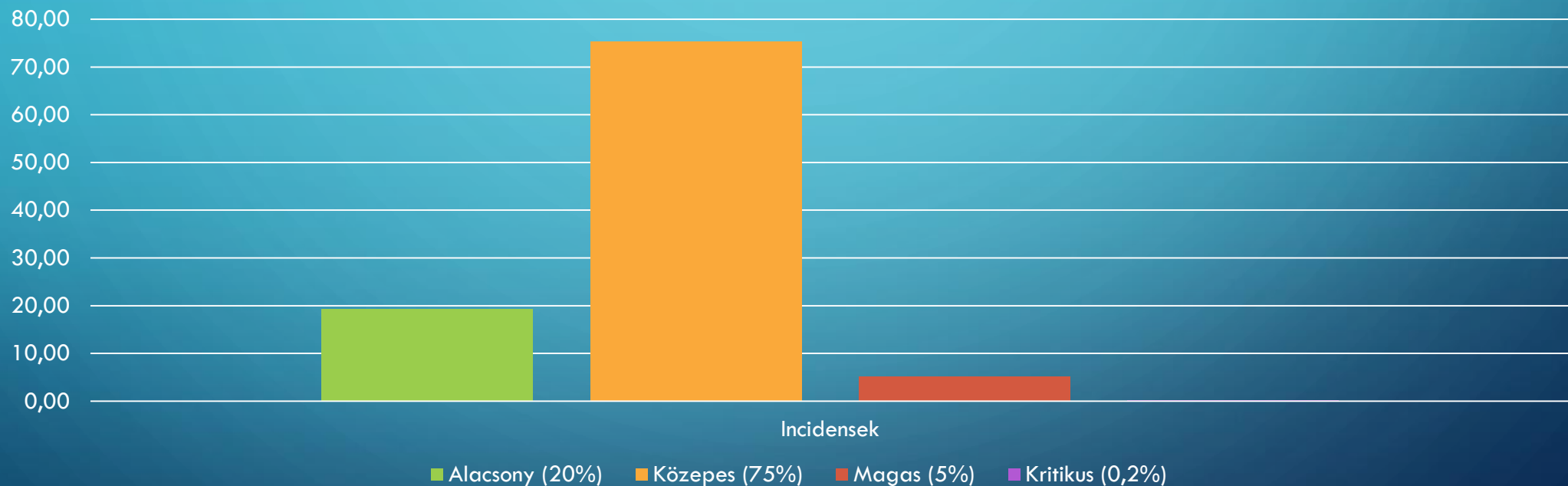
Megadom Önöknek a jelszavam, a felhasználónevem,
az oldalt, ahol azt használom,
minden adatot átadok Önöknek, csak kérem segítsenek!

VAN MÉG...

- Zaklatott tudós / professzor
- Zavaros, üldözési mániás állampolgárok (mikrohullám, nanotechnológia)
- Sz.gép bevizsgálása
- Hivatalos feljelentők
- Unatkozók
- ...és néha tényleges incidens is

NINCS JÓ MOZI DIAGRAM NÉLKÜL

Incidensek kockázat szerinti eloszlása – 2019.



KOMOLYRA FORDÍTVA A SZÓT...

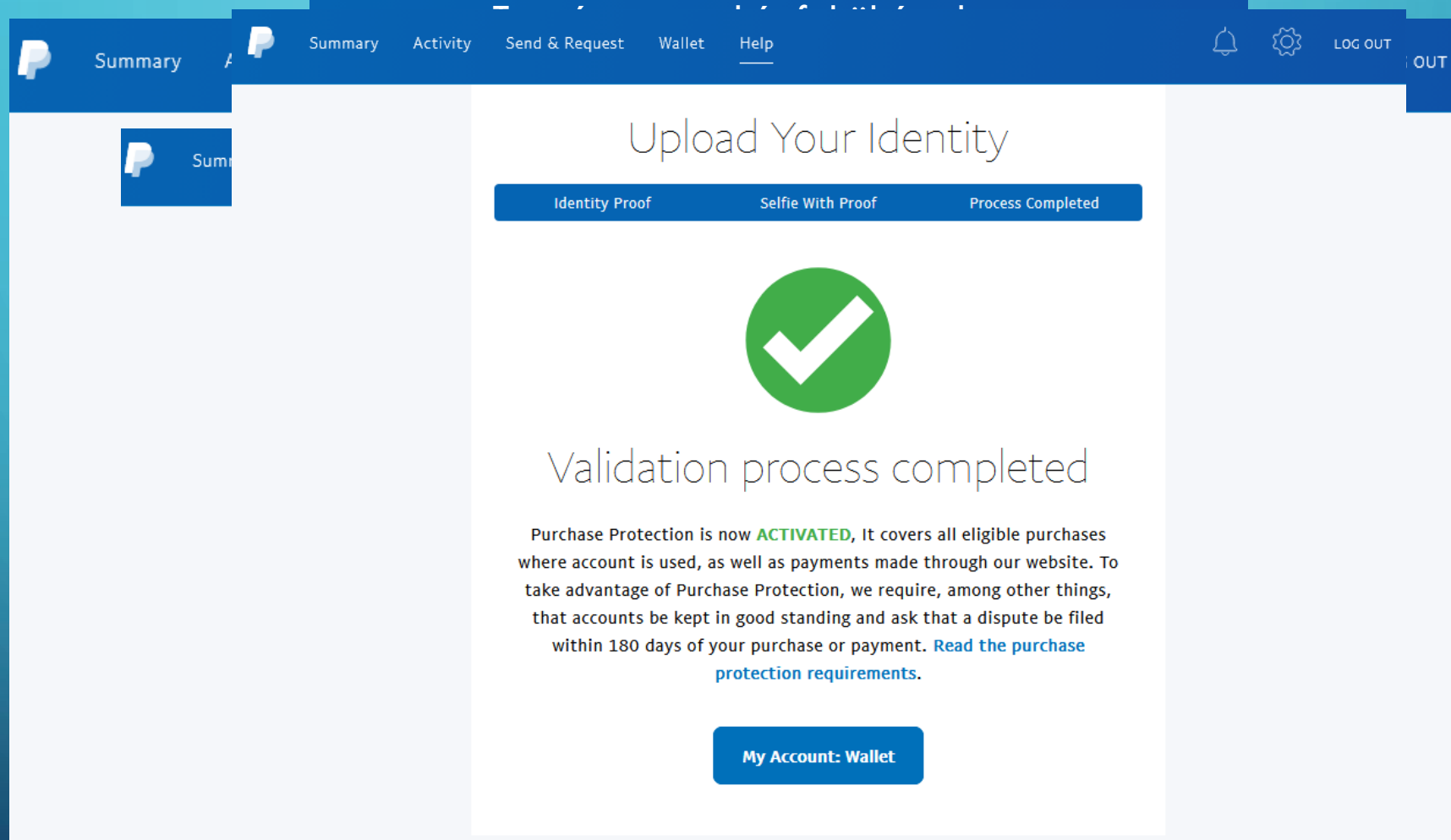
- Kórház
- Múzeum
- Kliensek
- Adathalászat

E-MAIL KLIENSEK

- Active Sync
- MyMail

PHISHING

Fiók korlátozása: lényeg, hogy validátsd magad!
Az OTP ... Es végül kézzel kell bekérni a banki adatokat is:



TLP:AMBER



TUDATOSÍTÁS

Pár napja történt...

Újra „beindultak” a csalók!

A napokban ismét több bejelentés érkezett a Nemzeti Adó- és Vámhivatalhoz (NAV), miszerint adathalászok kíséreltek megszerezni ügyfélkapus bejelentkezési és bankkártyaadatokat. A csalók nem fáradnak, újra és újra próbálkoznak. Senki ne dőljön be!

A NAV informatikai fejlesztései révén már nagyrészt elektronikusan kommunikál ügyfeleivel. Az adathalászok ezt használják ki, és megpróbálnak bizalmas információkat szerezni. A NAV nevében írt adó-visszatérítés lehetőségére felhívó elektronikus levelek, SMS-ek hibás nyelvi fordulatokat, tegező megszólítást, értelmezhetetlen szövegrészleteket tartalmaznak.

A csaló e-mailek és SMS-ek általában egy linket is tartalmaznak, ami a gyanútlan ügyfelet egy felugró űrlapra vagy honlapra vezeti. Az űrlapon a csalók általában a bankkártyák hátlapján található háromjegyű számot, az úgynevezett CVV/CVC kódot vagy az ügyfélkapus bejelentkezési adatokat kérik. Ha valaki megadja a bankkártyaadatait, számolnia kell azzal, hogy illetéktelenek pénzt emelhetnek le számlájáról.

Az ügyfélkapus adatokat mindenki csak a megfelelő oldalon (**www.nav.gov.hu**, **www.magyarorszag.hu**) adja meg, ugyanis a csalók sokszor olyan oldalakat szerkesztenek, amelyek arculati elemeiben is rendkívül jól utánozzák a valós bejelentkezési felületeket, azonban a webcím ebben az esetben árulkodó lehet.

A NAV soha, semmilyen körülmények között nem kér bankkártyaadatokat!

A NAV értesítési gyakorlata merőben eltér a megtévesztő módszertől, a hivatal ugyanis Ügyfélkapun keresztül, illetve postán, adószámla-kivonaton értesíti az ügyfeleket a túlfizetésként megjelenő tételekről.

A túlfizetést csak a 1917-es nyomtatvánnyal lehet visszaigényelni, „linkre kattintással” nem.

A gyanús üzenetekkel kapcsolatos további információkért, hasznos tanácsokért látogasson el a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézetének (NBSZ NKI) [honlapjára](#) .

KÉRDÉSEK

„Ez mind szép és jó mese, de hogyan tovább? Hogyan tudunk együttműködni?”

„Miért is hívtuk meg őket?”

„Vajon elérem még a buszomat, ha most észrevétlenül lelépek?”

„Jó, de hogyan tudnak segíteni?”

„Ez most komoly?”

„Jé, a 'Pacific Ocean'-ban minden ,c'-t máshogy ejtünk”

„Tényleg jelentsem be a spam-et is?”

„Hová is kell az incidenseket jelenteni?”

„Melyik is volt a Fourier sor?”