NE AKADJ **HOROGRA!**

Hogyan lehet felismerni és elkerülni az

ADATHALÁSZ TÁMADÁST

MI AZ ADATHALÁSZAT?

Az adathalászat során a támadók megszemélyesítés útján valamilyen érzékeny – például bejelentkezési – adatot igyekeznek kicsalni a célszemélytől. Mindezt leggyakrabban e-mail, SMS, vagy közösségi média hálózaton keresztül küldött üzenet formájában teszik, de előfordulhat, hogy telefonon keresik fel az áldozatot.

ADATHALÁSZ MÓDSZEREK

E-MAIL

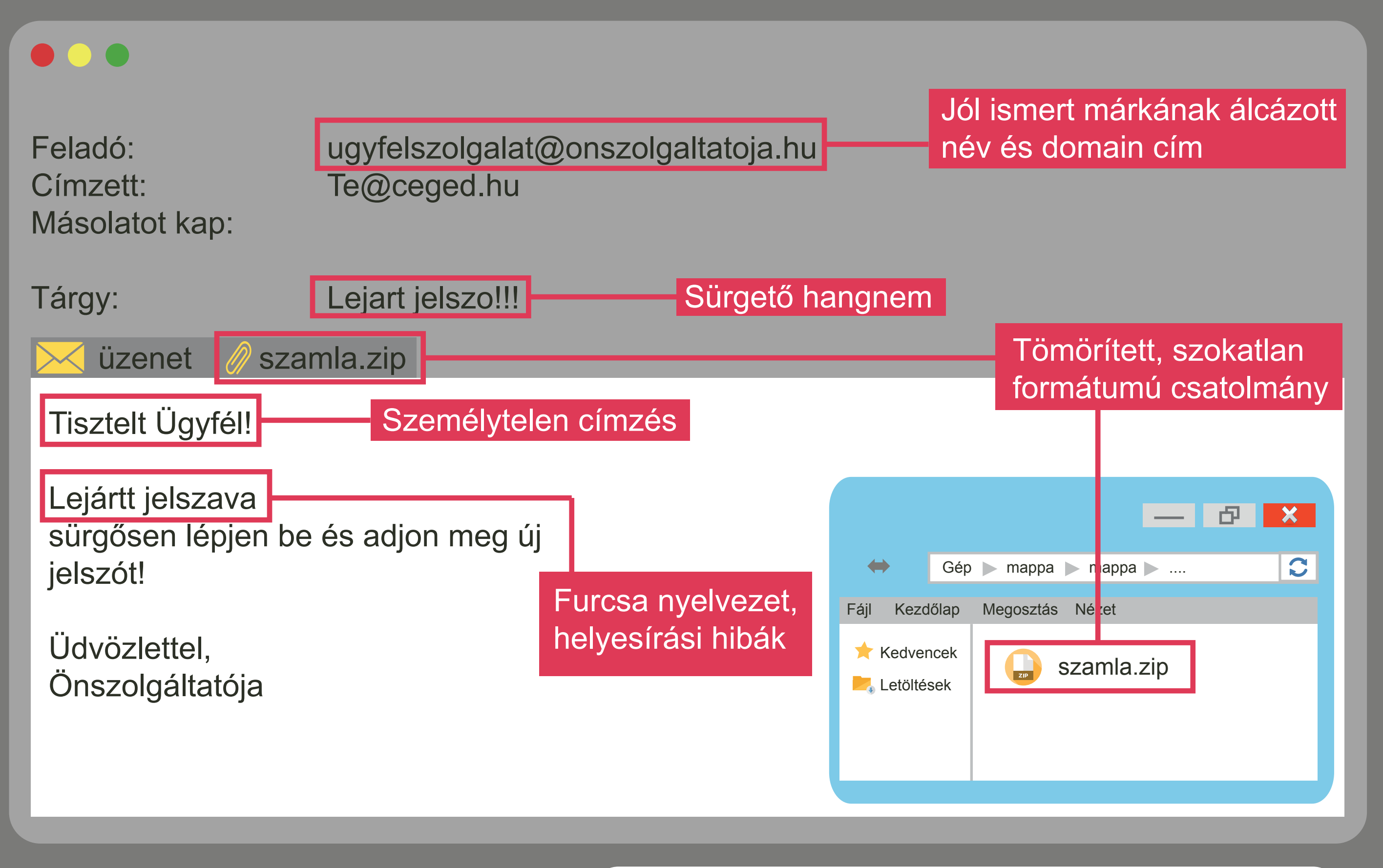
TELEFON

KÖZÖSSÉGI OLDALAK

E-MAIL

A csalók olyan megtévesztő e-mailt küldenek az áldozatnak, amelyek látszólag hivatalos forrásból származnak, és egy portálra mutató linket és/vagy csatolmányt tartalmaznak.

MIRE ÉRDEMES FIGYELNI?



Feladó: ugyfelszolgalat@onszolgaltatoja.hu
Címzett: Te@ceged.hu
Másolatot kap:

Tárgy: Lejart jelszo!!!

üzenet | szamla.zip

Tisztelt Ügyfél!

Lejártt jelszava sürgősen lépjen be és adjon meg új jelszót!

Üdvözlettel,
Önszolgáltatója

Jól ismert márkának álcázott név és domain cím

Sürgető hangnem

Tömörített, szokatlan formátumú csatolmány

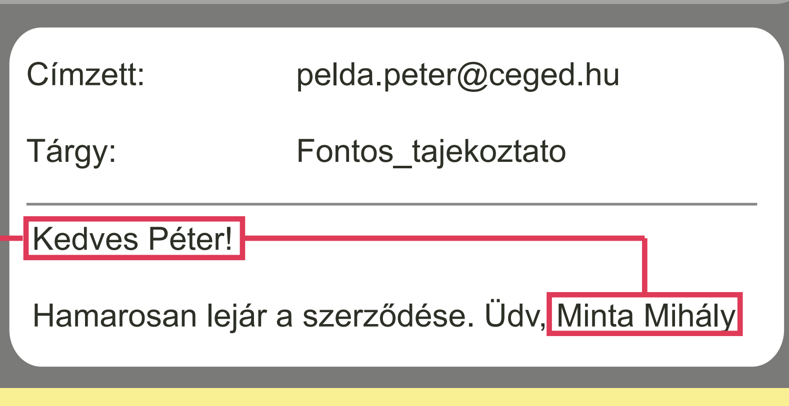
Személytelen címzés

Furcsa nyelvezet, helyesírási hibák

Személyre szabott üzenet

- szofisztikált támadások esetén:
  - ➔ személyes megszólítás
  - ➔ a levél végén megadott referencianév

Kiemelten veszélyeztetettek a pénzügyi osztályokon dolgozók!



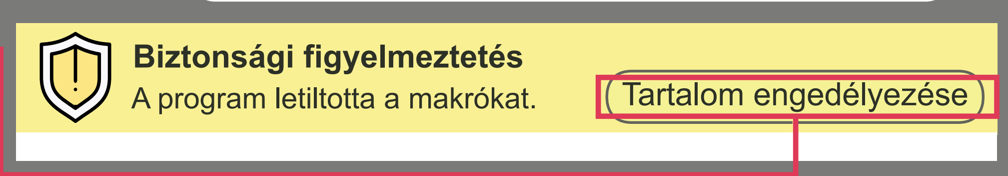
Címzett: pelda.peter@ceged.hu
Tárgy: Fontos_tajekoztato

Kedves Péter!

Hamarosan lejár a szerződése. Üdv, Minta Mihály

Beágyazott káros kódok

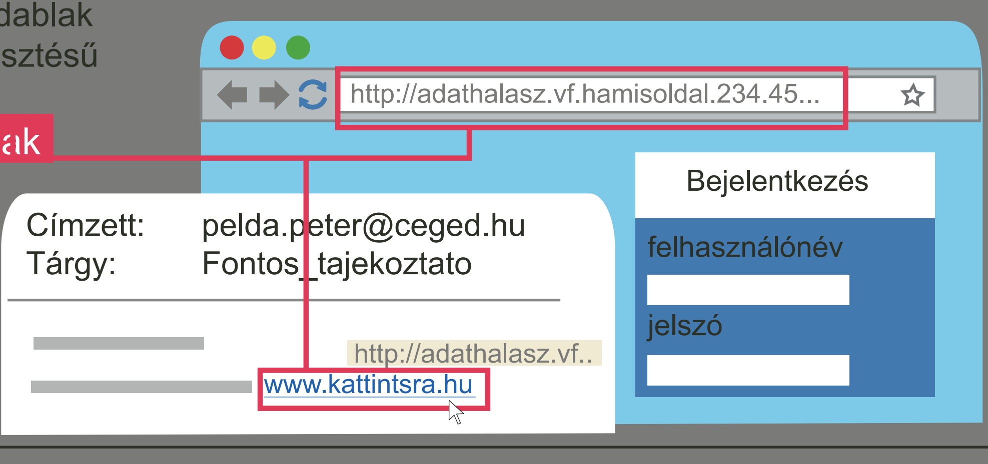
- a beágyazott káros kódok miatt felugrik a makrók engedélyezése párbeszédablak
- *.doc, .xls, .ppt stb.* kiterjesztésű dokumentumok



Biztonsági figyelmeztetés
A program letiltotta a makrókat.

Meghamisított weboldalak

- a legitimhez hasonló megjelenésű weboldalak
- az e-mailben szereplő link más (a hamisított) weboldalra mutat



http://adathalasz.vf.hamisoldal.234.45...

Címzett: pelda.peter@ceged.hu
Tárgy: Fontos_tajekoztato

http://adathalasz.vf..
www.kattintsra.hu

TELEFONOS ADATHALÁSZAT

Előfordul, hogy a támadók telefonon veszik fel a kapcsolatot áldozataikkal, hogy a gyors kommunikáció során a célszemély hirtelen döntésektől vezérelve osszon meg bizalmas információkat. A hívást megelőzően a támadó a közösségi oldalak segítségével információkat gyűjt áldozatairól, ezáltal erősítve a két fél közötti ismerősnek, olykor bizalmasnak tűnő kapcsolatot.

Közösségi oldalon megadott adatok

- a hívó fél csak a közösségi médiaoldalakon elérhető nyilvános információkra hivatkozik a beszélgetés során

Félelemkeltő trükk

- azonnal intézkedést kívánó veszélyre hívják fel a figyelmet

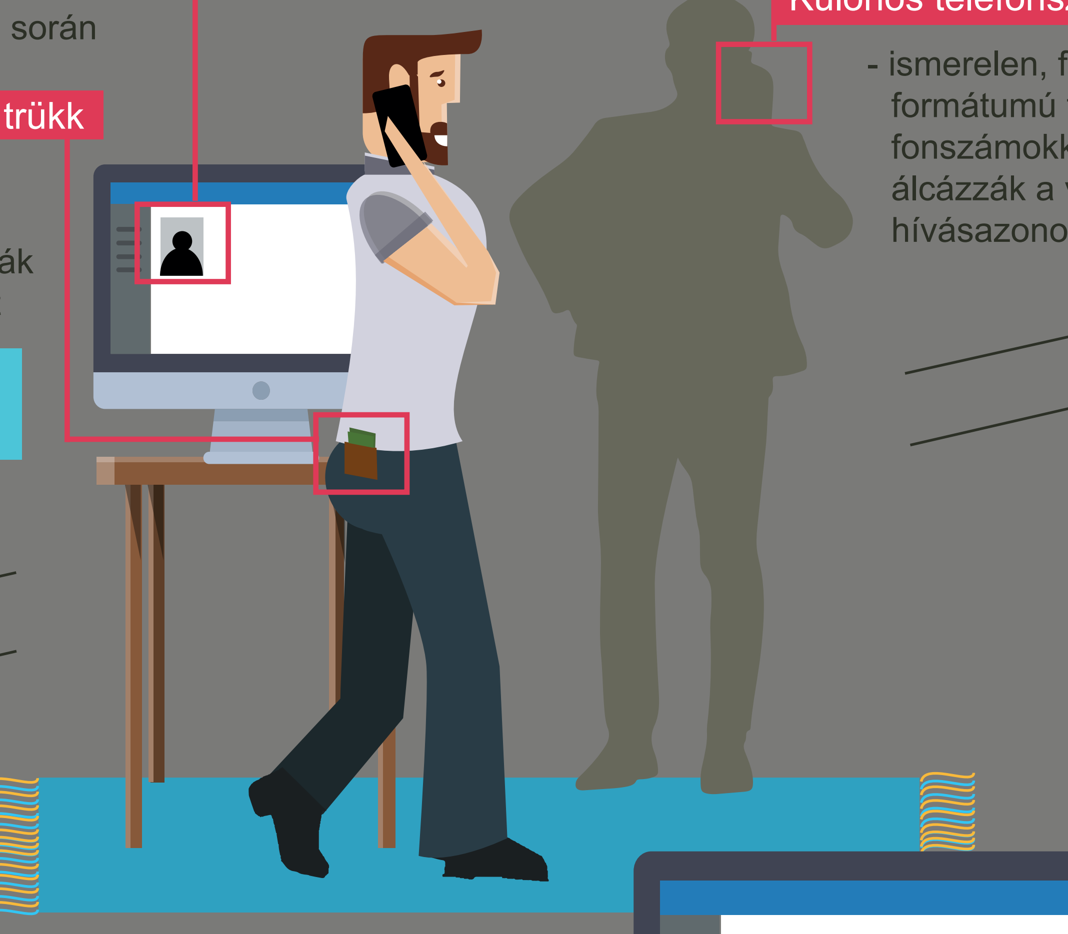
„Veszélyben a pénze!”

Meggyőző taktika

- a túl jó ajánlatok igénybevételéhez az áldozat kénytelen megadni adatait

Különös telefonszámok

- ismerelen, furcsa formátumú telefonszámokkal álcázzák a valódi hívásazonosítót



Hamisított profilok

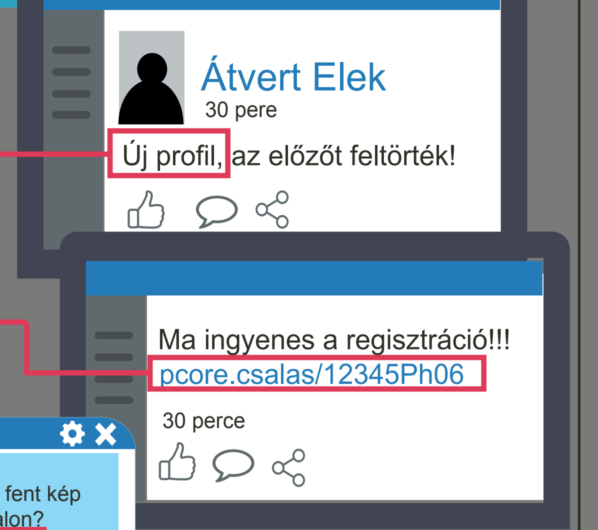
- a támadó másolatot készít egy legitim profilról és arra kéri a követőket/barátokat, hogy az új profilt kövessék

Nem valódi bejegyzések

- kattintásra ösztönző kiírások posztolása, amelyek adathalász weboldalakra irányítják át a felhasználót

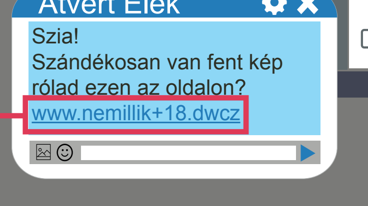
Rosszindulatú programok terjesztése

- a csalók rosszindulatú kódokat tartalmazó weboldalakra irányíthatják át a felhasználót



Átvert Elek
30 pere
Új profil, az előzőt feltörték!

Ma ingyenes a regisztráció!!!
pcore.csalas/12345Ph06
30 perce



Átvert Elek
Szia!
Szándékosan van fent kép rólad ezen az oldalon?
www.nemillik+18.dwcz

KÖZÖSSÉGI MÉDIA

Online biztonságunk érdekében lássunk át a csalin!

Mindig legyünk gyanakvóak **a mások által kezdeményezett olyan kapcsolatfelvételekkel szemben,** amikor nem tudunk minden kétséget kizáróan megbizonyosodni a másik fél identitásáról, ami különösen igaz az elektronikus kommunikációra. Amennyiben a fentiek alapján egy kicsit is gyanúsnak tűnik egy megkeresés, inkább hagyjuk azt figyelmen kívül.

Használjunk a böngészőben adathalász szűrőt, **amelyek ugyan nem nyújtanak 100%-os védelmet,** azonban a már bejelentett adathalász weboldalakról figyelmeztetést kaphatunk.

Ne a levélben megküldött hivatkozásra kattintsunk, **a webes bejelentkezések címeit inkább manuálisan gépeljük be.** A már ellenőrzött felületek címeit mentsük el a könyvjelzők közé, ezzel a későbbiekben jelentősen megkönnyíthetjük a dolgunkat.

Ne nyissuk meg a csatolmányt, **amennyiben ismeretlen forrásból származik, illetve gyanúsnak tűnik a levél.** Mindig figyelmesen olvassuk el a levelezőben felugró figyelmeztető üzeneteket, továbbá kapcsoljuk ki az automatikus makrófuttatási lehetőségeket.

Mindig ellenőrizzük a feladót, **mert néhány esetben már a küldő címéből is megállapítható, hogy a levél nem hivatalos forrásból származik.** Amennyiben ennek gyanúja felmerül, keressük fel az adott szervezetet más csatornán keresztül, és kérjünk megerősítést a kapcsolatfelvétel tényéről.

Ha megtörtént a baj...

- haladéktalanul változtassuk meg jelszavainkat,
- értesítsük az esetről az érintett szervezetet. A szolgáltatók többsége az ilyen jellegű bejelentések fogadására, külön erre a célra kijelölt (abuse) e-mail címet tart fent,
- amennyiben anyagi kár is bekövetkezett, tegyen feljelentést.

1996
Fortes fortuna adiuvat
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET