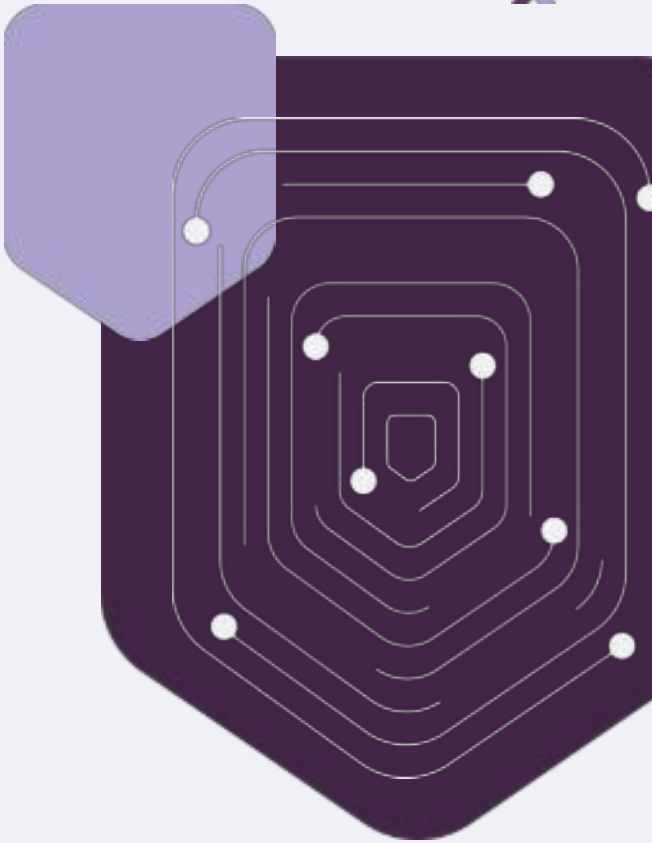
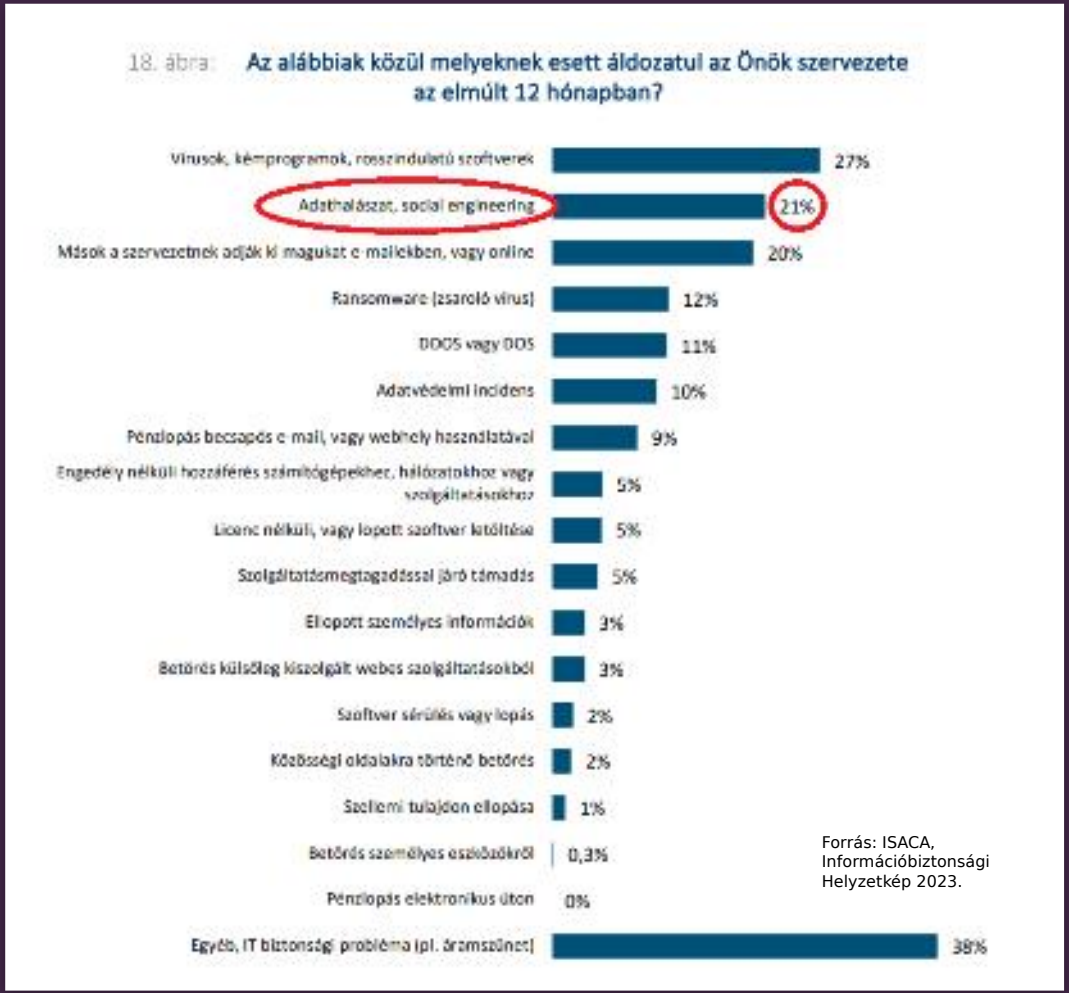
Adathalász szimuláció

Miért kell a kollégákat ilyennel “bosszantani”?
– Dr. Simon Norbert

Hétpecsét Információbiztonsági Egyesület
CVIII. Szakmai Fórum, 2023. november 15.

FORTIX





Forrás: ISACA, Információbiztonsági Helyzetkép 2023.

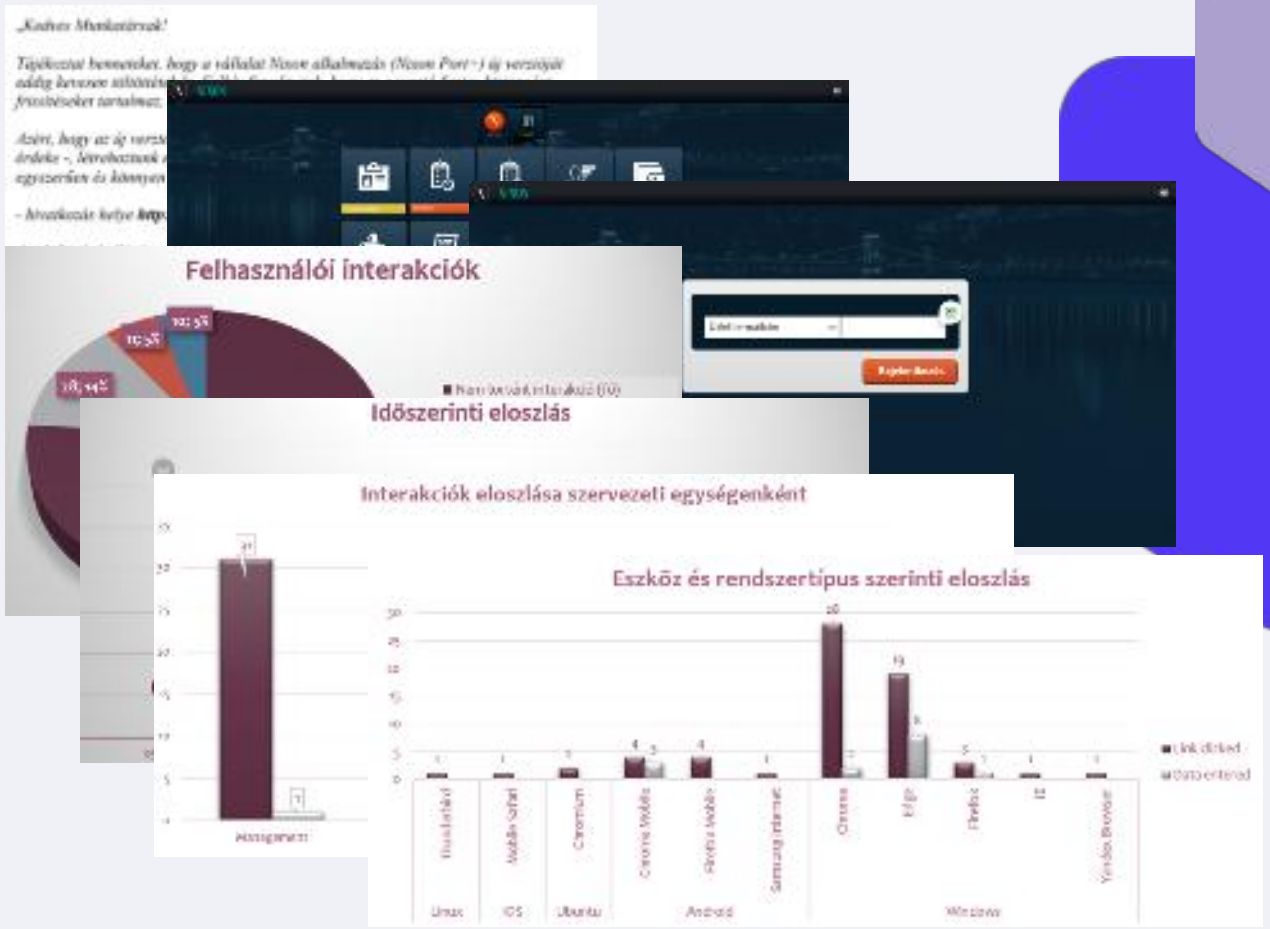
Mi is az adathalász szimuláció?

Ellenőrzött körülmények között egy valós támadás modellezése, amely során a felhasználói viselkedés monitorozásra kerül.

Vizsgált cégek: 100-6.500 fő

Kampány hossza: általában 4-5 nap

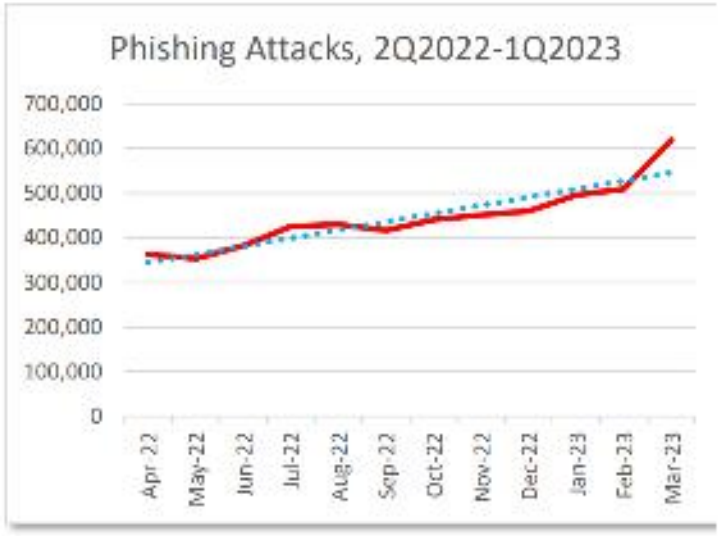
Téma: cégre szabott üzenet


„Kedves Munkatársak!
Felhasználói interakciók
Időszerinti eloszlás
Interakciók eloszlása szervezeti egységenként
Eszköz és rendszertípus szerinti eloszlás
Unix
iOS
Ubuntu
Android
Windows

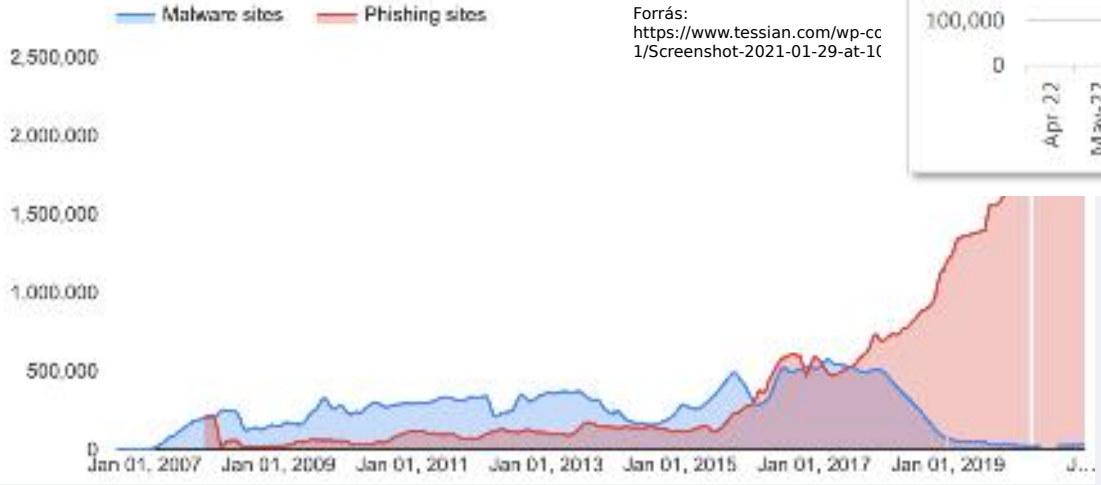
1. Tévhit

“Mi kicsi cég vagyunk.”

Forrás: APWG, Phishing Activity Trends Report, 1st Quarter 2023



Forrás: https://www.tessian.com/wp-cc 1/Screenshot-2021-01-29-at-1(



2. Tévhit

“Nálunk van rendszeres oktatás, a kollégák nem adnak meg adatokat.”

Forrás: LikedIn, The Cyber Security Hub

De mit mutatnak a számok?

A legtöbb interakció az 1-2. napon

57-76% nem nyitja meg az e-mailt

3-11% csak megnyitotta az e-mailt

2-38% megnyitotta az e-mailt és kattintott is a linkre

1-6% adatot is adott meg!!

Néhány érdekes adat

Ahol 144-en adatot írtak be, ebből 17 fő volt irodai alkalmazott vagy felsővezető

Jellemzően az alcsonyabb beosztásban nagyobb az adatbeírási arány

Az országon belül területi különbségek nem mutathatóak ki

Van aki többször is ad meg adatot (pl. adott esetben 6 felhasználó, több, mint 10X

Másodlagos hasznok

Információ a használt böngészőről

Kibuknak az inaktív e-mail fiókok

...

Egy fontos tanulság

Kapkodás...

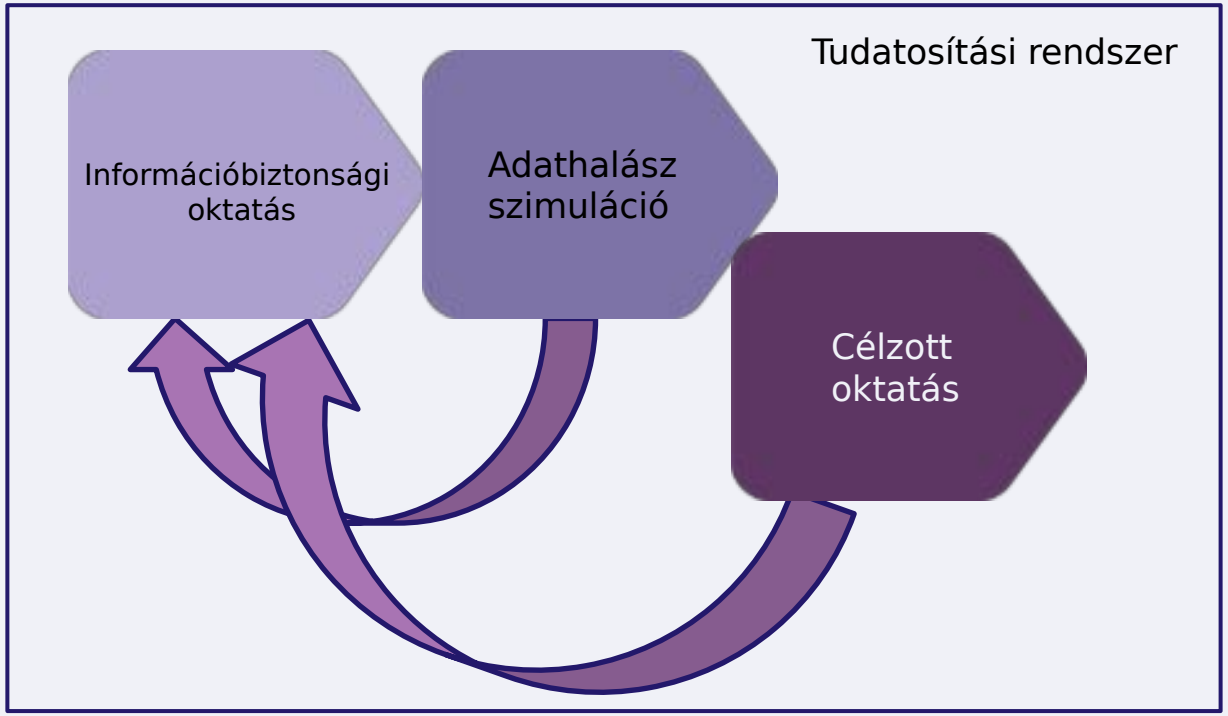
“Túltoltuk, Béláim!”

A fokozatosságra figyelni kell!

Visszajelzés fontossága

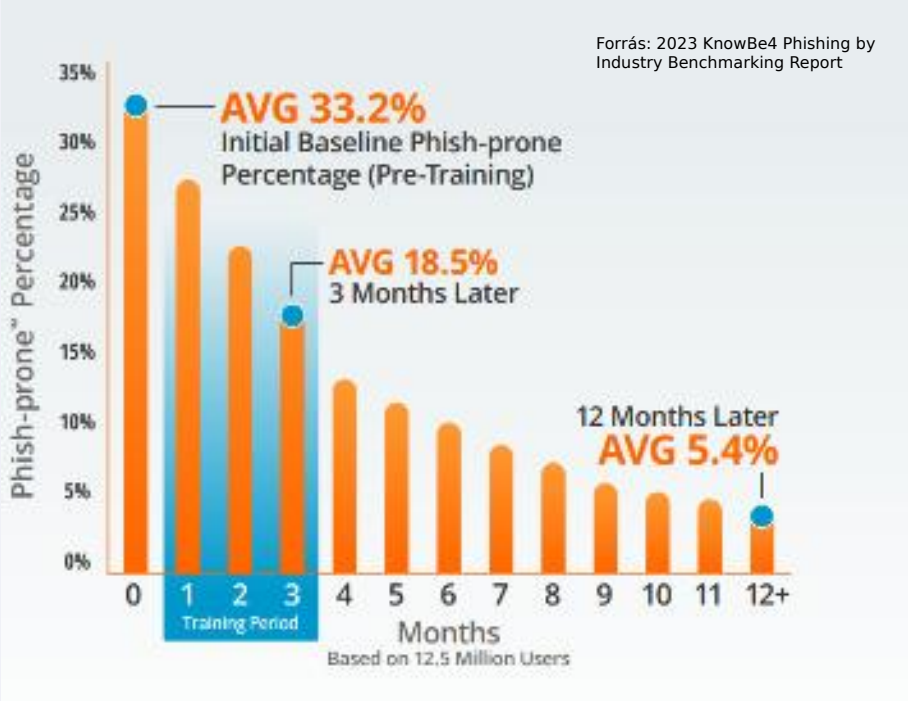
Forrás: https://coub.com/stories/6581-ratoti-legenyanya-jelenetek

A szimuláció szerepe a tudatosításban



Nemzetközi tendenciák

1. FÁZIS: Nincs tudatosítás és tesztelés
2. FÁZIS: Tudatosítás után 90 napon belüli tesztelés
3. FÁZIS: Folyamatos képzés és havi tesztelés



Adatbevitel változása

3 éven belül ismételt szimuláció esetén

5% → 5%

Nincs érzékelhető változás

Adatbevitel változása

Fél éven belül ismételt szimuláció esetén

6% → 1%

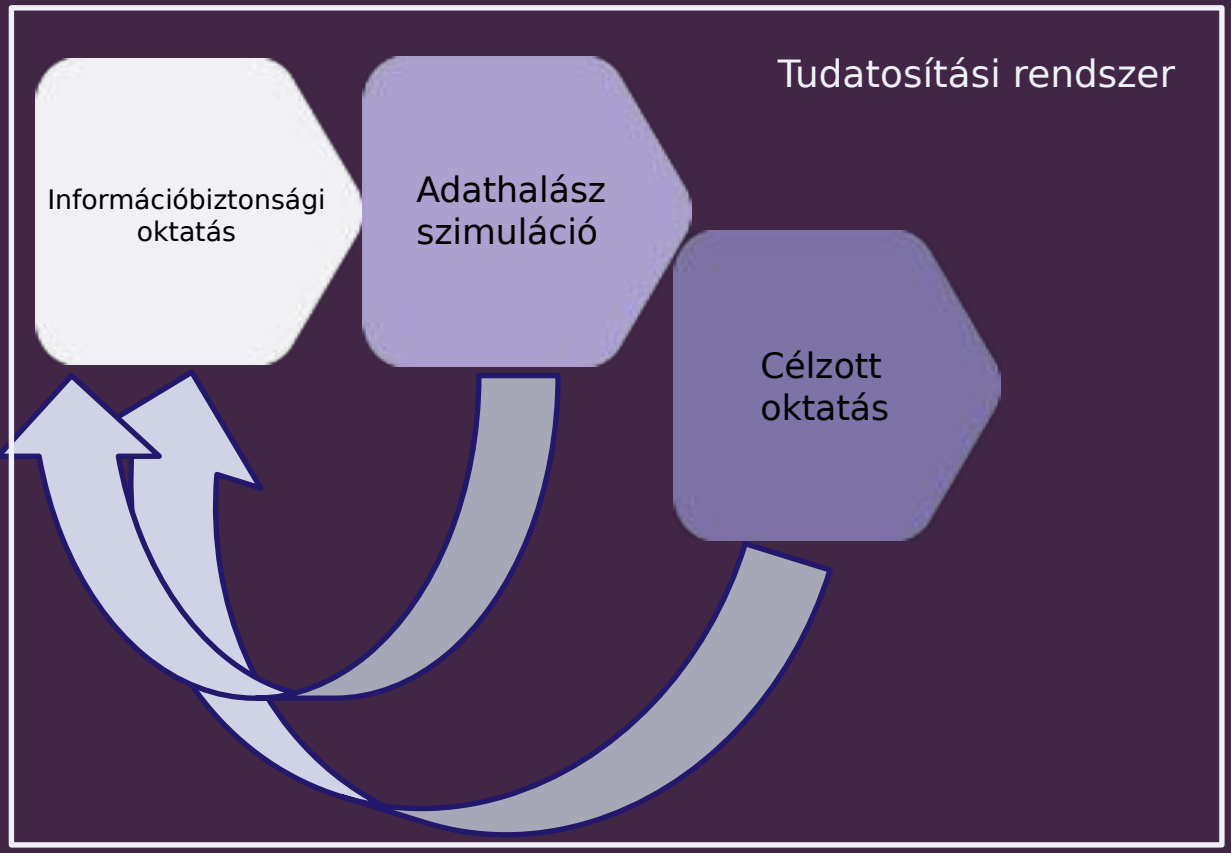
És kb. 200 bejelentés az IT felé az adathalász kísérletről

MI a jövő?

https://www.fortix.hu/phishing-szimulacio/

Tömeges spear phishing (szimulációk) AI segítségével.

Vidd el magaddal!



FORTIX

Kapcsolat:

Dr. Simon Norbert

+36 30 255 7866

norbert.simon@fortix.hu

Külön köszönet a segítségért Kóka Vajk Csanádnak!