Publicația dumneavoastra lunară de sensibilizare asupra securității informatice

# Da, sunteți o țintă

## Prezentare generală

Mulți oameni cred, în mod eronat, că nu sunt o țintă pentru atacatorii cibernetici deoarece ei, sistemele sau conturile lor nu au nicio valoare. Acest lucru este departe de adevăr. Dacă folosiți orice fel de tehnologie, la locul de muncă sau acasă, credeți-ne, sunteți valoroși pentru atacatori. Dar nu este totul pierdut. Beneficiați deja de cea mai bună apărare împotriva acestor atacuri cibernetice – dumneavoastră înșivă.

## De ce reprezentați o țintă

Există o mulțime de atacatori cibernetici, fiecare cu motivele lui (ei). Deci, de ce ar vrea să vă atace? Pentru că așa își vor atinge scopul. Iată două exemple comune ale atacatorilor cibernetici și de ce v-ar putea viza.

**Criminali cibernetici:** Scopul lor este sa facă oricât de mulți bani se poate. Internetul este foarte valoros pentru ei, deoarece astfel pot viza cu ușurință pe oricine doar prin apăsarea unui buton. Și există o MULȚIME de metode prin care pot face bani cu informația dumneavoastră. Printre exemple se numără: furtul de bani din conturi bancare sau de pensie, crearea unui card de credit în numele dvs., folosirea calculatorului dvs. pentru a ataca alte persoane sau spargerea conturilor dvs. de pe rețelele de socializare și vânzarea lor altor criminali. Sunt nenumărate metodele prin care atacatorii pot face bani prin intermediul dvs. Există sute de mii de astfel de criminali care se trezesc în fiecare dimineață cu scopul de a ataca cât mai mulți oameni, inclusiv pe dvs.

**Atacatori la țintă precisă:** Aceștia sunt atacatori cibernetici foarte bine pregătiți, care deseori lucrează pentru guverne, organizații de criminali sau firme concurente, care vă vizează la serviciu. Poate credeți că locul dvs. de muncă nu atrage prea multă atenție, însă veți fi foarte surprinși să aflați că atrage.

- Informațiile cu care lucrați la birou au o valoare extraordinară pentru diverse companii sau guverne.

- **Este posibil ca atacatorii care vă vizează la locul de muncă să nu fie interesați neapărat în dvs. ci vor să vă folosească calculatorul pentru a vă ataca unul din colegi sau alte sisteme informatice.**
- **Este de asemenea posibil ca acești atacatori să fie de fapt interesați în companiile cu care colaborați.**

## Am Anti-Virus, sunt protejat(ă)

OK, sunt o țintă, dar nu este nici o problemă. Voi instala un antivirus și un firewall pe calculatorul meu și voi fi protejat(ă), așa-i? Din păcate, nu. Mulți oameni consideră că sunt protejați o dată ce instalează anumite programe de securitate. Din nefericire, acest lucru nu este în întregime adevărat. Atacatorii cibernetici sunt din ce in ce mai pricepuți, iar multe dintre metodele lor de atac ocolesc cu ușurință tehnologiile de securitate. De exemplu, creează adesea malware special pe care antivirusul nu îl poate detecta. Ocolesc filtrele de e-mail cu un atac personalizat de tip phishing sau vă apelează și vă conving prin diverse metode sa le dați bani, numărul cardului dvs. de credit sau parolele. Tehnologia joacă un rol important în protejarea dvs., dar, în cele din urmă, dvs. înșivă sunteți cea mai bună apărare.

Din fericire, nu este așa de greu sa va protejați, totul se reduce la logică și comportament adecvat când vine vorba de cea mai bună apărare. Dacă primiți un e-mail, un mesaj sau un telefon extrem de urgent, ciudat sau suspect, cel mai probabil este un atac. Pentru a vă asigura că computerul și dispozitivele dvs. sunt protejate, mențineți-le programele la zi activând actualizarea automată. În cele din urmă, utilizați o propoziție-parolă puternică și unică pentru fiecare dintre conturile dvs. Cea mai bună apărare este să fiți conștient de riscurile cibernetice. Nu știți de unde să începeți? Abonați-vă la buletinul informativ OUCH! la sans.org/ouch.

## Versiunea în limba română

Ubisoft este o companie de jocuri. Un creator de lumi, dedicat îmbogățirii vieților jucătorilor cu experiențe de joc originale și memorabile. Aflați mai multe la: https://www.ubisoft.com/en-us/.

## Editor invitat

***Matt Bromiley*** *(@mbromileyDFIR) este expert în planuri de răspuns la incidente si în criminalistică digitală cu peste 8 ani de experiență. A lucrat cu organizații și incidente din întreaga lume. Matt este de asemenea, profesor de criminalistică digitală și planuri de răspuns la incidente, predând cursurile SANS FOR508 și FOR572.*

SANS SECURITY AWARENESS

## Resurse

| | |
|---|---|
| Oprește acel malware: | https://www.sans.org/sites/default/files/2018-06/201806-OUCH-June-Romanian.pdf |
| Inginerie Socială: | https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201701_ro.pdf |
| Atacurile si escrocheriile telefonice: | https://www.sans.org/sites/default/files/2018-07/201807-OUCH-July-Romanian.pdf |
| Propoziții - parolă: | https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201704_ro.pdf |
| Poster – Sunteți o țintă: | https://www.sans.org/u/L23 |