OUCH! | Decembrie 2015

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- Generalități
- Phishing
- Cum vă protejați

# Despre Phishing

## Generalităţi

Email-ul este una din căile primare în care comunicăm. Nu îl folosim în fiecare zi doar în activitățile de la serviciu ci și pentru a ține legătura cu prietenii și familia. În plus, email-ul este acum modul în care majoritatea firmelor asigură servicii online, cum ar fi confirmarea unor achiziții online sau disponibilitatea extraselor de cont. Deoarece atât de mulți oameni din toată lumea depind de email, acesta a devenit una din principalele metode de atac folosite de infractorii cibernetici. În acest număr explicăm conceptul de phishing, o metodă comună de atac pe email, și pașii pe care îi puteți face pentru a folosi email-ul într-un mod securizat.

### Editor Invitat

Dr. Lance Hayden este Managing Director la Berkeley Research Group. Expert în cultura și comportamentele din domeniul securității, este autorul studiului People-Centric Security: Transforming Your Enterprise Security Culture (Securitatea orientată spre oameni: Transformarea culturii securității din firma dumneavoastră), publicat de McGraw-Hill. Îl puteți găsi la **www.linkedin.com/in/drhayden**.

## Phishing

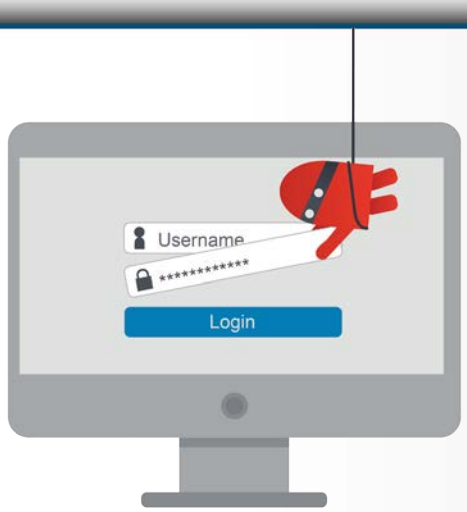
Conceptul de Phishing se referă la un atac care foloseste email-ul sau un serviciu de mesaje precum cele de pe site-urile de socializare online, care vă păcălește îndemnându-vă să recurgeți la o acțiune, cum ar fi să dați clic pe o adresă web sau să deschideți un fișier atașat. Căzând victimă unui astfel de atac riscați ca întreaga bază de informații ultra confidențiale și sensibile să fie furată și/sau computerul să vă fie infectat. Atacatorii depun eforturi foarte mari pentru a face ca mesajele lor de phishing să fie convingătoare. De exemplu, vor face ca email-ul să arate ca și cum ar veni de la cineva sau ceva cunoscut, cum ar fi un prieten, sau o companie în care aveți încredere și pe care o folosiți frecvent. Vor adăuga chiar și sigle ale băncii cu care lucrați sau vor falsifica adrese de email pentru ca mesajul să pară cât mai legitim. Apoi atacatorii transmit aceste email-uri phishing către milioane de oameni. Nu știu cine va deveni victima lor, tot ce știu ei este că cu cât trimit mai multe mesaje, cu atât au mai multe șanse de succes. Phishing-ul seamănă cu folosirea unei plase pentru a prinde pește; nu știi ce vei prinde, dar cu cât ai plasa mai mare, cu atât vei găsi mai mult pește. Există mai multe metode prin care atacatorii folosesc atacurile de phishing pentru a obține ce vor:

- **Culegerea de informații**: Scopul atacatorului este să culeagă informații personale cum ar fi parole, numere ale cardurilor de credit sau detalii bancare. Pentru a face aceasta, vă trimite o adresă care vă direcționează la un site care pare legitim. Acest website vă cere apoi să introduceți informații referitoare la cont sau datele personale. Website-ul este însă unul contrafăcut și orice informație introduceți acolo va ajunge direct la atacator.
- **Adrese ostile**: Scopul atacatorului este de a prelua controlul asupra sistemului dumneavoastră. Pentru a face

## Despre Phishing

aceasta, vă trimite un email cu o adresă. Dacă dați clic pe aceasta, vă va direcționa către un website care va lansa un atac asupra sistemului, care, dacă reușește, vă va infecta calculatorul.

- **Fişiere atașate cu conţinut ostil**: Scopul atacatorului este același: de a infecta și a prelua controlul asupra sistemului pe care îl folosiți. Dar în loc de adresă, atacatorul vă trimite un fișier infectat, cum ar fi un document Word. Deschiderea acestui document atașat va declanșa un atac, oferindu-i atacatorului controlul potențial asupra sistemului dumneavoastră.
- **Escrocherii**: Unele mailuri de phishing nu sunt altceva decât escrocherii transpuse în lumea digitală. Încearcă să vă păcălească spunându-vă că ați câștigat la loterie, pretinzând că sunt o organizație de caritate în căutare de donații, sau cerându-vă ajutorul pentru a transfera milioane de dolari. Dacă răspundeți la oricare dintre acestea, vor spune mai întâi că au nevoie de plăți pentru serviciile pe care le oferă sau vor solicita accesul la contul bancar, lăsându-vă astfel fără niciun ban.




*Cea mai bună apărare este logica. Dacă un email sau un mesaj este ciudat, suspicios sau prea frumos ca să fie adevărat, ar putea să fie un atac de phishing.*

## Cum vă protejați

În aproape toate cazurile, deschiderea și citirea unui email sau a unui mesaj sunt în regulă. Pentru ca un atac de phishing să reușească, răufăcătorii trebuie să vă păcălească și să vă convingă să faceți ceva. Din fericire, există unele indicii care arată că mesajul este un atac; iată-le pe cele mai des întâlnite:

- Email-ul creează un sentiment de urgență, cerând „acțiune imediată“ înainte de a se întâmpla ceva rău, cum ar fi închiderea contului dumneavoastră. Atacatorul dorește să vă grăbească astfel încât să faceți greșeli, fără să vă gândiți prea mult.
- Primiți un email cu un fișier atașat pe care nu îl așteptați sau email-ul vă îndeamnă să deschideți fișierul. Printre exemple se numără un email care spune că are atașat un fișier cu detalii ale unor concedieri neanunțate, informații referitoare la salariile angajaților sau scrisori din partea fiscului care vă anunță că sunteți executat silit.
- În loc să vă folosească numele, mesajul folosește o formulă de salut generică, de genul „Stimate Client“. Majoritatea prietenilor și companiilor care vă contactează vă cunosc numele.
- Email-ul vă solicită informații ultra-sensibile cum ar fi numărul cardului de credit sau parola.
- Email-ul pretinde a proveni de la o organizație oficială dar conține greșeli de gramatică sau de ortografie sau folosește adrese personale precum @gmail.com, @yahoo.com, or @hotmail.com.

## Despre Phishing

- Adresa web arată ciudat sau neoficial. Un pont ar fi să țineți săgeata cursorului peste adresa respectivă până când apare o notificare ce vă arată unde exact vă va direcționa. Dacă adresa din email nu se potrivește destinației din notificare, nu dați clic. Pe telefoanele mobile dacă țineți degetul pe adresă, vă va apărea aceeași notificare. Un pas și mai sigur este să copiați URL-ul din email în programul de navigare online sau să scrieți manual adresa.
- Primiți un mesaj de la cineva cunoscut, dar tonul sau frazarea parcă nu sună așa cum ar trebui. Dacă aveți suspiciuni, sunați expeditorul pentru a verifica dacă într-adevăr v-a trimis un mesaj. Pentru un atacator cibernetic este ușor să creeze un email care pare a fi de la un prieten sau de la un coleg de serviciu.

Dacă credeți că un email sau un mesaj este un atac de phishing, pur și simplu ștergeți-l. Până la urmă logica este cea mai bună apărare.

## Aflați mai multe

Abonați-vă la buletinul informativ lunar OUCH!, accesați arhiva și aflați mai multe despre programele de instruire asupra domeniului securității informației vizitând pagina web SANS http://www.securingthehuman.org

## Versiunea în limba română

Grupul Cegeka este un furnizor privat de servicii IT&C fondat în 1992. Având sediul central în Belgia, Cegeka este prezentă în Austria, Republica Cehă, Franța, Germania, Italia, Luxemburg, Olanda, România și Republica Slovacă. Compania furnizează servicii clienților din întreaga Europă: soluții Cloud pentru companii, servicii de securitate, dezvoltare de aplicații folosind tehnicile Agile, mentorat în metodologii Agile și externalizarea infrastructurii IT&C. Cegeka are 3200 de angajați și a realizat o cifră de afaceri combinată de 330 milioane euro în 2013. Pentru mai multe informații vizitați www.cegeka.com.

## Resurse

| | |
|---|---|
| Ingineria Socială: | https://www.securingthehuman.org/ouch/2014#november2014 |
| Cinci elemente de bază pentru păstrarea securității: | https://www.securingthehuman.org/ouch/2014#october2014 |
| Am fost victima unui atac; acum ce fac?: | https://www.securingthehuman.org/ouch/2014#may2014 |
| OnGuard Online: | https://www.onguardonline.gov/phishing |
| Recomandarea zilei: | https://www.sans.org/tip_of_the_day.php |



Echipa editorială: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducere: Cosmin Hănulescu

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus