Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

Opriți atacurile Phishing

Generalități

Email-ul și serviciile de mesagerie instantanee (cum sunt Skype, Twitter sau Snapchat) sunt unele dintre principalele mijloace de comunicare pe care le folosim. Nu numai că folosim cotidian aceste tehnologii în activitatea noastră profesională, dar și pentru a păstra legătura cu prietenii și familia. Cum atât de mulți oameni din întreaga lume depind de aceste tehnologii, ele au devenit una dintre principalele căi de atac folosite de răufăcători în spațiul cibernetic, o metodă de atac fiind cel de phishing. Aflați așadar ce este atacul de phishing și cum puteți detecta astfel de atacuri, indiferent dacă sunteți la serviciu sau acasă.

Ce este phishing-ul

Se numește phishing un tip de atac cibernetic ce folosește email-ul sau serviciile de mesagerie electronică pentru a vă păcăli ca să faceți anumite lucruri pe care n-ar trebui să le faceți, cum ar fi să accesați adrese online cu conținut fraudulos, să dezvăluiți parola personală sau să deschideți un email ce conține programe malware. Răufăcătorii depun eforturi mari să facă aceste mesaje convingătoare și să declanșeze factori emoționali cum ar fi curiozitatea sau sentimentul de urgență. Ei le pot face să pară că v-au parvenit de la cineva cunoscut, cum ar fi un prieten sau o companie de încredere pe care o folosiți frecvent. Sau poate că și adaugă logoul băncii dumneavoastră și falsifică adresa email ca să apară legitimă. Atacatorii trimit apoi aceste mesaje către milioane de oameni. Ei nu știu cine va mușca momeala, dar știu că vor avea mai multe victime pe măsură ce trimit mai multe mesaje.

Protejați-vă

Aproape în toate cazurile, deschiderea și citirea unui email este în regulă. Pentru ca un atac de phishing să funcționeze, răufăcătorii trebuie să vă păcălească să faceți ceva anume. Din fericire există indicii potrivit cărora un mesaj este un atac; iată-le pe cele mai frecvent întâlnite:

- Un puternic sentiment de urgență, ce solicită „acțiune imediată” înainte ca ceva rău să se întâmple, cum ar fi amenințarea închiderii unui cont sau riscul intrării la închisoare. Atacatorii vor să vă forțeze să faceți o greșeală.
- Presiunea de a ocoli sau a ignora politicile și procedurile de la serviciu.
- Inducerea unui sentiment puternic de curiozitate sau acel „prea bun ca să fie adevărat” (nu, n-ați câștigat la loterie...)
- O formulă de salut generică, gen „Dragă client”. Multe companii sau prieteni ce vă contactează vă știu numele deja.

- Solicitarea de informații strict confidențiale, cum ar fi numărul cardului de credit sau parola sau orice alt tip de informații pe care un expeditor legitim ar trebui să le știe deja.
- Mesajul pretinde că vine de la o organizație oficială, dar este scris cu greșeli gramaticale sau de ortografie ori folosește o adresă personală de email, cum ar fi cele de la gmail.com.
- Mesajul vine de la o adresă oficială (cum ar fi cea a superiorului ierarhic) dar are o adresă de răspuns — Reply-To — ce face referire la o adresă de email personală, privată.
- Primiți un mesaj de la cineva cunoscut, dar tonul și vocabularul folosite nu se potrivesc persoanei respective. Dacă aveți suspiciuni, sunați expeditorul pentru a verifica dacă într-adevăr v-a scris. Este ușor pentru escroci să creeze un mesaj care pare că este trimis de către un prieten sau coleg de serviciu.

În cele din urmă, simțul realității este cea mai bună defensivă. Dacă un mesaj sau email pare ciudat, suspect sau prea bun ca să fie adevărat, ar putea fi un atac de phishing.

Versiunea în limba română

Cegeka este un furnizor independent de servicii IT&C ce își ajută clienții din întreaga Europă în transformarea lor digitală, dezvoltarea de aplicații folosind metodologiile Agile, soluții de încredere de tip Cloud și managementul serviciilor 24/7. Cegeka este prezentă în Austria, Belgia, Republica Cehă, Franța, Germania, Italia, Olanda, Polonia, România și Republica Slovacă, având 3600 de angajați. Cegeka a realizat o cifră de afaceri de 368 milioane de euro în 2015. Pentru mai multe informații vizitați www.cegeka.com.

Editor invitat

Tonia Dudley a realizat și condus programe de sensibilizare cu privire la securitatea informației din 2011, ce includ și un curs premiat despre atacurile de phishing. O puteți urmări la www.linkedin.com/in/toniadudley.

Resurse suplimentare

Ingineria socială:	https://www.sans.org/u/Cb1
Ajutându-i pe ceilalți să se protejeze:	https://www.sans.org/u/Cb6
Recomandări și precauții în utilizarea email-ului:	https://www.sans.org/u/Cbg
Escrocheria CEO:	https://www.sans.org/u/Cbl
Traducerile și arhiva buletinului informativ OUCH!:	https://www.sans.org/u/Cbq

licență