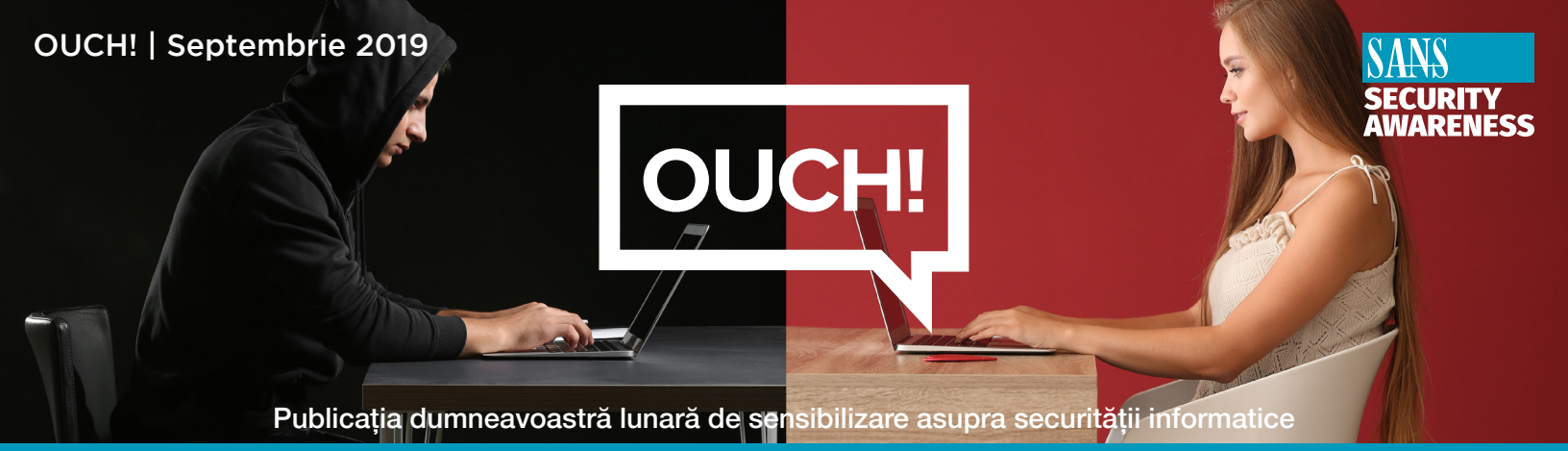
OUCH! | Septembrie 2019



Publicația dumneavoastră lunară de sensibilizare asupra securității informatice

Escrocherii prin mediile de socializare

Prezentare generală

Mulți dintre noi au primit e-mailuri de tip phishing, fie la serviciu, fie acasă. Acestea sunt e-mail-uri care par legitime, cum ar fi de la bancă, de la manager sau de la magazinul online preferat. Totuși, acestea sunt de fapt atacuri, care încearcă să vă determine să faceți o acțiune pe care nu ar trebui să o faceți, cum ar fi deschiderea unui atașament infectat, comunicarea parolei sau transferuri de bani. Probleme este că pe măsură ce noi devenim mai experimentați în depistarea și oprirea acestor atacuri, infractorii cibernetici descoperă noi modalități de a ne contacta și a ne înșela.

Încercările de escrocherie sau înșelătorie pot avea loc pe toate platformele de comunicare pe care le utilizați, de la Skype, WhatsApp și Slack la Twitter, Facebook, Snapchat, Instagram sau chiar aplicații de jocuri. Comunicarea prin aceste platforme sau canale pare mai informală sau mai de încredere, motiv pentru care atacatorii le folosesc pentru a-i înșela pe alții. În plus, cu tehnologiile de astăzi, este mult mai ușor pentru orice atacator de oriunde din lume să pretindă a fi orice sau oricine dorește. Este important să țineți cont că nu toate comunicările sunt ceea ce par, așa cum nici oamenii nu sunt întotdeauna cine par a fi.

Puncte cheie

Iată cele mai comune indicii ca mesajul pe care l-ați primit sau postarea pe care ați citit-o poate fi un atac.

Urgență: Un mesaj care denotă urgență si care necesită o „acțiune imediată” înainte de a se întâmpla ceva rău, cum ar fi amenințarea cu închiderea unui cont sau trimiterea la închisoare. Atacatorul vrea să vă grăbească și astfel să faceți o greșeală.

Presiune: Presionându-vă să ocoliți sau să ignorați politicile sau procedurile de la locul de muncă.

Curiozitate: Un puternic sentiment de curiozitate sau ceva care pare prea bun pentru a fi adevărat. Nu, nu ați câștigat la loterie.

Sensibil: O solicitare de informații extrem de sensibile, cum ar fi numărul cardului de credit, parola, sau orice altă informație pe care nu doriți să o împărtășiți.

Mesaj oficial: Mesajul pare a proveni de la o organizație oficială, dar are greșeli de gramatică sau ortografie. Majoritatea organizațiilor guvernamentale nu folosesc mediile de socializare pentru a comunica oficial cu dvs. Dacă nu sunteți sigur de legitimitatea mesajului, sunați respectiva organizație, dar utilizați un număr de telefon oficial, cum ar fi unul de pe site-ul lor web.

Personificare: Primiți un mesaj de la un prieten sau coleg de muncă, dar tonul sau formularea nu sună deloc familiar. Dacă aveți îndoieli, sunați expeditorul pentru a verifica că el a trimis mesajul. Este ușor pentru un atacator cibernetic să creeze mesaje care par a fi de la cineva cunoscut. În unele cazuri, aceștia pot sparge contul unui prieten, apoi vă contactează în numele lui. Fiți atenți mai ales la mesajele text, Twitter și alte formate de mesaje scurte, unde este mai dificil să vă dați seama de personalitatea expeditorului.

Dvs. sunteți cea mai bună apărare împotriva înșelătoriilor, escrocheriilor și atacurilor de acest gen. Dacă o postare sau un mesaj pare ciudat sau suspect, pur și simplu ignorați-l sau ștergeți-l, sau dacă este de la cineva cunoscut, sunați persoana respectivă pentru a confirma dacă a trimis într-adevăr acel mesaj.

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. Alflați mai multe la: https://www.ubisoft.com/en-us/.

Editor invitat

Dr. Jessica Barker *(@drjessicabarker) este un lider în studiul laturii umane a securității cibernetice. Este co-CEO la Cygenta, unde își urmează pasiunea de a influența în mod pozitiv sensibilizarea, comportamentele și cultura cibernetica din întreaga lume. Ea este președinta ClubCISO și o conferențiară populară.*

Resurse

Ingineria socială:	https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201701_ro.pdf
Atacurile și escrocheriile telefonice:	https://www.sans.org/sites/default/files/2018-07/201807-OUCH-July-Romanian.pdf
Opriți atacurile Phishing:	https://www.sans.org/sites/default/files/2018-04/201804-OUCH-April-Romanian_0.pdf
Escrocherii personalizate:	https://www.sans.org/sites/default/files/2019-02/201902-OUCH-February-Romanian.pdf