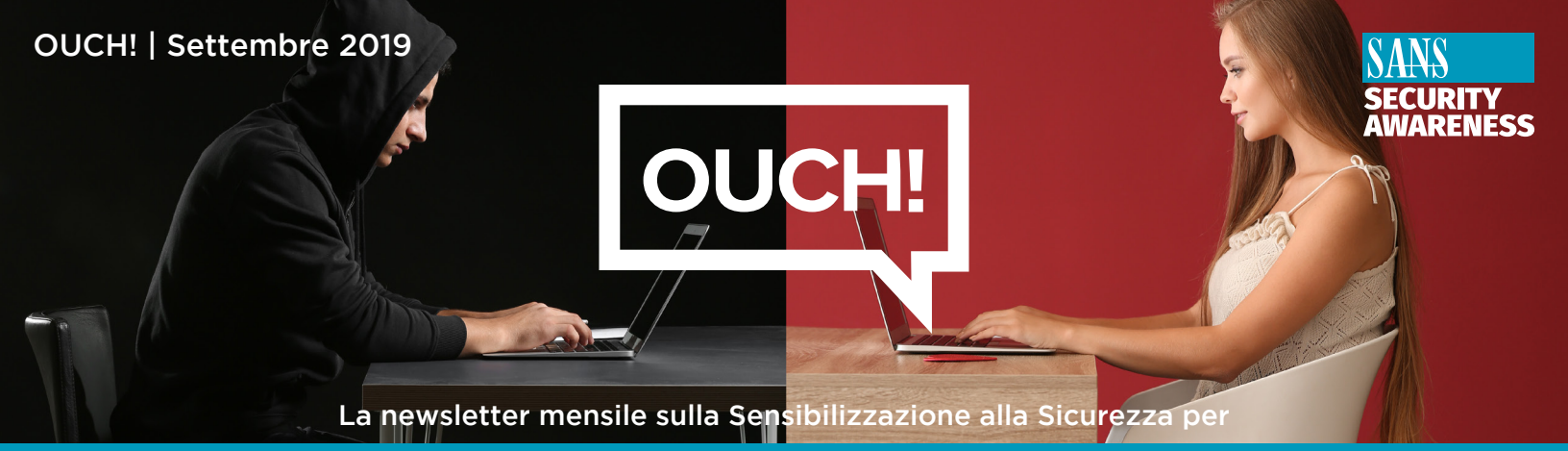
OUCH! | Settembre 2019



La newsletter mensile sulla Sensibilizzazione alla Sicurezza per

Truffe sui Social Media

In sintesi

A molti di voi sarà capitato di ricevere degli attacchi di phishing tramite email, sia a casa che al lavoro. Si tratta di messaggi che sembrano autentici, come quelli che potrebbe inviarti la tua banca, il tuo capo o il tuo negozio online preferito. In realtà si tratta di attacchi pensati per spingerti a compiere azioni che dovresti evitare, come aprire un allegato infetto, condividere una password o inviare del denaro. Purtroppo, più diventiamo abili nel riconoscere le minacce, e più i criminali inventeranno nuovi modi per contattare e ingannare le persone.

I tentativi di inganno possono utilizzare quasi ogni forma di comunicazione che usi, da Skype, WhatsApp e Slack, fino a Twitter, Facebook, Snapchat, Instagram e anche giochi online. La comunicazione attraverso questi canali può sembrare più informale o affidabile, ed è proprio per questo che i criminali informatici li usano per ingannare le loro vittime. Inoltre, grazie alle tecnologie odierne, è diventato molto più facile per i criminali fingere di essere qualunque altra persona o organizzazione. E' importante ricordare che i messaggi che riceviamo non sempre sono quello che sembrano, e che le persone che ci contattano, non sempre sono quello che vorrebbero farci credere.

Indizi chiave

Questi sono gli indizi più comuni per capire se il messaggio che hai ricevuto o il post che hai letto sono parte di un attacco.

Urgenza: Un messaggio che crea un senso di urgenza, chiedendoti di agire immediatamente per evitare problemi come la chiusura di un tuo account o una condanna penale. Il criminale vuole spingerti a commettere un errore.

Pressione: Cercare di spingerti ad ignorare le regole o le procedure che devi seguire al lavoro.

Curiosità: Creare un forte senso di curiosità o offrire qualcosa di troppo bello per essere vero. No, non hai vinto la lotteria.

Dati sensibili: Una richiesta di dati altamente sensibili, come il numero della tua carta di credito o una password, o qualsiasi altro dato che non andrebbe condiviso.

Messaggi ufficiali: Il messaggio sembra provenire da un'organizzazione legittima, ma presenta errori di grammatica e ortografia. La maggior parte delle organizzazioni governative non userà i social media per contattarti. Se non sei sicuro che si tratti di un messaggio autentico, chiama l'organizzazione usando il loro numero di telefono, come quello pubblicato sul loro sito web.

Furto d'identità: Ricevi un messaggio da un amico o collega di lavoro, ma il tono usato non ti sembra familiare. Se hai dei sospetti, chiama la persona al telefono per verificare che sia stata veramente lei ad inviare il messaggio. E' facile per un criminale informatico creare un messaggio che sembra provenire da qualcuno che conosci. In alcuni casi potrebbero ottenere il controllo di un account del tuo amico, per poi contattarti e fingere di essere quell'amico. Fai soprattutto attenzione ai messaggi di testo, Twitter e altri formati di comunicazione sintetici, dove è più difficile riconoscere la personalità di chi l'ha inviato.

Tu sei la migliore difesa contro inganni, truffe e altri attacchi di questo genere. Se un post o un messaggio sembra strano o sospetto, cancellalo o ignoralo, oppure, nel caso sia inviato da una persona che conosci, chiamala al telefono per avere conferma.

Guest Editor

Dr Jessica Barker *(@drjessicabarker) è un'esperta sul lato umano della sicurezza informatica. E' vice-amministratrice delegata di Cygenta, dove porta avanti il suo progetto per influenzare positivamente la consapevolezza e la cultura della sicurezza informatica nel mondo. E' la presidente del ClubCISO ed una relatrice pubblica molto apprezzata.*

Risorse

Ingegneria sociale:	https://www.sans.org/u/Uz6
Truffe al telefono:	https://www.sans.org/u/Uzb
Difendersi dal Phishing:	https://www.sans.org/u/Uzg
Attacchi personalizzati:	https://www.sans.org/u/Uzl