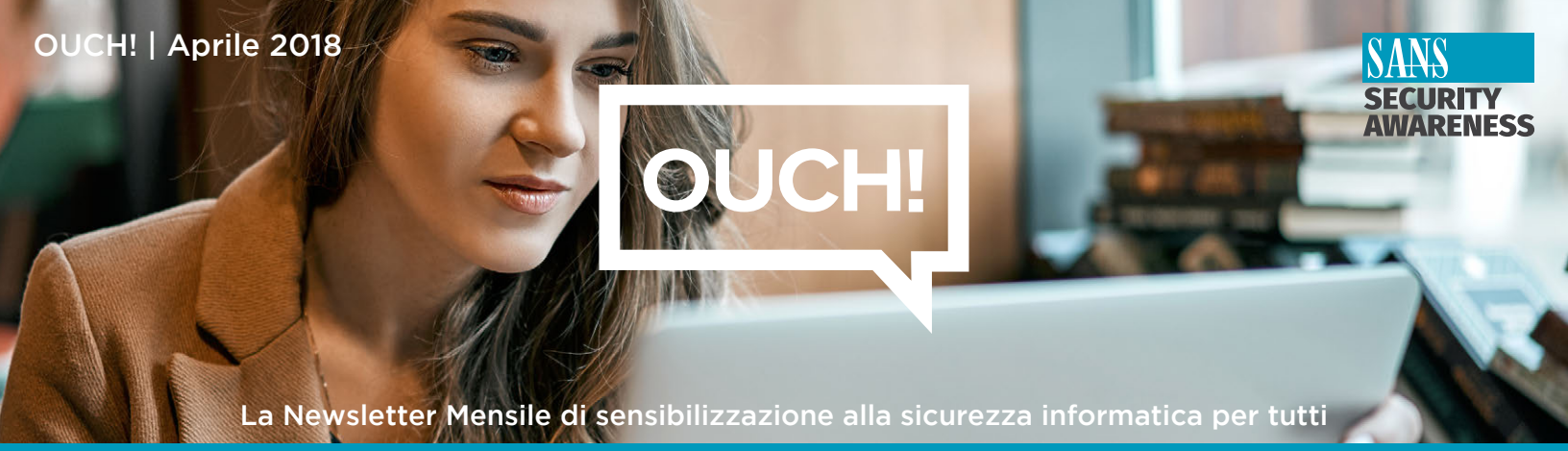

La Newsletter Mensile di sensibilizzazione alla sicurezza informatica per tutti

Basta con questi Phish !

Introduzione

I servizi di posta elettronica e di messaggistica (come Skype, Twitter o Snapchat) sono uno dei principali modi con i quali comunichiamo. Queste tecnologie non le usiamo ogni giorno solo per lavoro ma anche per rimanere in contatto con amici e familiari. Dal momento che molte persone in tutto il mondo utilizzano queste tecnologie, esse sono diventate uno dei principali obiettivi degli hacker, usando un metodo di attacco chiamato *phishing*. In questo articolo ti faremo scoprire cos'è il phishing e come puoi individuare e bloccare questi tipi di attacchi, indipendentemente dal fatto che tu sia al lavoro o a casa.

Cos'è il Phishing

Il *phishing* è un tipo di attacco che utilizza l'e-mail o un servizio di messaggistica per ingannare l'utente nel compiere un'azione che non dovrebbe invece effettuare, come ad esempio fare click su un link malevolo (o pericoloso), condividere la password o aprire un allegato di posta elettronica che contiene un virus (file infetto). Gli aggressori lavorano duramente per rendere questi messaggi convincenti e sfruttano aspetti emotivi delle persone, come ad esempio l'urgenza o la curiosità. Gli hacker sono abili nel far apparire questi messaggi come se provenissero da qualcuno o qualcosa che conosci, come un amico o una società fidata che usi frequentemente, magari aggiungendo anche i loghi della tua banca o falsificando l'indirizzo email in modo che il messaggio appaia più legittimo e sicuro. Gli aggressori, quindi, inviano questi messaggi a milioni di persone. Non sanno chi cadrà nella trappola, tutto quello che sanno è che più messaggi mandano, maggiore è la probabilità che più persone cadranno vittime.

Come proteggersi

In quasi tutti i casi, l'apertura e la lettura di una e-mail o di un messaggio non comporta conseguenze. Perché un attacco di phishing abbia successo, gli hacker devono convincerti a fare qualcosa. Fortunatamente ci sono alcuni indizi che rilevanoche dietro ad un messaggio si celi in realtà un attacco informatico; di seguito alcuni di questi:

- Un forte senso di urgenza, che richiede "un'azione immediata" prima che succeda qualcosa di dannoso o grave ti possa accadere, come minacciare di chiudere un account o addirittura mandarti in prigione. L'hacker vuole metterti fretta per farti commettere un errore.
- Urgenza per aggirare o ignorare le politiche o le procedure aziendali.
- Creare una grande curiosità oppure una reazione "troppo bello per essere vero" (no, non hai vinto la lotteria!).

- Un saluto generico come “Gentile cliente”. La maggior parte delle aziende o degli amici che ti contattano conoscono il tuo nome.
- Richiesta di informazioni altamente sensibili, come il numero di carta di credito o la password o qualsiasi altra informazione che il legittimo mittente dovrebbe già conoscere.
- Il messaggio dice di provenire da un’organizzazione ufficiale ma ha una grammatica o un’ortografia scadente, oppure utilizza un indirizzo e-mail personale come ad esempio @gmail.com.
- Il messaggio proviene da un’e-mail ufficiale (come ad esempio il tuo capo) ma ha un indirizzo di risposta diverso, indirizzato cioè all’indirizzo di posta elettronica di qualcun altro.
- Ricevi un messaggio da qualcuno che conosci ma dal tono o dal contenuto non sembra proprio essere lui o lei. Nel dubbio, chiama il mittente per verificare che sia stato effettivamente lui ad inviartelo. Ricorda: per un cyber-attacker è facile creare un messaggio che sembra provenire da un amico o da un collega.

In definitiva, il buon senso è la tua migliore difesa. Se una e-mail o un messaggio sembra strano, sospetto oppure troppo bello per essere vero, potrebbe trattarsi di un attacco di phishing.

Versione Italiana

Italtel è una società multinazionale che progetta e realizza soluzioni e servizi di Information & Communication Technology basati su prodotti propri e di partner. Offre un ricco catalogo di servizi professionali di ingegneria, di servizi gestiti e soluzioni di Cybersecurity, collaboration, IoT, digitalizzazione delle reti e servizi di comunicazione.
Per maggiori informazioni www.italtel.com e seguici su Twitter (@Italtel)

L’autrice di questo numero

Tonia Dudley ha sviluppato e gestito programmi di sensibilizzazione sulla sicurezza dal 2011, tra i quali la creazione di un premiato programma di formazione sul phishing.

Puoi maggiori informazioni Tonia Dudley: www.linkedin.com/in/toniadudley.

Risorse

Social Engineering:	https://www.sans.org/u/Cb1
Aiutare gli altri a proteggersi:	https://www.sans.org/u/Cb6
Email: cosa fare e cosa non fare:	https://www.sans.org/u/Cbg
Frodi CEO:	https://www.sans.org/u/Cbl
OUCH! Traduzioni e archivi:	https://www.sans.org/u/Cbq

License