Newsletter mensile di suggerimenti sulla sicurezza informatica

OUCH!

IN QUESTO NUMERO

Social Network in sicurezza

L'AUTORE DI QUESTO NUMERO

A questo numero di OUCH! ha collaborato Ted Demopoulos. Ted è un consulente specializzato in sicurezza nonché istruttore SANS da più di 10 anni. Per maggiori informazioni consultate il sito http://demop.com.

INTRODUZIONE

I Social Network, come Facebook, Twitter, Google+, Pinterest e LinkedIn, sono strumenti potenti e spesso divertenti che ci permettono di incontrare, interagire e condividere contenuti con persone in tutto il mondo. A queste possibilità si affiancano però anche dei rischi, non solo per chi li utilizza direttamente, ma anche per la sua famiglia, i suoi amici e l'azienda per la quale lavora. In questa newsletter illustreremo quali sono questi pericoli e come utilizzare i Social Network in modo più sicuro.

PRIVACY

Una preoccupazione piuttosto comune nell'uso dei Social Network è la protezione della privacy delle proprie informazioni personali e dei dati sensibili di altri. Una loro violazione potrebbe portare a effetti spiacevoli e indesiderati tra i più vari, tra cui:

- **carriera in pericolo:** molte aziende effettuano ricerche sui siti di Social Network sia durante i controlli pre-assunzione sia come attività periodica di monitoraggio del personale. Una serie di post imbarazzanti, non importa di quanto tempo fa, potrebbe contribuire a impedire una possibile assunzione o promozione. Le opzioni di privacy che avete scelto potrebbero non proteggervi in modo adeguato, dal momento che un'azienda vi potrebbe chiedere di seguire le sue pagine di permettervi di inviare il vostro curriculum;
- **attacchi personali:** molti criminali informatici raccolgono informazioni personali allo scopo di utilizzarle contro le proprie vittime: potrebbero, ad esempio, utilizzare i dati recuperati per indovinare la risposta alla "domanda segreta" per resettare le password online, oppure creare campagne di mail fasulle (chiamate spear phishing), o ancora compilare moduli col vostro nome. Questi attacchi possono spesso avere anche risvolti nel mondo reale, quando sono volti a identificare dove lavorate o il luogo in cui vivete;
- **danni alla vostra azienda:** le informazioni sensibili pubblicate sulla vostra azienda possono far gola sia a criminali informatici sia alla concorrenza. I vostri post potrebbero inoltre causare danni reputazionali al vostro datore di lavoro. Verificate le policy di sicurezza aziendali prima di pubblicare contenuti che la riguardino.

Social Network in sicurezza

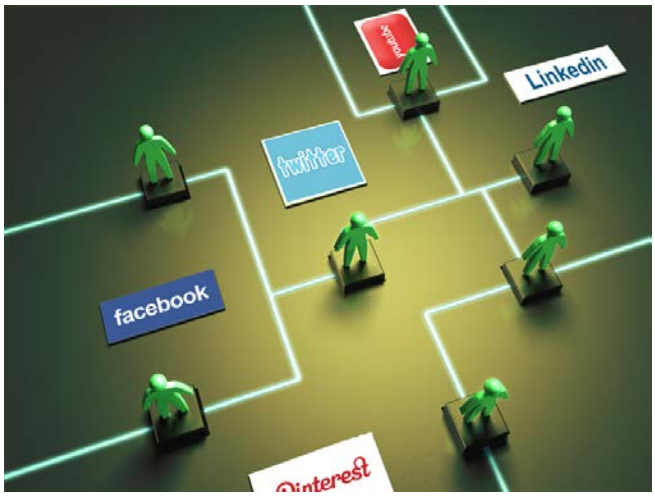
La miglior forma di protezione sta nel limitare le informazioni pubblicate. Di certo le opzioni di privacy offrono qualche sicurezza, ma tenete presente che possono essere spesso poco chiare, cambiare frequentemente senza comunicazione e ingenerare, quindi, confusione: ciò che credete sia privato potrebbe diventare pubblico per svariate ragioni. Inoltre, la privacy dei vostri dati è tanto sicura quanto le persone con cui li condividete: maggiore è il numero di contatti a cui trasmettete informazioni, maggiore sarà la possibilità che ciò che pubblicate diventi di dominio pubblico. Infine, il miglior modo di proteggere la privacy è di seguire questa semplice regola: se non volete che vostra madre o il vostro capo vedano i vostri post, non pubblicateli.

Cercate inoltre di monitorare quali informazioni vengono postate su di voi dai vostri contatti: si potrebbero creare situazioni imbarazzanti o persino pericolose nel caso vengano pubblicate informazioni o foto che vi riguardano e che non vorreste vengano divulgate. Assicuratevi che i vostri amici comprendano quello che possono postare su di voi e ciò che, invece, è meglio non pubblicare. Nel caso pubblichino qualcosa che non vi aggrada, chiedeteglli di rimuoverlo. Al contempo, rispettate la privacy degli altri quando pubblicate qualsiasi tipo di contenuto.

SICUREZZA

Oltre alle preoccupazioni riguardanti la privacy, i siti di Social Network possono essere utilizzati da criminali informatici per attaccare voi e i dispositivi che utilizzate, come il vostro computer o il vostro smartphone. Ecco alcuni suggerimenti per proteggervi.

- **Login:** proteggete gli account dei Social Network con password forti, non condividetele con nessuno e non utilizzatele per altri siti. Alcuni Social Network supportano l'autenticazione forte, come ad esempio la verifica in due passi: attivatela, laddove sia disponibile.
- **Crittografia:** molti Social Network vi permettono di utilizzare la crittografia (HTTPS) per rendere sicura la connessione al sito web. Alcuni di essi, come Twitter e Google+, la attivano di default, mentre altri richiedono che sia abilitata manualmente nelle configurazioni dell'account. Laddove possibile, utilizzate l'HTTPS.
- **Email**: trattate con cautela le email che sembrano provenire da un Social Network, in quanto potrebbe trattarsi facilmente di attacchi inviati da criminali informatici. Il modo più sicuro per rispondere a un messaggio del genere è di collegarsi al sito web direttamente e controllare da lì i messaggi e le notifiche;



I Social Network sono strumenti interessanti e divertenti, ma fate attenzione a ciò che pubblicate e verificate ciò che pubblicano i vostri contatti.

Social Network in sicurezza

- **Link pericolosi**: purtroppo i Social Network vengono spesso utilizzati per truffe di vario genere. I criminali informatici pubblicano link maligni che, se selezionati, conducono a siti web che tenteranno di infettare il vostro computer. Un messaggio che apparentemente appare provenire da un vostro amico, potrebbe invece essere stato inviato da qualcun altro che ha compromesso il suo account. Se un famigliare o un amico pubblica un messaggio strano che non potete verificare (ad esempio, affermando di essere stato rapinato e chiedendovi del denaro), chiamatelo per avere conferma che l'abbia effettivamente inviato lui.
- **App**: alcuni Social Network vi permettono di installare applicazioni di terze parti, come giochi e utilità. Sappiate che queste applicazioni vengono sottoposte a un controllo di qualità non sempre efficace e possono avere la possibilità di ottenere un accesso completo al vostro account e a informazioni private. Installate solo le app di cui avete realmente bisogno e che provengono da siti ben conosciuti e di cui avete fiducia. Rimuovetele una volta che non ne fate più utilizzo.

I Social Network costituiscono un modo interessante per comunicare con il mondo. Se seguite i suggerimenti illustrati in questa newsletter, sarete in grado di utilizzarli nel modo più sicuro. Per ulteriori informazioni sull'utilizzo dei Social Network o per riferire attività non autorizzate, consultate le pagine dedicate alla sicurezza del servizi che state utilizzando.

RISORSE

Alcuni dei link presenti in questa newsletter sono stati accorciati per migliorarne la leggibilità utilizzando il servizio TinyURL.

Undici suggerimenti per la sicurezza nei social network:
http://tinyurl.com/4yzvr6s

La sicurezza in Facebook:
https://www.facebook.com/safety

Le configurazioni di sicurezza di Facebook:
https://www.facebook.com/settings?tab=security

Linkedin: sicurezza e privacy:
http://tinyurl.com/c9vpqf5

Google+: Come preservare la sicurezza dell'account:
http://tinyurl.com/bod35x3

PER SAPERNE DI PIÙ

Abbonatevi a OUCH!, la newsletter mensile sulla sicurezza informatica, consultate i suoi archivi e approfondite le soluzioni di sicurezza di SANS visitandoci presso http://www.securingthehuman.org.

VERSIONE IN ITALIANO

La versione in italiano è curata da Advanction S.A., un'azienda impegnata nella Sicurezza, nel Risk Management Operativo e nella Security Awareness. Seguila su www.advanction.com e su Twitter (@advanction).

Redazione: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Versione in italiano curata da Advanction S.A.: Stefano Bonacina, Silvestro Maestri, Giorgio Ferrari