SANS SECURING THE HUMAN ADVANCTION

OUCH! | Luglio 2015

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

I social network

Introduzione

I siti dei social network come Facebook, Twitter, Instagram e LinkedIn costituiscono una risorsa importante che ci permette di incontrare, interagire e condividere con persone in tutto il mondo. A queste interessanti caratteristiche si accompagnano però anche dei rischi, non solo per voi ma anche per la vostra famiglia, gli amici e la vostra azienda. In questa newsletter spiegheremo quali sono questi pericoli e come utilizzare questi siti in modo sicuro.

L'autore di questo numero

Tanya Baccam è consulente in tematiche di sicurezza da molto tempo. Per più di un decennio è stata autrice e istruttrice di corsi SANS tra cui SEC502, SEC542, SEC401, MGT414, AUD507 e molti altri. Seguitela su Twitter: **@tbaccam**.

Privacy

Una preoccupazione molto comune relativa ai social media riguarda la protezione delle informazioni personali. Tra i potenziali pericoli troviamo:

- **Effetti negativi sul futuro**. Alcune aziende svolgono ricerche nei social network come parte delle attività di background check, quella serie di controlli sul personale attuale o in corso di assunzione. Foto o post imbarazzanti, non importa anche se vecchi, possono ostacolare sia un'assunzione sia una promozione. Anche molte università effettuano controlli simili sugli studenti che richiedono l'iscrizione. Le opzioni di privacy potrebbero non essere sufficienti a proteggervi, perché l'azienda o l'università potrebbe chiedervi di seguire le sue pagine, attività che potrebbe portare a condividere le vostre informazioni.
- **Attacchi contro di voi**. Criminali informatici potrebbero analizzare i vostri post e usarli per ottenere un accesso alle vostre informazioni o a quelle della vostra azienda. Potrebbero, ad esempio, utilizzare le informazioni che condividete per indovinare le risposte alle vostre domande segrete allo scopo di resettare la vostra password online, creare email mirate contro di voi (spearphishing) o chiamare qualche vostro collega spacciandosi per voi. Questi attacchi potrebbero avere ripercussioni anche nel mondo reale, portando, ad esempio, a identificare dove vivete o lavorate.
- **Danneggiare accidentalmente il vostro datore di lavoro**: I criminali o concorrenti possono utilizzare le informazioni riservate che pubblicate sulla vostra organizzazione contro il vostro datore di lavoro. Inoltre, i vostri messaggi possono potenzialmente causare danni alla reputazione per l'organizzazione. Assicuratevi di controllare le politiche dell'organizzazione prima di pubblicare informazioni sul vostro lavoro, in aggiunta alcuni dei tuoi post di social media possono essere monitorati.

I social network

Il miglior modo per proteggersi è limitare le informazioni che pubblicate. Le opzioni di privacy possono offrire un certo grado di protezione, ma sono spesso confuse e cambiare di frequente senza che ve ne rendiate conto. Quello che pensavate fosse privato potrebbe, all'improvviso e per varie ragioni, diventare pubblico. Considerate che la privacy dei vostri post è tanto sicura quanto lo sono le persone con cui li condividete: più amici o contatti li condivideranno a loro volta, più probabilmente questa informazioni diventerà pubblica. Dovete presumere che qualsiasi cosa pubblichiate potrebbe diventare pubblica e rimanere così presente in modo permanente su Internet.

Fate infine attenzione a ciò che i vostri amici pubblicano sul vostro conto. Se viene pubblicato qualche post su cui non siete d'accordo, comunicate loro di rimuoverlo. Se rifiutano o se vi ignorano, contattate il socia il network e chiedetegli di rimuovere il contenuto indesiderato. Al contempo, siate rispettosi quando pubblicate qualcosa sul conto di altri.



I social network sono strumenti interessanti e potenti, ma fate attenzione a ciò che condividete e con chi lo condividete.

Sicurezza

Oltre agli aspetti relativi alla privacy, ecco alcuni suggerimenti per proteggere i vostri account sui social network.

- **Login**. Proteggete ogni vostro account con una password unica e forte e non condividetela con nessuno. Molti social network supportano l'autenticazione forte, come la verifica in due passaggi. Abilitate sempre questi metodi quando sono disponibili. Non utilizzate gli account dei social network per collegarvi ad altri siti, poiché se venissero compromessi, anche tutti gli altri account lo sarebbero.
- **Configurazioni di Privacy**. Se avete impostato le configurazioni di privacy, assicuratevi di verificarle e testarle con regolarità. I social network offrono spesso la possibilità di configurare e modificare le proprie impostazioni. Inoltre, molte app e servizi permettono di assegnare ai contenuti pubblicati un tag (etichetta) relativo alla locazione geografica . Verificate regolarmente le vostre impostazioni, nel caso vogliate mantenere questa informazione privata.
- **Crittografia**. I social network implementano la crittografia mediante HTTPS per rendere sicuri i vostri collegamenti con i loro siti. Alcuni di essi, come Twitter e Google+, attivano questa funzione di default, mentre altri richiedono l'impostazione manuale. Verificate le impostazioni dei social network che usate e abilitate l'HTTPS per default, quando possibile.
- **Email**. Fate attenzione alle email provenienti da siti di social network, poiché potrebbe facilmente trattarsi di attacchi inviati da criminali informatici. Il modo migliore per rispondere a questi messaggi è di collegarsi direttamente al sito del social network, meglio se da un segnalibro già salvato in precedenza, leggere il messaggio e rispondere dal sito stesso.

I social network

- **Link pericolosi/truffe**. Fate attenzione ai link sospetti o alle potenziali truffe pubblicate sui social network, poiché vengono utilizzati per diffondere attacchi. Solo perché un messaggio è pubblicato da un amico non significa che provenga veramente da lui, poiché il suo account potrebbe essere stato compromesso. Se un membro della vostra famiglia ha pubblicato un messaggio strano che non potete verificare (comunicandovi, ad esempio, che è stato derubato e voi dovete inviargli del denaro) contattatelo al telefono o in altro modo per verificare che il messaggio provenga veramente da lui.
- **App**. Molti siti di social media offrono app mobili per l'accesso online. Scaricate queste app solo da siti affidabili e proteggete il vostro smartphone con una password forte. Se dovesse andare smarrito mentre è sbloccato, chiunque potrebbe accedere i vostri social network e pubblicare sotto la vostra identità.

I social network sono un modo fantastico per comunicare e rimanere in contatto con il mondo. Se seguirete i suggerimenti che vi abbiamo illustrato sarete più sicuri. Per saperne di più su come usare i social network in modo sicuro o per comunicare attività sospette, fate riferimento alle pagine relative alla sicurezza dei servizi che utilizzate.

Per saperne di più

Iscriviti ad OUCH!, la newsletter mensile dedicata alla security awareness, consulta i suoi archivi online, e scopri le soluzioni di SANS sulla security awareness visitando il sito
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).

Risorse

Le passphrases:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_it.pdf
La verifica in due passagg:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201308_it.pdf
Usare le app in modo sicuro:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201501_it.pdf
Insegnare ai bambini la sicurezza online:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201506_it.pdf
Pagina sulla sicurezza di Facebook:	https://www.facebook.com/safety

Direzione editoriale: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis