SICUREZZA INFORMATICA

SOCIAL NETWORK

REGOLE DI COMPORTAMENTO

Ver.1.0, 20 marzo 2015

Pagina lasciata intenzionalmente bianca

Proteggersi dai rischi legati all'uso dei "social network"

I siti web di *social networking* come Facebook, Twitter, LinkedIn, sono servizi che realizzano "reti sociali" fra utenti, consentendo di connettersi con altre persone e condividere informazioni come foto, video e messaggi sia a scopo puramente relazionale, sia per motivi legati all'ambito lavorativo.

Nonostante le funzionalità dei siti e delle applicazioni social possano differire anche parecchio, tutti consentono in varia misura di condividere informazioni sulla propria persona e offrono strumenti di comunicazione con altri utenti dello stesso servizio: forum, chat, servizi di messaggeria istantanea, ecc.

L'enorme diffusione e popolarità di questi siti comporta un elevato grado di rischio nel loro utilizzo. La natura stessa di questi siti incoraggia gli utenti a diffondere informazioni personali e, in alcuni casi, sensibili. L'intermediazione della rete Internet e la mancanza di contatto fisico con i destinatari diretti e indiretti delle informazioni condivise possono dare agli utenti *social* un falso senso di anonimità e di sicurezza, portandoli ad ignorare le più comuni cautele che si utilizzano di norma nei rapporti personali. Anche la voglia di "mettersi in mostra" sui *social* per impressionare amici, collaboratori e potenziali datori di lavoro può portare a comportamenti che possono mettere a rischio la privacy, gli affetti, la carriera e, in casi estremi, anche la nostra stessa incolumità.

Inoltre, i siti di *social networking* possono essere sfruttati per condurre attacchi informatici, diffondere *malware* e spam, compiere furti di identità e altri illeciti, in maniera analoga a quanto avviene con altri tipi di siti Web e con la posta elettronica.

Suggerimenti per la sicurezza sui social network

Di seguito si elencano alcuni suggerimenti su come comportarsi in maniera sicura e responsabile nell'utilizzo dei servizi social, in modo da evitare la maggior parte dei rischi. Queste semplici regole di comportamento vanno seguite scrupolosamente, specialmente nel caso di accesso ai *social network* da parte di minori, che, se proprio non può essere evitato, deve sempre essere mediato e supervisionato da adulti consapevoli.

1. **Ricordarsi sempre che Internet è come una piazza pubblica**: tutto ciò che viene pubblicato diviene visibile a tutti e, una volta pubblicato, è quasi impossibile rimuoverlo. Quindi, pubblicate soltanto informazioni, foto e video che non vi possano potenzialmente creare problemi se viste da estranei o, in generale, da persone diverse dal loro destinatario diretto.

2. **Limitare la quantità di informazioni personali pubblicate**: non diffondete informazioni che potrebbero essere utilizzate in maniera malevola o fraudolenta da terzi, come la vostra data di nascita, il vostro indirizzo di casa, le vostre abitudini, i vostri spostamenti, la vostra situazione finanziaria o medica. Esercitate la medesima

cautela nei riguardi di informazioni personali di amici, parenti, colleghi, ecc. Queste informazioni potrebbero essere utilizzate da criminali per profilare le loro potenziali vittime e guadagnare l'accesso ai loro conti bancari o ai loro beni fisici.

3. **Diffidare dagli sconosciuti**: l'uso di Internet rende facile camuffare la propria identità e le proprie intenzioni. Quando interagite con qualcuno per la prima volta via *social*, assicuratevi che sia proprio chi dice di essere prima di dargli informazioni su di voi o, peggio, di accettare di incontrarlo di persona. Diffidate anche se un messaggio sembra provenire da un vostro amico: potrebbe essere falso o provenire da un account violato.

4. **Utilizzare le impostazioni per la privacy**: le impostazioni di *default* dei siti social possono in alcuni casi consentire a chiunque di accedere al vostro profilo e di contattarvi. In questo caso, modificate le impostazioni in modo da limitare l'accesso solo a determinate persone. Tenete sotto controllo le condizioni d'uso e le impostazioni dei servizi *social* che utilizzate in quanto possono essere variate dai gestori in qualsiasi momento. In generale, prima di iscrivervi su un *social network* leggete l'informativa sulla privacy del sito e verificate se il gestore monitora i contenuti pubblicati dagli utenti e fornisce le informazioni raccolte a terze parti per scopi commerciali.

5. **Fare attenzione alle applicazioni di terze parti**: le applicazioni, I *widget* e I giochi disponibili su molti siti social possono nascondere delle insidie. Siate cauti quando decidete quali applicazioni attivare e, soprattutto, nel concedere a queste applicazioni i permessi di accesso ai vostri dati.

6. **Non credere a tutto quello che viene pubblicato online**: molte persone tendono a pubblicare informazioni false o esagerate. A volte si tratta di scherzi innocenti, altre volte di vere e proprie truffe. Siate cauti nel valutare la veridicità delle informazioni pubblicate sui *social*, anche quando vengono dai vostri "amici".

7. **Pensare prima di "cliccare"**: fate attenzione quando cliccate su link, immagini e video contenuti nei messaggi sui *social network*. Potrebbero essere fraudolenti e reindirizzarvi verso siti malevoli realizzati per diffondere *malware* o rubare credenziali. Quando accedete al vostro profilo social digitate l'indirizzo direttamente nel *browser* o memorizzatelo come segnalibro.

8. **Utilizzare sempre le necessarie contromisure "tecniche"**: usate password robuste per accedere ai vostri profili social; non usate mai le stesse credenziali per servizi diversi; mantenete il vostro PC sicuro aggiornando costantemente sistema e applicazioni, in particolare il vostro browser; installate e mantenete aggiornato un buon anti-virus.