

08/02/2010

www.enisa.europa.eu

Instantly Online - 17 Regole d'oro per combattere i rischi in rete e per una navigazione mobile nei Social Networks più sicura

Oggi l'agenzia di "sicurezza cibernetica" dell'EU - ENISA (European Network and Information Security Agency) ha presentato un nuovo report sull'accesso ai Social Networks tramite telefono cellulare dal titolo "[Online as soon as it happens](#)". Il report evidenzia i rischi e le minacce associate all'uso dei Social Networks tramite dispositivo mobile, come ad esempio il furto di identità, la fuga di informazioni aziendali e la lesione della reputazione. La relazione indica inoltre 17 "regole d'oro" su come contrastare tali rischi.

I siti di Social Networks (SNS) hanno registrato un'enorme crescita in Internet. 211 milioni di utenti (su 283 milioni) in Europa utilizzano i Social Networks online, in particolare Facebook, in 11 dei 17 paesi presi in considerazione. I Social Networks, insieme ad altri mezzi digitali, rappresentano il modo moderno per tenersi in contatto con conoscenze professionali e personali. Le modalità con cui le persone si incontrano, condividono opinioni, comunicano informazioni ed idee, di conseguenza, stanno cambiando. La crescente popolarità dei Social Networks, ha determinato un aumento nella richiesta di accesso continuo e immediato agli stessi tramite telefono cellulare, i cosiddetti Mobile Social Networks. Attualmente oltre 65 milioni di utenti accedono a Facebook tramite dispositivo mobile. Gli utenti che usufruiscono dei Social Network dai dispositivi mobili sono 50% più attivi rispetto agli utenti con accesso da linea fissa e si stima che entro il 2012 saranno 134 milioni.

Molti degli utenti dei Mobile Social Networks utilizzano il proprio telefono anche per gestire le e-mail professionali, i dati personali, i contatti, le fotografie e i codici di accesso. Di conseguenza, lo smarrimento di un telefono cellulare può causare danni di grave entità, se per esempio viene utilizzato illegittimamente per accedere ai Social Networks. Molti telefoni cellulari vengono venduti con applicazioni di Social Networks già installate, i cosiddetti servizi "on-deck".

Dai molteplici episodi verificatisi in Italia, Francia, Spagna, Grecia e Regno Unito, emerge che molti utenti di Social Network, sia con accesso da cellulare che da rete fissa, sono ampiamente inconsapevoli dei rischi legati alla sicurezza, alla privacy e a un abuso delle informazioni pubblicate online sui Social Networks, e non sanno come proteggere la propria privacy. Il report identifica un certo numero di rischi e pericoli specifici legati all'uso dei Social Networks tramite dispositivi mobili. Il [report di ENISA](#) fornisce una panoramica generale della situazione e sottolinea, in particolare, che gli utenti in mobilità dei Social Network necessitano di una maggiore consapevolezza sull'uso sicuro dei Social Network tramite cellulare, per evitare conseguenze impreviste e indesiderate. Tali rischi includono il furto di identità e la lesione alla reputazione personale o aziendale, nonché la fuga di informazioni. Di seguito citiamo due esempi.

- **Falso profilo su Facebook.** Un professore dell'Università di Torino ha scoperto che qualcuno aveva creato un profilo offensivo a suo nome su Facebook, lesivo della sua reputazione.

08/02/2010

www.enisa.europa.eu

- **Fuga di informazioni aziendali.** In seguito a un episodio verificatosi nel 2008, la compagnia aerea Virgin Atlantic ha licenziato 13 impiegati che avevano pubblicato su Facebook dei commenti negativi sull'igiene degli aerei della compagnia o dei passeggeri. Anche il personale addetto al check-in di British Airlines dell'aeroporto di Gatwick ha pubblicato messaggi su Facebook in cui i passeggeri venivano appellati "puzzolenti" e vi erano commenti negativi sulla confusione che regnava all'aeroporto di Heathrow.

Il report, inoltre, fornisce una visione esauriente del mondo dei Social Networks in considerazione della direttiva europea sulla tutela dei dati (Dir. 95/46/CE). Il direttore esecutivo di ENISA Udo Helmbrecht commenta:

"Questa relazione fornisce consigli semplici e pratici agli utenti su una presenza più sicura in Rete, in qualsiasi luogo e momento, durante l'utilizzo dei Social Network in mobilità."

Il documento contiene 17 "regole d'oro" di carattere pratico, tra cui quelle riportate qui di seguito:

- Ricordarsi di effettuare il log out, ovvero di "uscire" dal Social Network, una volta conclusa la navigazione.
- Non consentire al Social Network di memorizzare la propria password (questa funzione si chiama "Auto-complete").
- Non mescolare i contatti di lavoro con quelli personali.
- Segnalare immediatamente lo smarrimento e/o il furto di telefoni cellulari con contatti, fotografie o dati personali in memoria.
- Impostare correttamente il livello di privacy sul profilo.

Per la lista completa dei consigli, **scaricare il [documento completo](#)**.
(<http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens>)

Per interviste: Ulf Bergstrom, portavoce, ENISA, press@enisa.europa.eu, cellulare: +30-6948-460143, o Isabella Santa, Senior Expert nell'Awareness Raising. ENISA, awareness@enisa.europa.eu