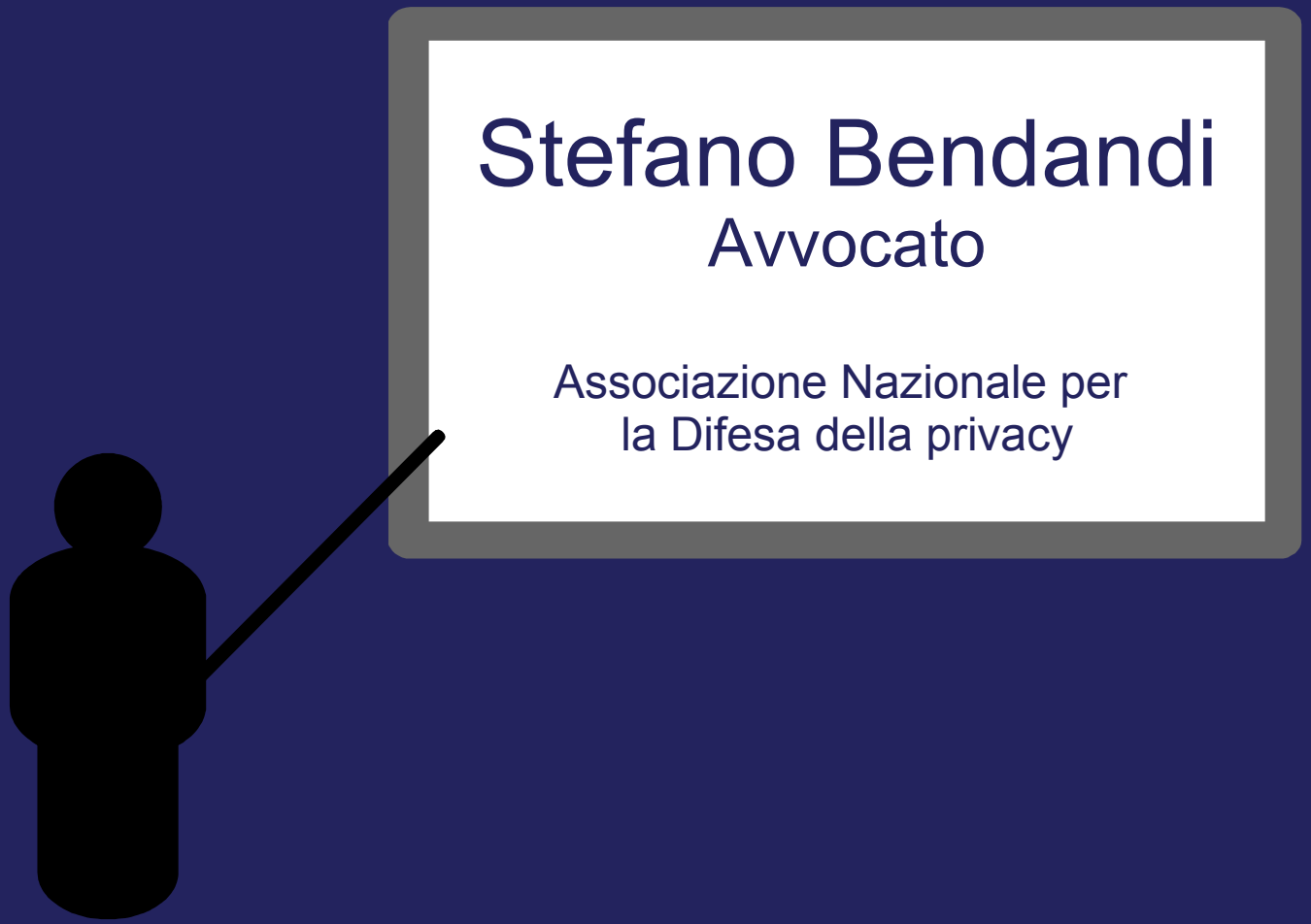
Social network: la privacy online



Perchè i social network hanno così successo ?

Vantaggi

- Agevolano la nascita di nuove relazioni
- Rendono possibile la collaborazione “online”
- Possono favorire la crescita del business
- Fanno trapelare un senso di intimità nelle relazioni
- Offrono un controllo sui dati e contenuti

Svantaggi

- “Devono” catturare l'attenzione dei nuovi utenti
- Lo sviluppo non considera privacy e sicurezza
- Il senso di intimità nelle relazioni è apparente
- Gli utenti sono più propensi a rivelare informazioni personali
- Gli utenti non sono selettivi nella scelta dei contatti

Quali rischi per gli utenti ?

1. Creazione di dossier elettronici

- I dati associati ai profili possono essere collezionati da “chiunque”
- Alcuni dati possono essere accessibili mediante pagine di ricerca
- Le informazioni raccolte sono utilizzabili in contesti e con finalità differenti
- Rischi: spamming, imbarazzo, ricatti, danni alla reputazione

2. Aggregazione di dati secondari

- Disponibilità di dati comportamentali (data, durata della connessione, ip, profili visitati)
- Le policies sono ambigue o poco trasparenti
- L'esigenza di ottimizzazione può celare scopi differenti (pubblicità, discriminazione, vendita a terzi)
- Rischi: profilazione abusiva dei comportamenti degli utenti

3. Riconoscimento facciale

- Le immagini costituiscono uno pseudonimo digitale
- Sono associabili a profili relativi a servizi eterogenei (sn,blog,sito web,ecc...)
- Il riconoscimento non è più una realtà disponibile alle sole forze dell'ordine
- Rischi: accesso ad una quantità di informazioni eccessiva

4. Content-based image retrieval

- Tecnica sviluppata nella “digital forensic”
- Permette il riconoscimento delle caratteristiche di un ambiente/luogo
- Possibilità di dedurre dati di localizzazione
- Rischi: stalking, spamming, pubblicità
- Problema sottovalutato da fornitori di servizi ed utenti

5. Immagini e metadati

- Le immagini possono essere etichettate con nome, profilo, email della persona ritratta
- L'interessato perde il controllo dei suoi dati
- Le immagini digitali spesso includono metadati (seriale del dispositivo)
- Il seriale può consentire di risalire all'indirizzo del titolare attraverso la relativa garanzia

6. Cancellazione dei dati

- La cancellazione non rimuove i contenuti
- Ambiguità delle policies o semplice disattivazione dei profili
- Incremento dell'effetto “dossier digitale”
- Non conformità con la direttiva 95/46/CE
- Rischi: la perdita di controllo sulla propria identità

7. Spamming

- Gli spammer vogliono sfruttare a loro vantaggio i SN
- Automatizzazione di inviti e post (software)
- Creazione di falsi profili per garantire l'accettazione degli inviti
- Rischi: inefficienza, perdita di fiducia, furto di password, phishing, attacchi contro la reputazione

8. XSS, virus e worm

- Posting in html e componenti di terze parti = suscettibilità agli attacchi XSS
- Gli attacchi possono essere vettori per virus e worm
- Virus Samy (MySpace): 1 milione di profili in 20 ore
- Rischi: compromissione account, DoS, phishing

9. Aggregatori sociali

- Integrano i dati di reti differenti in una singola applicazione (Snag, ProfileLinker)
- Accesso a più account basato sulla stessa autenticazione user/password
- Possibilità di accesso ai dati di più servizi con strumenti di ricerca integrati
- Rischi: furto di identità e perdita di privacy

10. Phishing

- Attacchi specifici basati su informazioni attendibili
- Vulnerabilità all'ingegneria sociale
- Gli stessi SN diventano piattaforme di phishing (JS/Quickspace.A su MySpace)
- Rischi: furto di identità, compromissione di account, danni economici e alla reputazione

11. Perdita di informazioni

- Inefficacia del meccanismo di visibilità dei dati
- E' molto facile diventare “amici” di chiunque
- Il processo può essere automatizzato tramite software specifici
- Meccanismi, come i captcha, non sono attivi
- Rischi: accesso ad informazioni private, spamming, phishing, pubblicità non desiderata

12. Attacchi alla reputazione

- Creazione di profili con una falsa identità
- Fattori che accrescono gli effetti:
  - Le connessioni sociali facilitano gli attacchi contro le persone più note di un gruppo
  - Difficoltà della vittima di accesso al falso profilo
  - Autenticazione debole in fase di registrazione
- Rischi: danni alla reputazione, phishing, pubblicità indesiderata

13. Persecuzione

- Gli utenti sono localizzabili attraverso i propri dati (indirizzo, telefono, email, im)
- Alcuni dati possono rivelare lo status “online”
- Implicazioni maggiori nelle piattaforme di SN mobili
- Rischi: perdita di privacy, intimidazioni, danni psicologici o fisici

14. Cyberbullismo

- Circa 1/10 dei giovani viene coinvolto in fenomeni di bullismo tecnologico
- Fattori di vulnerabilità dei SN:
  - Possibilità di comunicare con gruppi ristretti
  - Facilità di rimanere anonimi (falsi profili)
  - Presenza di strumenti nella stessa interfaccia
  - Gap generazionale

15. Spionaggio industriale

- Impostazioni di privacy deboli o trascurate
- Possibilità di accedere ad informazioni su:
  - Liste di personale dipendente
  - Connessioni tra il personale
  - Informazioni sugli stakeholders
  - Informazioni confidenziali (qualifiche, funzioni)
  - Informazioni sulle infrastrutture IT

Quali sono le possibili contromisure ?

Contromisure

- Revisione dei framework legislativi
- Educazione e consapevolezza degli utenti:
  - Linee guida chiare e dettagliate
  - Disponibilità di informazioni contestuali
  - Divieto di pubblicare certi dati
  - Formazione adeguata per gli sviluppatori
- Maggiore trasparenza nel trattamento dei dati

Contromisure

- Procedure di denuncia degli abusi chiare e dettagliate (user-friendly)
- Miglioramento del livello di controllo degli accessi
  - Autenticazione forte
  - Altri meccanismi (ad es. captcha)
- Strumenti per la completa rimozione di account e contenuti generati dagli utenti

Contromisure

- Impostazioni predefinite relative alla privacy:
  - Miglioramento dei livelli di sicurezza
  - Differenziazione per età
  - Linee guida comprensibili
- Sistemi intelligenti di filtraggio dei contenuti
- Restrizioni alla creazione di account fittizi ed utilizzo di agenti software (robot)

Contromisure

- Adozione di sistemi basati sulla reputazione:
  - Filtri sui commenti (indici di qualità)
  - Registrazione utenti solo su presentazione
  - Adozione di procedure per riferire:
    - Furti di identità
    - Pubblicazioni di contenuti sconvenienti
    - Pubblicazioni di informazioni di geolocalizzazione
- Consenso esplicito degli interessati per etichettare le immagini con dati personali

Contromisure

- Controlli sui dati risultato delle ricerche
- Strumenti per contrastare spam e phishing
- Tecniche di anonimizzazione delle immagini
- Creazione di framework portabili di SN (decentralizzazione)
- Analisi delle implicazioni dei nuovi trend

Contatti

Avv. Stefano Bendandi

Studio di consulenza
Via G. Mazzarino 8
65126 Pescara (PE)
Tel e Fax 085.67430

Web: http://www.stefanobendandi.com
Blog: http://stefanobendandi.blogspot.com

Grazie per l'attenzione !

Licenza