

Moduli di formazione InCyT

Sicurezza delle informazioni per i dipendenti

Unità n.: (4) Settimana 8

Nome dell'unità (modulo): (Social Networking)

<i>Attività di apprendimento</i>	☐ Webinar ☐ Esercizi ☐ Workshop ☐ Presentazione ☐ Altro Webinar in streaming, testi, esercizi di autovalutazione, esercizi con risposte su forum di discussione e nell'ambito delle sessioni organizzate con il formatore/mentore, e-portfolio.
<i>Apprendimento responsabile</i>	- David Sommer - Ileana Amburgo
<i>Obiettivi dell'attività di apprendimento</i>	- Ruoli di social network - Funzionalità delle piattaforme di social network - Sicurezza e privacy nelle reti sociali - Minacce alle reti sociali online e soluzioni per evitarle - L'interdisciplinarietà nelle reti sociali
<i>Competenze da acquisire</i>	TS3 Sicurezza della rete TS4 Test di penetrazione (vulnerabilità sfruttabili) TS5 Rilevamento delle intrusioni SS3 Analisi cognitiva e comportamentale
<i>Durata dell'attività di apprendimento</i>	2 settimane
<i>Apprendimento requisiti</i>	Cosa serve? - Accesso a Internet - Browser Internet - MS Office365

Brevi informazioni sul modulo

 Descrizione
I social network aiutano le persone e le organizzazioni a connettersi con gli amici, sono mezzi di comunicazione, aiutano a lanciare una nuova idea di business, a vendere prodotti o servizi e ad estendere la portata del proprio marchio. Certo, ci sono anche degli svantaggi, come la riduzione delle capacità di comunicazione faccia a faccia. Poiché le organizzazioni utilizzano intensamente i social media, gli aggressori sfruttano la fiducia e la natura pubblica di queste piattaforme per sferrare attacchi. La sicurezza dei social network è importante per il successo aziendale e privato, quindi la formazione dei dipendenti, come quella prevista in questo modulo, può dare un grande contributo. I dipendenti imparano a conoscere tali aspetti leggendo il testo corrispondente, guardando i webinar in streaming, risolvendo esercizi al proprio ritmo e riflettendo su quanto appreso (e-portfolio). Tutti i documenti del modulo sono presenti sulla piattaforma digitale interattiva del progetto. I discenti possono verificare le loro risposte negli esercizi di autovalutazione. Le risposte agli altri esercizi devono essere salvate nei forum di discussione corrispondenti e discusse con il tutor durante l'incontro comune organizzato una volta alla settimana. Gli studenti possono lavorare in modo cooperativo con gli altri e con il tutor, in particolare durante gli incontri settimanali.

Contenuto del materiale didattico

Introduzione

Anche grazie alla crescente tecnologia, i social network (online) sono diventati molto popolari negli ultimi anni. Uno dei motivi è la loro capacità di fornire agli utenti una piattaforma per comunicare con la famiglia, gli amici e i colleghi.

Per social network si intende l'uso di siti di social media basati su Internet per connettersi e comunicare con amici, familiari, colleghi, clienti o clienti.

I social media aiutano le persone ad avere relazioni migliori con la famiglia, gli amici, i clienti e i dispositivi mobili che supportano i social media stanno guadagnando sempre più interesse rispetto ad altre modalità di accesso a Internet.

I social network hanno i loro server in centri dati co-localizzati, quando possibile, con i principali Network Access Point (NAP) di Internet, dove i grandi fornitori di servizi Internet si collegano tra loro e dove forniscono l'accesso diretto alle connessioni veloci di Internet.

Ruoli di social network

I social network possono avere un ruolo sociale, lavorativo o entrambi, utilizzando siti come Facebook, Twitter, LinkedIn e Instagram. La Figura 1 mostra alcuni ambiti in cui i social network svolgono un ruolo (Milsova et al.): intrattenimento, creazione di opportunità di lavoro, carriera, miglioramento delle abilità sociali e sviluppo di relazioni con altri individui.

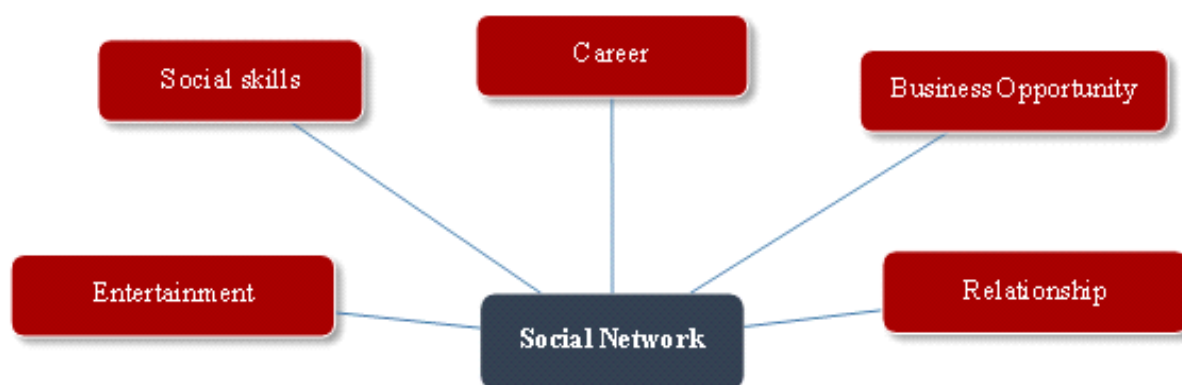


Figura 1: Ruoli delle reti sociali

I social network sono una base per i marketer che cercano clienti. I marketer utilizzano i social network per aumentare il riconoscimento del marchio e incoraggiarne la fedeltà. I social media possono aiutare a mettere in contatto persone e aziende e a promuovere la conoscenza del marchio. Ad esempio, un utente abituale di Twitter può venire a conoscenza di un'azienda per la prima volta attraverso il feed di notizie e decidere di acquistare un prodotto o un servizio. Le possibilità dell'azienda di trovare e fidelizzare nuovi clienti aumentano grazie ai social network. I marketer utilizzano i social network per migliorare i tassi di conversione, fornendo accesso e interazione con clienti nuovi, recenti e vecchi. Condividendo post di blog, immagini, video o commenti sui social media, un maggior numero di persone visiterà il sito web dell'azienda e diventerà cliente. Ma non esiste un unico approccio alle strategie di marketing: ogni azienda è unica e ha un target demografico, una storia e un mercato competitivo diversi. Poiché le società di social network vogliono che le aziende paghino per la loro pubblicità, spesso limitano il numero di contatti che le aziende ricevono attraverso i post non retribuiti. Ad esempio, se un'azienda ha 500 follower, questi ultimi non possono ricevere tutti lo stesso post. La natura evolutiva dei social network rende difficile tenere il passo con i cambiamenti e influenza anche il tasso di successo del marketing di un'azienda.

Facebook, Instagram, Facebook Messenger e Twitter sono i siti di social networking più popolari in Europa e Stati Uniti. Altri includono Pinterest, Tumblr, Snapchat, TikTok, YouTube, WhatsApp, Messenger by Google

e Tumblr. LinkedIn è un altro sito popolare, che aiuta a mettere in contatto i professionisti con collaboratori, contatti di lavoro e datori di lavoro. Facebook rimane il social network più grande e più popolare, con 2,91 miliardi di persone che utilizzano la piattaforma su base mensile, al 31 dicembre 2021. La Figura 2 mostra il numero di utenti delle piattaforme.

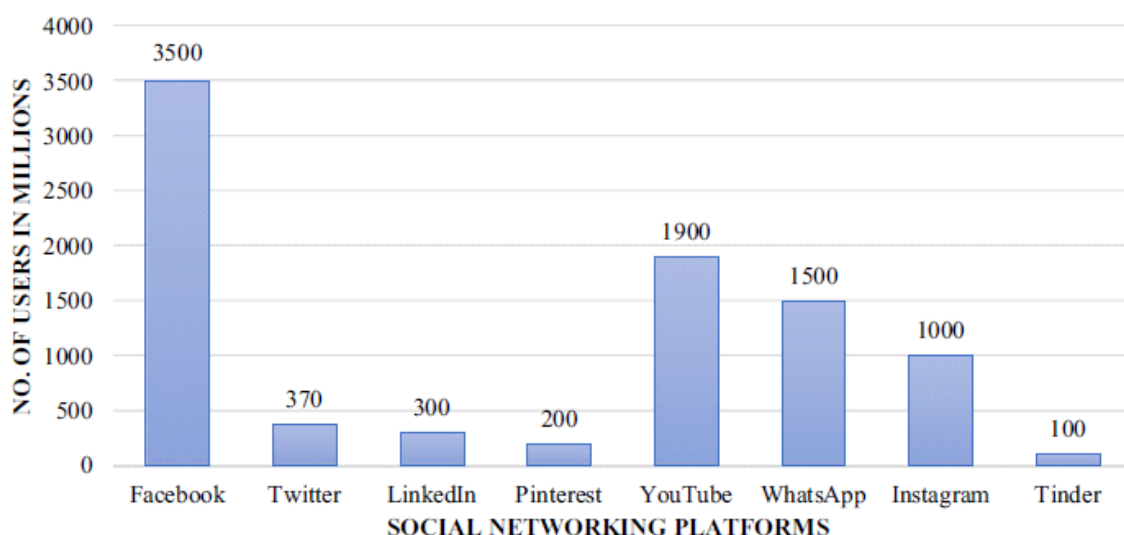


Figura 2: Numero di utenti sulle piattaforme (<https://www.dreamgrow.com/top>)

Funzionalità dei social network

Il social networking si basa sullo sviluppo e sul mantenimento di relazioni personali e commerciali attraverso la tecnologia, grazie all'uso di siti di social networking. Questi siti permettono a persone e aziende di connettersi tra loro per sviluppare relazioni e condividere informazioni, idee e messaggi.

I membri della famiglia lontani possono rimanere in contatto attraverso i siti personali di social network come Facebook, condividendo foto e inviando altri messaggi della loro vita. Le persone possono anche entrare in contatto con altri (sconosciuti) che condividono gli stessi interessi. Gli individui possono trovarsi tra loro attraverso la partecipazione a gruppi, liste e l'uso di hashtag.

Ma ci sono anche degli svantaggi legati ai social media, tra cui la diffusione della disinformazione e gli alti costi di utilizzo e mantenimento dei profili dei social network.

Ogni social network ha un uso specifico, ma le funzionalità di queste piattaforme sono simili e possono essere classificate in tre tipi principali:

- Le funzioni di rete servono a promuovere le relazioni sociali tra gli utenti all'interno delle piattaforme virtuali. In particolare, forniscono funzionalità per la costruzione e il mantenimento del grafo della rete sociale.
- Le funzioni dati sono responsabili della gestione dei contenuti forniti dagli utenti e delle comunicazioni tra gli utenti. La varietà contribuisce a migliorare (estendere) l'interazione degli utenti e a rendere la piattaforma più attraente.

- Le funzioni di controllo degli accessi mirano a implementare le misure di privacy definite dall'utente e a limitare l'accesso non autorizzato ai dati e alle informazioni fornite dall'utente. La Figura 3 mostra le funzionalità fornite da una tipica piattaforma di social network virtuale e fornisce ulteriori dettagli (Cutillo et al. 2010).

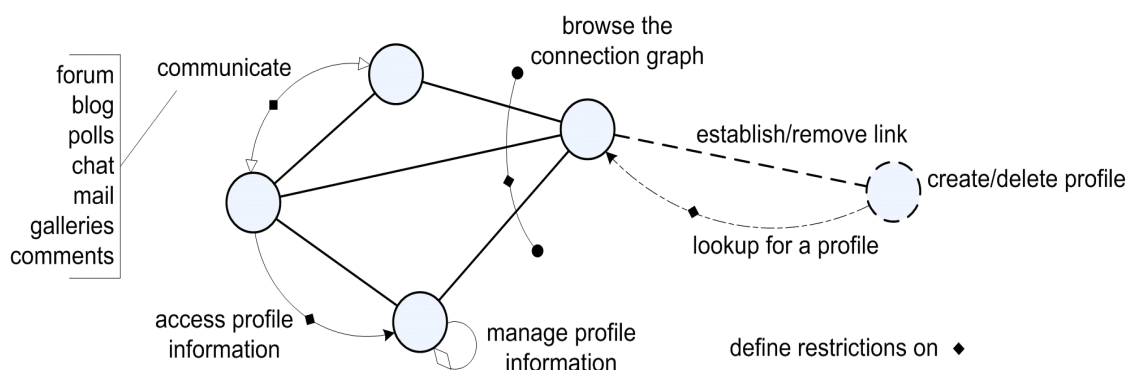


Figura 3: Principali funzionalità di una tipica piattaforma di social networking
(<https://hal.archives-ouvertes.fr/hal-00687145>)

I siti di social networking possono essere classificati in "connessioni sociali", "condivisione di contenuti multimediali", "professionali" e "forum di discussione" (Figura 4 Jain et al., 2021).

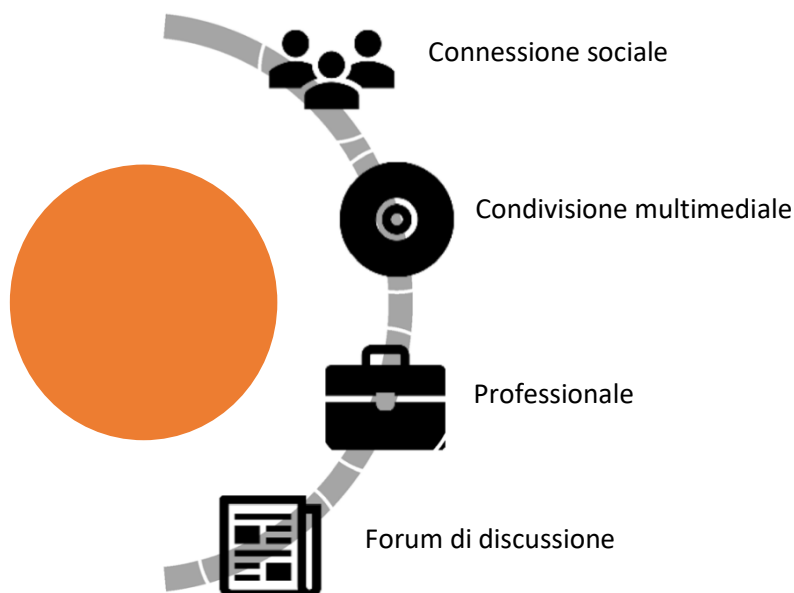


Figura 4: Siti di social networking (Jain et al, 2021)

Vantaggi e svantaggi dei social network

I social network hanno la capacità di influenzare sia gli individui che le aziende, sia in positivo che in negativo, ed è quindi importante prendere in considerazione vantaggi e svantaggi dell'utilizzo di questi siti di social media.

Vantaggi

I social network consentono di mantenere i contatti con familiari e amici che altrimenti non sarebbero possibili a causa della distanza o della perdita di contatto. Le persone possono anche entrare in contatto con altri individui che condividono gli stessi interessi e sviluppare nuove relazioni.

I social network consentono alle aziende di entrare in contatto con clienti nuovi ed esistenti. Le aziende possono anche utilizzare i social media per creare, promuovere e aumentare la consapevolezza del marchio. Inoltre, si affidano alle recensioni e ai commenti dei loro clienti, importanti per il marchio. Possono aumentare le vendite e il posizionamento nei motori di ricerca.

I social network possono aiutare a creare un nuovo marchio. Un'azienda può utilizzare i social network per dimostrare l'elevato livello di servizio ai clienti e migliorare i prodotti e le relazioni con i consumatori. Ad esempio, se un cliente si lamenta di un prodotto o di un servizio su Twitter, l'azienda si scusa e interviene per migliorare la situazione.

Svantaggi

I social network possono contribuire alla diffusione della disinformazione. Sahoo e Gupta (2020) hanno scoperto che su Twitter la disinformazione ha il 70% di probabilità in più di essere condivisa rispetto alle informazioni corrette.

Il networking sui social media può avere un impatto negativo sulle aziende. Le critiche a un marchio si diffondono molto rapidamente sui social media. Questo comporta degli svantaggi per il dipartimento di pubbliche relazioni (PR) di un'azienda.

Il social network in sé è gratuito, ma la costruzione e il mantenimento di un profilo aziendale richiedono ore di lavoro e costi settimanali. Le aziende hanno bisogno di molti follower prima che una campagna di social media marketing inizi a generare un ritorno positivo sull'investimento (ROI). Ad esempio, inviare un post a 15 follower non ha lo stesso effetto che inviarlo a 15.000 follower.

Sicurezza e privacy nelle reti sociali

Le informazioni condivise sui social network e sui media si diffondono molto velocemente, il che rende interessante per gli aggressori acquisirle. Esistono problemi di sicurezza e di privacy legati alle informazioni condivise dagli utenti quando questi caricano contenuti personali come foto, video e audio. Gli aggressori possono utilizzare le informazioni condivise per scopi illegittimi.

Vengono brevemente presentate alcune minacce alla sicurezza e alla privacy e le soluzioni esistenti che possono garantire la sicurezza degli utenti dei social network.

Grazie all'uso intensivo della tecnologia, le interazioni sono state estese attraverso Internet. Purtroppo, la mancanza di consapevolezza degli utenti in materia di sicurezza e privacy può potenzialmente portare a

vari attacchi informatici attraverso i social media. Le minacce che gli utenti hanno rilevato fin dall'inizio dei social network possono essere suddivise in tre categorie: minacce convenzionali, minacce moderne e minacce mirate (Fig. 5, Jain e Gupta, 2018). Le minacce convenzionali includono le minacce che gli utenti hanno sperimentato fin dall'inizio del social network. Le minacce moderne sono attacchi che utilizzano tecniche avanzate per compromettere gli account degli utenti e gli attacchi mirati sono attacchi mirati a un particolare utente che possono essere commessi da qualsiasi utente per varie vendette personali.

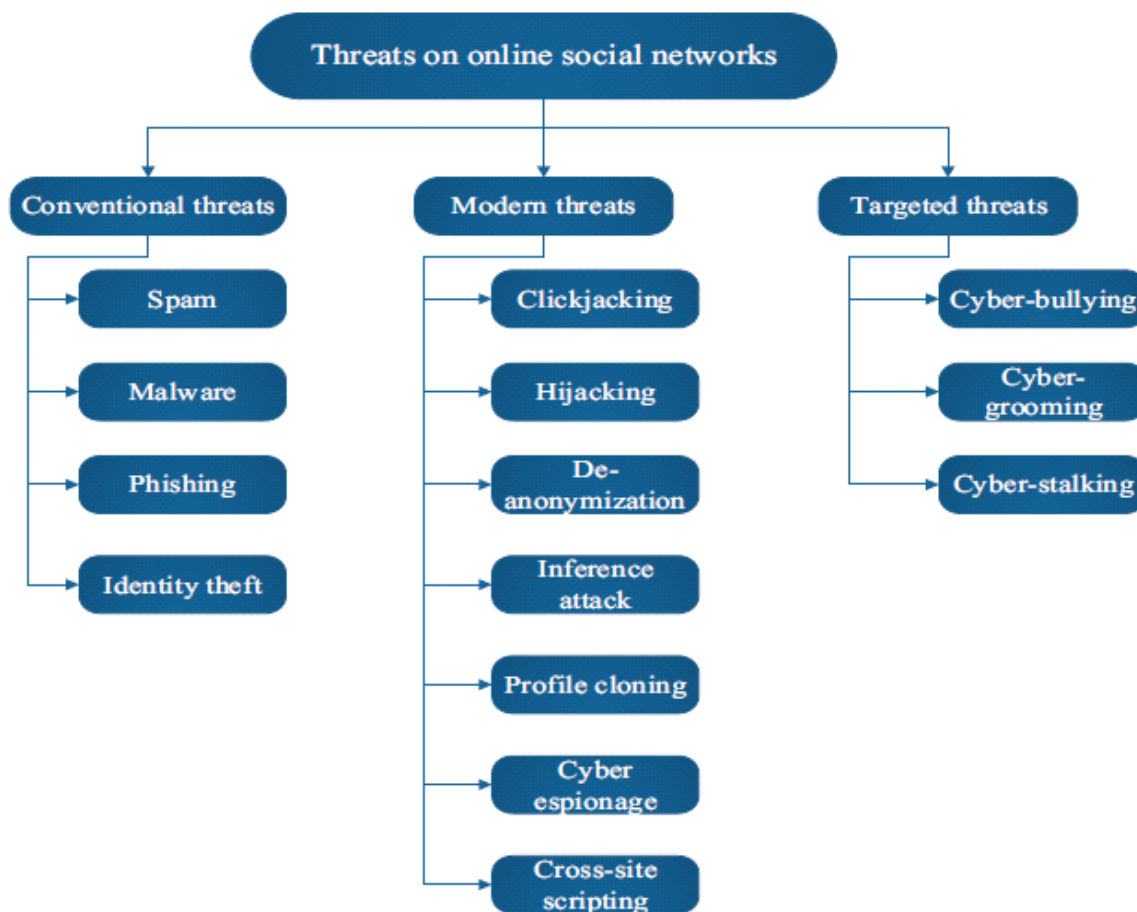


Figura 5: Classificazione delle minacce (Jain et al, 2018)

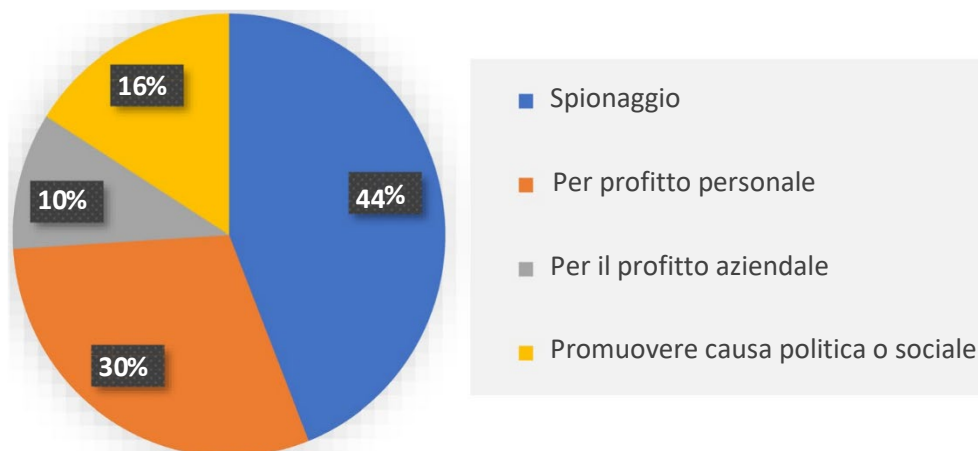


Figura 6: La maggior parte dei tipi di hacking nel 2021 (Jain et al, 2021)

Soluzioni alle minacce

I ricercatori del mondo accademico e industriale cercano di trovare soluzioni per le minacce nei social network per diversi tipi di hacking, come mostrato nella Figura 6. Le soluzioni e gli approcci proposti possono essere classificati in due gruppi: soluzioni degli operatori di social network e soluzioni accademiche (Jain et. al, 2021). Sono state proposte soluzioni e approcci che possono essere classificati in due gruppi: soluzioni degli operatori di social network e soluzioni accademiche (Jain et al, 2021). La Figura 7 mostra la classificazione. Di seguito viene presentata una breve descrizione.

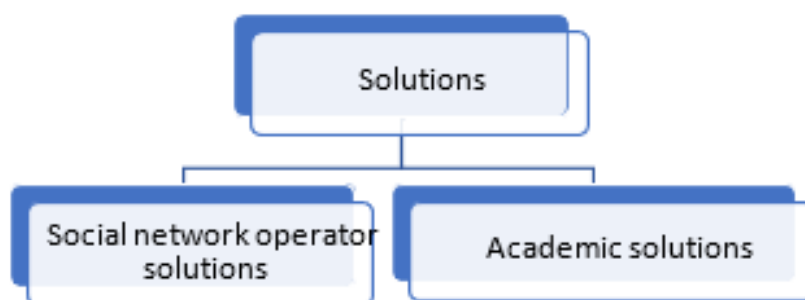


Figura 7: Classificazione delle soluzioni alle minacce (Jain et al, 2021)

Soluzioni per operatori di social network

Meccanismo di autenticazione

Per assicurarsi che solo un utente legittimo si stia registrando in un social network e non un Bot sociale, sono state proposte procedure di autenticazione come CAPTCHA, l'autenticazione a più fattori e l'identificazione tramite foto di amici. Ad esempio, social network come Twitter e Facebook utilizzano principi di autenticazione a due fattori. Questo principio utilizza una password di accesso e un codice di verifica ricevuto

tramite un dispositivo mobile. Ciò contribuisce a ridurre il rischio di compromissione di un account e impedisce a un aggressore di dirottare un account legittimo e pubblicare contenuti dannosi.

Impostazioni di sicurezza e privacy

Molti siti di social network forniscono impostazioni di sicurezza e privacy configurabili per consentire al cliente di proteggere le informazioni personali da accessi indesiderati da parte di estranei o applicazioni. Ad esempio, il cliente di Facebook può modificare le proprie impostazioni di sicurezza e selezionare il pubblico (come gli amici, gli amici degli amici e tutti) nella rete, che può vedere i suoi dettagli, le sue foto, i suoi post e altre informazioni sensibili.

Segnala gli utenti

I social network proteggono le persone dagli attacchi fornendo la possibilità di segnalare qualsiasi forma di abuso o violazione delle norme da parte di qualsiasi utente della loro rete. Ad esempio, se un utente vede su Facebook qualcosa che corrisponde ai suoi sentimenti, ma non viola i termini di Facebook, può utilizzare una segnalazione (link) per inviare un messaggio a colui che l'ha pubblicato chiedendogli di eliminarlo o rimuoverlo.

Quando Facebook riceve una segnalazione di un utente, questa viene esaminata e rimossa in base agli standard della comunità di Facebook.

Soluzioni basate sulla ricerca accademica

Rilevamento del phishing

Il phishing ha compromesso la privacy e la sicurezza di molte applicazioni web tradizionali, come siti web, siti di social network, e-mail e blog. Di conseguenza, sono state sviluppate diverse tecniche anti-phishing per rilevare gli attacchi di phishing. Per esempio, Aggarwal et al. hanno proposto la tecnica PhishAri per l'identificazione in tempo reale degli attacchi di phishing che avvengono su Twitter. La tecnica utilizza caratteristiche specifiche di Twitter, come l'età dell'account e il numero di follower, per rilevare se il tweet pubblicato è di phishing o sicuro.

Rilevamento del cyberbullismo

Il cyberbullismo è l'uso di mezzi elettronici come e-mail, chat, conversazioni telefoniche e social network online per opprimere una persona. A differenza del bullismo tradizionale, il cyberbullismo è un processo continuo che si svolge attraverso i social media. Sebbene il rilevamento del cyberbullismo sia più complesso di quello del linguaggio razzista e dello spam, alcuni ricercatori hanno cercato di rilevarlo utilizzando una rappresentazione più complessa dei documenti e informazioni aggiuntive sulle vittime e sui bulli. Le tecniche di apprendimento automatico possono essere applicate per rilevare il cyberbullismo.

Clickjacking

Un sistema automatizzato è in grado di analizzare le pagine web per proteggere l'utente dagli attacchi di clickjacking. Si tratta di un codice in grado di rilevare la sovrapposizione di elementi cliccabili. Oltre a questa soluzione, è stato adottato anche lo strumento NoScript, che include una funzione anti-clickjacking.

Cyberstalking

Le tecniche di crittografia sono disponibili per i dispositivi delle versioni recenti di Android e iOS. Se un dispositivo viene rubato, il ladro non può leggerne il contenuto se la crittografia è abilitata. Inoltre, qualsiasi tentativo di leggere le informazioni dalla memoria interna o esterna viene vanificato dall'esistenza di una password del dispositivo. Esistono diverse tecnologie che possono essere utilizzate contro gli stalker, come il blocco delle impronte digitali dello smartphone.

Rilevamento dello spam

Un framework chiamato Spam Spotter può aiutare a contrastare un attacco di spam su Facebook. Si basa su un sistema di supporto decisionale intelligente (IDSS). Raccoglie tutte le informazioni rilevanti dal profilo dell'utente con l'aiuto di un processo decisionale in IDSS e poi le analizza mappando i dati dell'utente alla classificazione di un profilo utente come spammer o legittimo.

Malware

I Cross Site Scripting Worms (XSS worm) sono programmi dannosi che si propagano attraverso i visitatori di un sito web saltando per infettare progressivamente altri visitatori.

Il worm si propaga più lentamente quando i membri visitano soprattutto i loro amici piuttosto che gli estranei. Può anche essere rallentato dalla natura clusterizzata dei social network.

Sebbene il mondo accademico abbia sviluppato soluzioni innovative per affrontare le misure di sicurezza legate alla sicurezza dei social network, esse mancano di implementazione e fattibilità nel mondo reale. È quindi urgente rivedere in modo continuo e iterativo i problemi di sicurezza nei social network, tenendo conto degli sviluppi tecnologici.

L'interdisciplinarietà nelle reti sociali

Il campo interdisciplinare che si riferisce alle reti sociali è la social network analysis (SNA) e include approfondimenti da altre discipline delle scienze sociali come la sociologia, l'antropologia, la psicologia, la comunicazione e altre. La SNA fa parte di un campo interdisciplinare ancora più vasto che si occupa dello studio di tutti i tipi di reti, chiamato scienza delle reti, che comprende lavori di fisica, informatica, scienza dei dati, biologia, ingegneria, matematica e altri campi. La relazione tra questi campi è illustrata nella Figura 8 (https://bookdown.org/omarlizardo/_main/1-2-what-is-a-social-network.html).

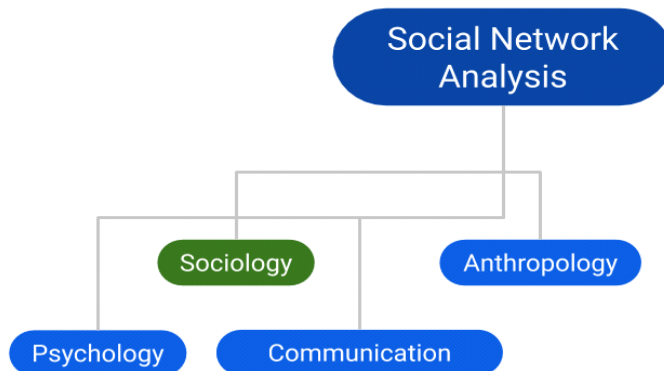


Figura 8: Relazioni tra campi in SNA

(https://bookdown.org/omarlizardo/_main/1-2-what-is-a-social-network.html)

Domande:

Domande Forum di discussione a cui rispondere con una breve spiegazione.

1. I ruoli delle reti sociali
2. Siti di social network
3. Campi interdisciplinari in relazione alle reti sociali

Allegati:

1. Presentazione
2. Filmati

Riferimenti

Aggarwal A., Rajadesingan A & Kumaraguru P. (2012). PhishAri: rilevamento automatico del phishing in tempo reale su Twitter. eCrime Res. Summit, eCrime. 1-12.

Ankit Kumar J., Somya Ranjan S. & Kaubiyal J. (2021). Cause di violazione dei dati a livello mondiale. URL: <https://www.statista.com/statistics/263303/proportion-of-the-most-common-causes-for-possible-identity-theft/>

Cutillo, A., Manulis, M. e Strute, T. (2010). Sicurezza e privacy nelle reti sociali online. EUROCOM. TU Darmstadt.

Gupta B. & Sahoo, S. (2021). Sicurezza delle reti sociali online: principi, algoritmi, applicazioni e prospettive. CRC Press.

- Jain A. & Gupta B. (2018). Rilevamento di attacchi di phishing in siti web finanziari e di e-banking utilizzando la relazione di similarità dei link e visiva. *Int J Inf Comp Secur* 10(4):398-417.
- Jain, A. , Sahoo, S.R. & Kaubiyal, J. (2021). Sicurezza e privacy dei social network online: analisi e revisione completa. *Complex Intell. Syst.* 7, 2157-2177.
- Kangur, K. (2022). I 15 maggiori siti e applicazioni di social media. URL: <https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/>.
- Mislove A., Viswanath B., Gummadi K. e Druschel, P. (2010). Tu sei chi conosci. In: Atti della terza conferenza internazionale ACM su Web search e data mining-WSDM '10, 251.
- Rydstedt, G. (2018). Clickjacking - OWASP. URL: <https://owasp.org/www-community/attacks/Clickjacking>.
- Sahoo SR, Gupta BB (2020). Rilevamento di profili falsi nei big data multimediali delle reti sociali online. *Int J Inf Comput Secur* 12(2-3), 303-331.