MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Social Network

Pericoli e insidie
che si nascondono dietro
ai social media

Sommario

Cosa troverai in questa brochure

Introduzione

Negli ultimi anni, l'utilizzo sempre più frequente dei **Social Network** come Facebook (oggi Meta), Instagram, Tiktok, etc., ha trasformato radicalmente i modi di **interagire**, informarsi ed intrattenere.

Trascorriamo, infatti, gran parte del nostro tempo sui Social Network per tenerci sempre aggiornati, mantenere **legami** con i nostri affetti, creare nuove connessioni sociali e per **condividere esperienze** ed **opinioni**.

Interagire sui **Social Network** senza adottare le giuste precauzioni può fornire ai **criminali informatici** preziose **informazioni** che, se analizzate e correlate le une fra le altre, possono essere **sfruttate** dagli stessi per sferrare **attacchi** informatici mirati.

Per mezzo della condivisione incontrollata di foto, luoghi che si è frequentato, opinioni e pensieri, è possibile fornire del materiale utile ai truffatori che, facendo leva sugli **interessi** ed emozioni delle potenziali vittime, sono in grado di sferrare **attacchi** informatici **altamente credibili**.

Attacchi sui Social Network in Italia

82.675 Segnalazioni inoltrate dai cittadini tramite il portale **www.commissariatodips.it** nel corso del 2024.

29.763 **Segnalazioni** di sicurezza cibernetica che hanno riguardato **minacce legate ai social network.**

Le caratteristiche di un attacco veicolato tramite Social Network

Inganno tramite ingegneria sociale: il truffatore cerca di mettersi in contatto con le potenziali vittime, studiando le loro abitudini ed inviando loro dei messaggi che attirano l'attenzione.

Alta efficacia: è uno degli attacchi informatici più insidiosi in cui si sfruttano vari tipi di abuso e di crimine digitale, come il cyberbullismo e le molestie online.

Semplicità operativa: l'attaccante crea un profilo social apparentemente legittimo avvalendosi anche dell'intelligenza artificiale.

Canale di attacco: all'interno dei messaggi inviati dal criminale informatico è presente un link compromesso, usato per violare l'account.

Fonte
Polizia Postale e per la Sicurezza Cibernetica – Report Annuale 2024.

Attento ai social!

Rischi

01 Violazione dei dati personali

Una **navigazione poco consapevole** sui **Social Network** può esporti maggiormente a subire **attacchi mirati** di Ingegneria Sociale. Tali attacchi sono finalizzati ad indurti a **condividere informazioni riservate** come ad esempio credenziali di accesso, dati personali o informazioni bancarie.

02 Furto di identità digitale

La condivisione incontrollata di informazioni di carattere strettamente personale può indurre i criminali informatici a **violare gli account presenti sui social network**. Gli attaccanti, tramite il **furto di identità digitale**, commettono illeciti come aprire conti bancari a nome della persona violata, effettuare transazioni fraudolente e/o compromettere la propria reputazione.

03 Minacce informatiche

Un uso imprudente dei Social Network può diventare un canale per la **diffusione di malware**, quali programmi dannosi in grado di compromettere la sicurezza dei dati e dei dispositivi che utilizzi per navigare. Infatti, potresti essere indotto a cliccare su **link malevoli** presenti in post o messaggi, che potrebbero contenere malware capaci di installarsi sul dispositivo e accedere ai tuoi dati personali, come la corrispondenza o la galleria fotografica.

Contromisure

Sii prudente nel condividere informazioni personali sui social network: diffida da **richieste urgenti** e verifica sempre l'identità di chi ti contatta.

Limita la quantità di informazioni personali **pubbliche**, verifica le impostazioni di **privacy** dei tuoi profili, non accettare richieste di contatto da **sconosciuti** e non usare la stessa **password** per più account.

Non cliccare mai su **link sospetti** ricevuti via messaggi privati o presenti in post, soprattutto se provengono da contatti sconosciuti e controlla sempre l'URL prima di aprirlo.

Come difendersi?

Utenze private

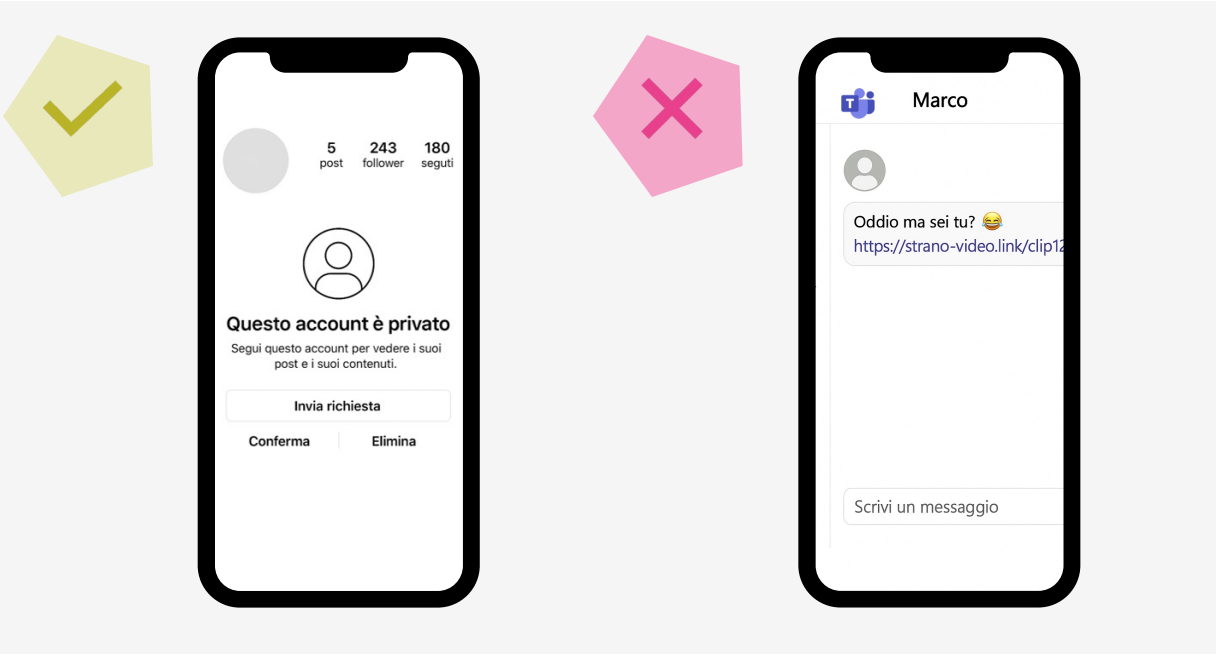
Per evitare che potenziali **truffatori** possano **utilizzare** le **informazioni** condivise sui **Social Network,** proteggi il tuo account modificando le impostazioni di privacy, attivando la modalità «**profilo privato**». Inoltre, **non utilizzare** la tua **e-mail lavorativa** per **registrarti** su piattaforme **Social,** in questo modo, **ridurrai il rischio** di subire attacchi informartici su tale indirizzo.

Condivisione limitata

Per proteggere la tua **privacy**, è importante **limitare la condivisione** di informazioni legate alla sfera lavorativa e personale sui social network. Anche nei contesti di messaggistica professionale, come **Teams**, è bene **evitare l'invio di documenti sensibili**, preferendo canali più sicuri. Queste semplici attenzioni aiutano a ridurre il rischio che dati personali o aziendali vengano **utilizzati in modo improprio.**

Comportamenti attenti

Quando utilizzi i **social network o applicazioni di messaggistica**, anche per scopi lavorativi come nel caso di Teams, è importante **prestare attenzione** ai contenuti che visualizzi, in particolare se provengono da **fonti sconosciute o poco affidabili**. Se clicchi su link esterni, **verifica** sempre che il sito di destinazione sia sicuro e utilizzi il protocollo **https://**, per evitare rischi legati a **truffe o siti malevoli.**



Security Trend

Presunte violazioni dei termini d'uso di Facebook (Meta)

Tra le tecniche più utilizzate dai criminali informatici per perpetrare attacchi vi è quella di inviare un **messaggio** sulla **chat** di **Facebook** (Meta), in cui viene **segnalata** una presunta **violazione** delle **policy** di utilizzo del noto **Social Network**.

Per spingere la potenziale vittima a interagire con il **link malevolo**, il messaggio è formulato in modo da informare l'utente sulle modalità di **verifica delle informazioni correlate all'utilizzo del proprio account**. L'obiettivo apparente è quello di permettere all'utente di disconoscere una **presunta violazione** in corso e/o presentare un **reclamo**.

I truffatori, spacciandosi dunque per un team di controllo di Facebook, minacciano una pluralità di utenti di chiudere l'account social entro le **24 ore** dalla ricezione della comunicazione, mirando a generare un **senso di urgenza**, inducendo l'utente ad agire senza riflettere in un tempo limitato.

L'utente, qualora interagisse con il link compromesso, subirebbe una violazione del suo account, con possibile **furto** dell' **identità digitale** e **violazioni privacy**.

maggio 2025

La truffa del sondaggio su Whatsapp

È stato osservato un nuovo trend in cui i criminali informatici, sfruttando **applicazioni** di **messaggistica**, veicolano dei **link malevoli** da account presenti nella rubrica della potenziale vittima. Si tratta di una forma di **Smishing**, una peculiare forma di phishing veicolata tramite messaggi.

Nello specifico, sfruttando la nota piattaforma di messaggistica istantanea di Meta, **Whatsapp**, gli attaccanti veicolano dei **messaggi** di richiesta di **partecipazione** ad un **sondaggio**, finalizzato all'assegnazione di una **borsa** di **studio** per un proprio parente.

La vittima, ritenendo **affidabile** il **mittente** (un utente in rubrica) è indotta a **cliccare** sul **link** compromesso, consentendo ai criminali informatici di **rubare il proprio account.**

L'utente, qualora interagisse con il **link compromesso,** consentirebbe ai criminali informatici di sottrarre il suo account, compromettendo la sua **identità digitale** e mettendo in atto **ulteriori truffe.**

febbraio 2025

MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Restate sintonizzati:

nuovi approfondimenti sulla cybersecurity vi aspettano nelle prossime pubblicazioni.