Giugno 2025

REGIONE MOLISE

Sistemi Informativi - Cyber Security Brochure

I Social Network

I pericoli e le insidie che si
nascondono dietro ai social media

Regione Molise - Servizio Sistemi Informativi e Transizione al Digitale

Progetto PNRR: M1C1I1.5 “Cybersecurity” formazione tecnica

Cosa troverai in questa brochure

Sommario

Introduzione

Negli ultimi anni, i **social network** hanno cambiato profondamente il modo in cui le persone comunicano, diventando strumenti centrali nella vita quotidiana tramite cui condividere passioni ed eventi importanti della propria vita. Allo stesso modo anche **Enti, Società e Pubbliche Amministrazioni** li utilizzano sempre più per promuovere servizi, raccontare attività e creare un **dialogo diretto con i cittadini**, volto ad intercettarne bisogni, istanze e nuove sensibilità.

La divulgazione delle informazioni tramite social network da un lato consente di ridurre le distanze tra Enti e cittadini, dall'altro aumenta la potenziale **superficie di attacco** per criminali informatici.

L'elevato livello di esposizione e la natura aperta di tali piattaforme, come descritto precedentemente, rendono i social network un vettore privilegiato per **attacchi informatici**. Gli utenti condividono informazioni che possono essere **raccolte** e **manipolate** dagli attaccanti. Indipendentemente dall'uso personale o professionale, in Italia i social network maggiormente utilizzati sono **WhatsApp**, **Instagram**, **Facebook** e **TikTok**.

Lo sapevi?

In Italia si contano circa 43 milioni di utenti attivi sulle piattaforme di social network.*

Perché i Social Network sono pericolosi?

Un esempio di attacco Phishing tramite «**Instagram**»

L'attaccante crea un **profilo Instagram** apparentemente legittimo.

Invia una **richiesta di messaggio** alla vittima designata.

Il messaggio ha un testo per incuriosire la vittima, con un **link malevolo**.

La vittima clicca sul **link** e **inserisce** le sue credenziali o dati personali.

***Fonte:** ANSA - TikTok most used social media platform in Italy

Quali sono i rischi?

La crescente **diffusione dei social network** ha contribuito all'emergere di modalità specifiche di attacco informatico, incrementando in modo significativo il livello di esposizione ai rischi, quali:

Violazione dei dati

Una **navigazione poco consapevole** sui Social Network potrebbe esporre l'utente ad attacchi mirati di ingegneria sociale, esponendola a possibili **frodi** e truffe informatiche di vario genere e natura. L'attaccante, induce l'utente a **rivelare dati personali** o eseguire azioni non sicure.

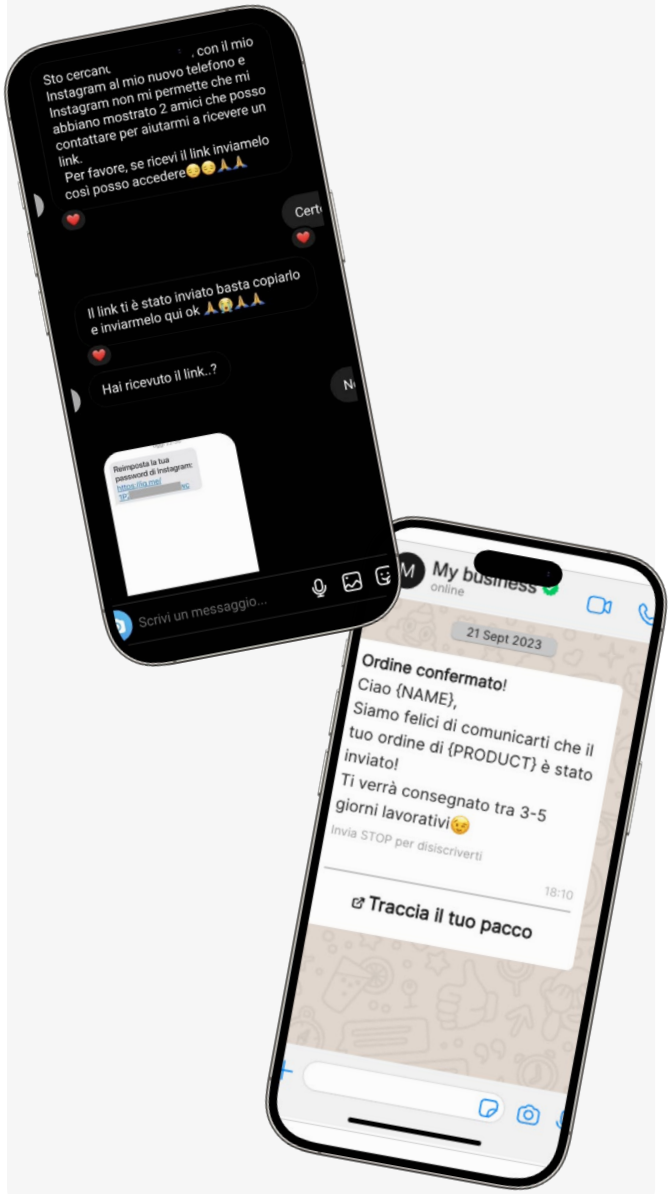
Furto d'identità

La condivisione di **dati personali** ed informazioni considerate come sensibili (es. numeri di carta di credito, password, etc.) potrebbe comportare una maggiore esposizione ad essere soggetti a **furti di identità online**. Questo espediente è infatti spesso utilizzato dai criminali informatici per compiere **attività illecite** di varia natura.

Diffusione Malware

Un **utilizzo imprudente** dei **Social Network** può diventare un canale per la propagazione di **malware:** programmi dannosi mirati ad intaccare la sicurezza dei dati e dispositivi. Gli utenti sui Social possono infatti essere indotti ad aprire link pubblicati come **post** o inviati tramite **messaggi,** che contengono software pericolosi.

Esempi reali di attacchi informatici tramite Social Network e app di messaggistica



Come difendersi?

Attraverso l'acquisizione delle credenziali di accesso, l'attaccante assume il controllo di un profilo social. L'**account compromesso** può essere utilizzato per lanciare ulteriori attacchi, truffare i contatti, diffondere malware o effettuare richieste fraudolente.

Imposta password uniche per ogni piattaforma e attiva l'**autenticazione multi-fattore** (MFA) con app come Google o Microsoft Authenticator.

I social network possono favorire tecniche di **social engineering**. La pubblicazione di dati sensibili come foto, abitudini o dettagli lavorativi può essere sfruttata dagli hacker per costruire **attacchi mirati** e ingannare gli utenti.

Durante la creazione dell'account, inserisci le **informazioni strettamente necessarie** e limita il **tracciamento** delle **azioni** durante la navigazione.

Uno degli attacchi che fa leva sul social engineering è il **phishing**, che sfrutta le informazioni personali condivise sui social per confezionare messaggi ingannevoli. I contenuti appaiono credibili perché basati su dati reali, aumentando così il rischio che l'utente clicchi su link malevoli.

Non condividere dati personali o sensibili (*es.* interessi, localizzazione, opinioni politiche) e **non** cliccare sui link provenienti da account sospetti.

Il **catfishing** è una tecnica di inganno che consiste nella creazione di **profili falsi** sui social network, utilizzando identità rubate o inventate. L'attaccante entra in contatto con le vittime fingendosi una persona affidabile, con l'obiettivo di richiedere informazioni personali e/o sensibili.

Imposta i profili social come **privati** e, in caso di messaggi sospetti, **blocca** l'account mittente e **segnalalo** alla piattaforma.

Security Trends

Marzo 2025

Furto di account Telegram e attacchi Smishing a tema INPS

Con un comunicato pubblicato nel mese di marzo 2025, il CERT-AGID ha segnalato una truffa informatica che coinvolge **falsi bot su Telegram**, mascherati da servizio "*Safeguard*", noto per la sicurezza nelle criptovalute.

I bot guidano l'utente in una **finta verifica** durante la quale, tramite la scansione di un QR code, l'attaccante ottiene l'**accesso all'account** Telegram della vittima.

Inoltre, è stato rilevato che il dominio utilizzato per ospitare i bot è collegato ad un gruppo di hacker noto per svolgere degli **attacchi di Smishing** (Phishing via sms) a tema INPS: attraverso link fraudolenti, l'utente viene reindirizzato su siti che imitano l'Ente previdenziale.

La truffa unisce **due tecniche** di attacco informatico distinte (**furto di account** e **smishing**) con l'obiettivo di compromettere identità digitali e rubare informazioni sensibili, sfruttando la fiducia degli utenti e l'aspetto legittimo delle piattaforme utilizzate.

Fonte: CERT-AGID - Furto account Telegram e Smishing Attack

Agosto 2024

Truffa delle false offerte di lavoro tramite Instagram e Telegram

Ad Agosto 2024 la **Polizia Postale** ha riferito che attraverso vari social network dedicati alla **messaggistica** è stato recapitato a diversi utenti un **messaggio** che riporta "Ciao! Mi dispiace disturbarla! Posso avere un po' del tuo tempo?".

Secondo l'allerta della Polizia Postale, si tratta di un **tentativo di truffa sempre più diffuso**. Il messaggio arriva da una presunta **reclutatrice** che propone un **impiego part-time**: seguire profili **Instagram**, mettere "**mi piace**" a dei contenuti e inviare **screenshot** come prova.

In cambio, **si promettono guadagni** tra i 100 e i 500 euro al giorno, con pagamento tramite **PayPal** o **Postepay**. Inizialmente, i truffatori inviano piccoli compensi per guadagnare la fiducia della vittima. Poi, con varie scuse, **chiedono il versamento di denaro** per sbloccare i guadagni, partecipare a corsi o firmare falsi contratti. In altri casi vengono richiesti **dati personali o bancari**.

La Polizia Postale raccomanda di **non rispondere** a messaggi da mittenti sconosciuti, **bloccare** i contatti sospetti e **non cliccare su link** che potrebbero compromettere il dispositivo.

Fonte: Polizia di Stato - Messaggio truffa su Telegram per chi cerca lavoro

In arrivo nel prossimo Journal

Ransomware

Il Malware che attacca
e tiene in ostaggio i
tuoi dati

Per segnalare possibili minacce o problemi di sicurezza, od eventuali temi che vorresti approfondire scrivi a:

sistemi.informativi@regione.molise.it

Il presente Cyber Security Journal e tutti gli altri contenuti informativi a tema sicurezza informatica, sono disponibili all'interno dell'intranet di Regione Molise al seguente link:

"PERSONALE"