

06.02.2026

OSINT e furto dell'identità – quando pubblicare i propri dati diventa un pericolo

Oggi accedere alle informazioni personali è più facile che mai. Non tutti sanno, però, che i criminali informatici utilizzano in modo mirato l'Open Source Intelligence (OSINT) per collezionare identità, creare profili e preparare truffe. In combinazione con il furto di identità, si tratta di una minaccia seria.

Che cos'è l'Open Source Intelligence (OSINT)?

Per OSINT si intende la raccolta e l'analisi sistematica di informazioni accessibili al pubblico. Non si tratta di dati hackerati, ma di contenuti che si trovano liberamente su Internet. Spesso sono le stesse persone a pubblicarli. Presi singolarmente, in genere appaiono innocui, ma combinati tra loro possono produrre un profilo personale ben dettagliato.

Tra le tipiche fonti di OSINT ci sono:

- Social network (Facebook, Instagram, TikTok, ecc.)
- Registri ed elenchi pubblici
- Siti Internet, forum e commenti
- Immagini, video e metadati
- Precedenti fughe di dati e set di dati pubblicati

Come funziona l'OSINT nella pratica?

I criminali informatici utilizzano l'OSINT in modo mirato e strutturato. Come prima cosa collezionano informazioni liberamente accessibili come nome, indirizzo e-mail, numero di telefono o nome utente. Successivamente, combinano tra loro questi dati valutando i contenuti dei social media, come post, foto o commenti. In questa analisi confluiscono anche informazioni su datori di lavoro, hobby o destinazioni frequenti. Da questa moltitudine di dettagli apparentemente innocui nasce così, poco alla volta, il profilo completo di una persona, dal quale si possono evincere abitudini, contatti sociali e relazioni di fiducia. Su questa base, i malintenzionati preparano attacchi mirati, come tentativi di truffa particolarmente credibili o furti di identità. Bisogna sottolineare che tutta l'operazione si basa su informazioni legalmente accessibili, benché gli scopi siano illegali.

Come ridurre il rischio di OSINT

Una protezione completa contro gli attacchi basati sull'OSINT è quasi impossibile, ma il rischio si può ridurre notevolmente. La cosa più importante è controllare regolarmente le impostazioni sulla privacy sui social network e condividere le informazioni personali con attenzione e in scarsa quantità. Anche i profili, i post e le foto più vecchi andrebbero controllati periodicamente e, se necessario, eliminati. Inoltre, si consiglia di non utilizzare gli stessi indirizzi e-mail e nomi utente su più piattaforme. Infine, bisogna fare particolare attenzione se si ricevono richieste o messaggi contenenti molti dettagli personali. La regola generale è questa: meno dati sono accessibili al pubblico,

più sarà difficile usarli in modo improprio.

In conclusione

L'OSINT mostra l'impatto che possono avere le informazioni pubblicamente accessibili, nel bene e nel male. Nelle mani sbagliate diventano la base per compiere furti dell'identità e truffe mirate. Essere consapevoli delle tracce che si lasciano online è il primo passo per rafforzare in modo duraturo la propria sicurezza digitale.