

Social engineering

Per ottenere informazioni riservate i criminali sfruttano spesso la buona fede, la disponibilità o l'insicurezza delle persone. Che si tratti di telefonate fittizie, falsi agenti di polizia o attacchi di phishing, nel social engineering il mirino è sempre puntato sulla persona. La protezione migliore è la «sana sfiducia».

Protegetevi dagli attacchi di social engineering così:

- Comunicate il minor numero possibile di informazioni personali su di voi. Sui social network, in particolare, è opportuno agire con grande cautela nella pubblicazione di informazioni.
- In generale non comunicate mai a un'altra persona password o codici, come i PIN delle vostre carte o i dati d'accesso all'Online Banking. I dati d'accesso e i codici PIN appartengono solo e soltanto a voi!
- Siate sospettosi quando ricevete richieste di informazioni via e-mail o al telefono, soprattutto se venite messi sotto pressione. Anche le e-mail di mittenti conosciuti e le telefonate da numeri noti possono essere falsificate!

Gli attacchi di social engineering mirano spesso a strapparvi informazioni personali o riservate (come dati di accesso, password ecc.) per utilizzarle poi illecitamente.

I criminali cercano come prima cosa di raccogliere la maggior quantità possibile di informazioni sulla vittima. Servendosi di queste informazioni sarà infatti più semplice ingannarla. Per esempio, il criminale potrebbe poi presentarsi come una persona che conoscete.

Lo strumento ideale per raccogliere informazioni è Internet. Soprattutto su [reti sociali](https://www.ebas.ch/it/media-e-reti-sociali/) (https://www.ebas.ch/it/media-e-reti-sociali/) come Facebook, LinkedIn, Instagram e simili si trovano enormi quantità di informazioni personali che possono essere utili a chi sferra l'attacco per avvicinarsi a una persona in modo mirato e apparire affidabile.

In generale, solo una sana dose di sfiducia protegge contro le persone che non conoscete – ma anche contro quelle che pensate di conoscere. Spesso è utile chiedersi, ad esempio, che tipo di informazioni si rendono pubbliche su di sé e a chi.

Interrompere la comunicazione in caso di sospetti

Se venite contattati inaspettatamente o se qualcosa vi sembra sospetto in generale, non rivelate ulteriori informazioni e interrompete la comunicazione. In caso di sospetti sul servizio e-banking non comunicate nulla e informate immediatamente il vostro istituto finanziario. I recapiti si trovano [qui](https://www.ebas.ch/it/partner/) (https://www.ebas.ch/it/partner/).

Esempi di attacchi di social engineering

- Ricevete un'e-mail che vi invita ad aprire un link ed effettuare l'accesso su un sito Internet, oppure a fornire informazioni personali.
- Una persona vi telefona e desidera porvi certe domande per un sondaggio (p. es. sul reddito, sulle misure di sicurezza adottate per il vostro computer ecc.).
- Un hacker falsifica il mittente di un'e-mail presentandosi come una persona nota (è possibile che l'allegato contenga un malware).

- Ricevete un'e-mail dal vostro capo che vi chiede di effettuare un pagamento urgente.
- Alla vostra postazione di lavoro si presenta una persona che si spaccia per un tecnico e vi fa credere di dover eseguire dei lavori di manutenzione sul vostro computer.
- Una persona si finge un tecnico (ad es., di una compagnia telefonica o elettrica ecc.) e cerca di accedere al vostro computer, alla vostra casa o alla vostra azienda.
- Chi sferra un attacco di social engineering può giungere persino al punto di candidarsi per ottenere un impiego mirato in un'impresa e impadronirsi poi di informazioni specifiche.

Il social engineering è un metodo che prevede l'uso di espedienti psicologici mirati per manipolare le persone con l'obiettivo di ottenere informazioni sensibili o innescare determinati comportamenti. A tal fine vengono utilizzati deliberatamente la fiducia, la pressione o l'inganno. La manipolazione spesso passa inosservata e può colpire chiunque. È quindi importante essere vigili e proteggere i propri dati personali.



«Sembrava così urgente che non ho controllato...»

Le storie che iniziano così non finiscono mai bene.

Se ricevete una richiesta inaspettata o sospetta, interrompete la comunicazione. Informatevi per evitare le frodi. www.ebas.ch

eBanking ma sicuro!
by Hochschule Luzern