MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Cyber Security Brochure

L'arte dell'inganno

Cos'è e come funziona il Social Engineering

Sommario

Cosa troverai in questa brochure

Introduzione

Negli ultimi anni, l'evoluzione dei sistemi digitali ha trasformato il modo in cui comunichiamo, lavoriamo e accediamo ai servizi online.

In questo contesto, il **Social Engineering** è diventata una delle minacce più diffuse, poiché sfrutta il fattore umano anziché le vulnerabilità di tipo tecnologico.

Attraverso **interazioni apparentemente legittime**, gli attaccanti cercano di ottenere la **fiducia** delle persone per indurle a compiere azioni che favoriscono il successo dell'inganno. Dettagli personali condivisi con leggerezza, o semplici **informazioni rese pubbliche**, possono essere utilizzate e sfruttate per condurre **attacchi mirati** idonei a **compromettere** la **sicurezza** delle **informazioni**.

Comprendere la natura del Social Engineering e riconoscere la facilità con cui può insinuarsi nelle comunicazioni digitali è il primo passo per sviluppare **maggiore consapevolezza** e adottare comportamenti più attenti nelle interazioni online.

Evoluzione attacchi di Phishing e Social Engineering 2020-2024

+35% La loro diffusione è aumentata del 35% nel 2024 rispetto agli anni precedenti.

Il **fattore umano** rimane la principale causa di rischio, essendo coinvolto nell'**80-90%** degli attacchi informatici.

Le caratteristiche principali del Social Engineering

Sfruttamento delle informazioni pubbliche: Dati reperiti online vengono analizzati per creare messaggi personalizzati e ad alto tasso di successo.

Manipolazione psicologica: L'attaccante sfrutta emozioni, fiducia e comportamenti abituali per indurre la vittima a compiere azioni dannose.

Apparenza di legittimità: Gli attacchi si presentano come comunicazioni reali, credibili e coerenti con il contesto della vittima.

Compromissione e persistenza: Il criminale informatico esfiltra i dati personali della vittima e potrebbe riutilizzarli per compiere attacchi più sofisticati.

Fonti: Rapporto CLUSIT 2025

Non cadere nell'inganno!

Rischi

01 Raccolta invisibile e progressiva di informazioni

Gli attaccanti non colpiscono mai in modo casuale, ma sono soliti **raccogliere informazioni** su di te passo dopo passo. Dati come il tuo **ruolo lavorativo**, le tue **abitudini** o i **contenuti** che condividi online, se combinati, permettono di creare un profilo molto dettagliato. Questo processo invisibile rende gli attacchi convincenti e difficili da riconoscere.

02 Manipolazione psicologica

Gli attaccanti studiano il tuo linguaggio, le tue abitudini e i tuoi **punti deboli** al fine di **convincerti ad effettuare azioni dannose**. Attraverso e-mail, messaggi o telefonate ti inducono infatti a compiere azioni che normalmente eviteresti: cliccare link sospetti, aprire allegati potenzialmente malevoli, rivelare dati personali o concedere autorizzazioni di accesso.

03 Furto di credenziali

Attraverso pagine di login **create con artificio**, i criminali possono indurti a rivelare **dati sensibili** come credenziali di accesso, PIN e altre informazioni riservate. Una volta ottenuti, i truffatori possono accedere a servizi intestati a tuo nome e compiere azioni illecite, ad esempio operare su conti ed effettuare bonifici o impersonificarti per compiere ulteriori **attività fraudolente**. Inoltre, se utilizzi la stessa password compromessa per più account, l'accesso illecito potrebbe estendersi anche ad altri sistemi e servizi.

Contromisure

Evita di pubblicare sui social, forum o altre piattaforme pubbliche foto di badge, documenti o **qualsiasi** altro **contenuto** che possa permettere a qualcuno di **risalire** ad **informazioni altamente confidenziali o private**.

Quando una comunicazione ti appare **sospetta** o ti induce ad agire in un periodo di tempo limitato, **verifica** attentamente la **legittimità** della richiesta prima di interagire.

Non fornire password, codici o **dati sensibili** via e-mail, chat o telefono. Quando accedi ai servizi online, scegli **password complesse** e attiva l'**autenticazione a più fattori** (**MFA**) se disponibile.

Come difendersi?

Condivisione limitata

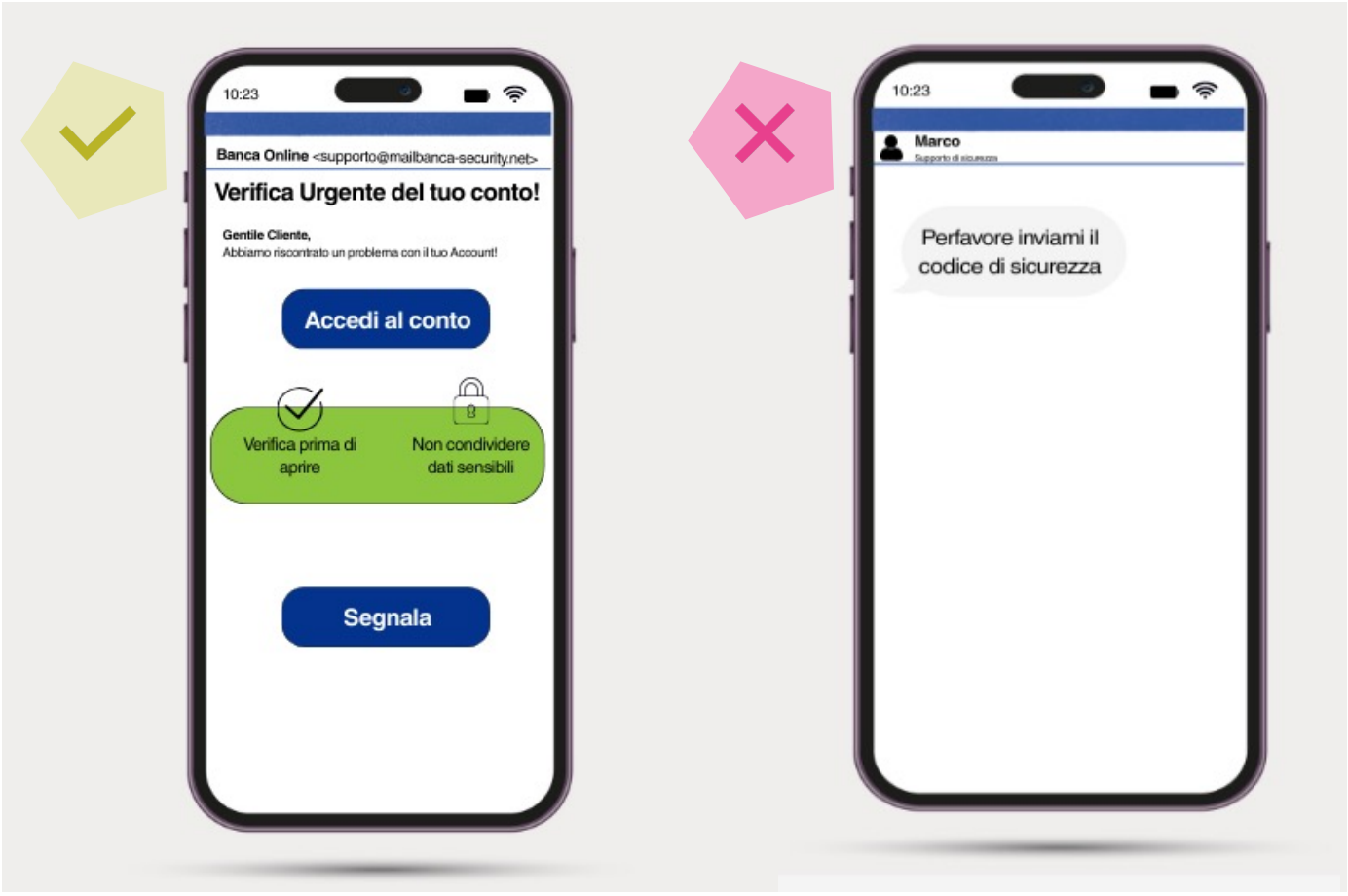
Nelle interazioni online **limita la diffusione di informazioni** personali e professionali. Ridurre **l'esposizione informativa** contribuisce a diminuire il rischio di subire attacchi di tipo Social Engineering, rendendo più **difficile sfruttare elementi** reali per simulare richieste legittime.

Verifica del contesto

Quando ricevi messaggi, e-mail o comunicazioni presta sempre attenzione al **tono** utilizzato. Richieste caratterizzate da **urgenza** immotivata, formalismi incoerenti rispetto al contesto o un' eccessiva confidenzialità potrebbero rappresentare un **segnale** di **comunicazioni malevole**.

Segnala anomalie

Se ricevi messaggi sospetti o noti comportamenti insoliti online, non ignorarli. **Avvisa** subito la persona o contatta direttamente l'Ente o l'azienda attraverso i canali ufficiali. Una **segnalazione tempestiva** può aiutare a prevenire problemi, proteggere dati e persone.



Security Trend

Campagna malevola via e-mail a nome del Direttore Generale ACN

Nel luglio 2025 è stata rilevata una **campagna** di **phishing** veicolata tramite **e-mail**, che ha sfruttato indebitamente il **nome** del **Direttore** Generale dell'Agenzia per la Cybersicurezza Nazionale (**ACN**).

Al fine di conferire apparente **ufficialità** e **autorevolezza** alla comunicazione, il messaggio risultava inviato da un indirizzo e-mail privato, ma riportava nel campo mittente nome e cognome del Direttore Generale, accompagnati dalla sua qualifica istituzionale. Tale tecnica costituisce un tipico espediente di **spoofing identitario**, volto a indurre il **destinatario** ad **attribuire legittimità** alla comunicazione sulla base del ruolo evocato.

Per quanto riguarda invece il contenuto dell'e-mail, lo stesso informava l'utente dell'esistenza di un presunto "**reato informatico**" a suo carico, connesso alla visualizzazione di contenuti illeciti, prospettando l'emissione di un'ordinanza dell'autorità giudiziaria e l'avvio di **azioni legali** in caso di **mancata risposta** entro un termine **ristretto** di 24 ore.

L'utilizzo strumentale di una figura istituzionale di alto profilo, unitamente a presunte ritorsioni giudiziarie e all'imposizione di un termine di risposta particolarmente ristretto, costituisce un **chiaro indicatore dell'impiego** di **tecniche** di **Social Engineering**.

luglio 2025

Truffa del "voto alla ballerina" su WhatsApp

Nel febbraio 2026 è stata rilevata una **campagna di phishing** diffusa tramite WhatsApp, conosciuta come "**voto alla ballerina**". Il **messaggio**, apparentemente proveniente da un **contatto** già presente in **rubrica,** quindi percepito come **affidabile**, invitava a **cliccare** su un **link** per sostenere una bambina in un presunto concorso di danza.

Il collegamento rimandava a una **pagina web** che richiedeva **l'inserimento** del **numero** di **telefono** e di un **codice OTP** ricevuto via SMS. La comunicazione di tali informazioni consentiva agli attaccanti di **appropriarsi dell'account** WhatsApp della **vittima**. Una volta ottenuto l'accesso, i malintenzionati inviavano **messaggi** ai **contatti** della rubrica simulando **situazioni** di **emergenza** e richiedendo **trasferimenti** di **denaro** urgenti. Nel frattempo, il legittimo titolare dell'account, estromesso dal proprio profilo, non era nelle condizioni di avvisare tempestivamente amici e familiari.

L'episodio rappresenta un caso emblematico di **Social Engineering**, in quanto l'attacco fa leva sulla **fiducia** tra **contatti conosciuti** e sul **coinvolgimento emotivo** legato a una presunta iniziativa che riguarda una bambina. Attraverso queste leve, la vittima viene indotta ad **abbassare** il **livello** di **attenzione** ed interagire con e-mail fraudolente.

febbraio 2026

MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Restate sintonizzati:

nuovi approfondimenti sulla cybersecurity vi aspettano nelle prossime pubblicazioni.