Il **social engineering** è una forma di attacco che sfrutta l'interazione umana e le debolezze psicologiche per ingannare le persone e ottenere informazioni sensibili o accesso non autorizzato a sistemi o dati. Piuttosto che cercare di violare direttamente le protezioni tecnologiche, gli attaccanti manipolano le persone per farle rivelare informazioni o compiere azioni che compromettono la sicurezza.

**Tecniche più comuni di social engineering:**

1. **Phishing**:
   * **Descrizione**: È una tecnica che consiste nell'invio di email o messaggi che sembrano provenire da fonti affidabili, come banche, servizi di pagamento o aziende conosciute. Gli attaccanti cercano di convincere le vittime a cliccare su link malevoli o a fornire informazioni personali, come password, numeri di carte di credito o altre credenziali sensibili.
   * **Esempio**: Ricevi un'email che sembra provenire dalla tua banca, con un messaggio urgente che richiede di verificare il tuo conto. Cliccando sul link, vieni indirizzato a una pagina web falsa che cattura le tue credenziali.
2. **Spear Phishing**:
   * **Descrizione**: Variante più mirata del phishing. L'attaccante personalizza il messaggio basandosi su informazioni specifiche della vittima, rendendo l'inganno più credibile.
   * **Esempio**: Un dipendente di un'azienda riceve un'email apparentemente dal suo superiore con una richiesta urgente di fornire dati aziendali riservati.
3. **Vishing** (Voice Phishing):
   * **Descrizione**: Gli attaccanti utilizzano chiamate telefoniche per convincere le vittime a rivelare informazioni personali o finanziarie.
   * **Esempio**: Una telefonata da qualcuno che si finge impiegato di un istituto bancario e chiede informazioni sulla tua carta di credito per risolvere un "problema urgente".
4. **Tailgating (o Piggybacking)**:
   * **Descrizione**: L'attaccante si introduce fisicamente in un'area riservata, seguendo qualcuno che ha l'accesso autorizzato, spesso passando dietro di loro in momenti di distrazione o confusione.
   * **Esempio**: Un attaccante si posiziona vicino all'ingresso di un edificio aziendale e, fingendo di aver dimenticato il badge, segue un dipendente che gli apre la porta.
5. **Pretexting**:
   * **Descrizione**: In questa tecnica, l'attaccante inventa uno scenario falso (pretesto) per convincere la vittima a rivelare informazioni sensibili. L'attaccante potrebbe fingersi un'autorità o una figura di fiducia per creare credibilità.
   * **Esempio**: Un attaccante si spaccia per un dipendente del reparto IT dell'azienda e chiede informazioni come password per "aggiornare il sistema".
6. **Baiting**:
   * **Descrizione**: Gli attaccanti utilizzano esche fisiche o digitali per attirare le vittime a compiere azioni dannose. Un esempio classico è lasciare una chiavetta USB infetta in un luogo pubblico, sperando che qualcuno la raccolga e la inserisca nel proprio computer.
   * **Esempio**: Un dipendente trova una chiavetta USB etichettata come "Confidenziale" nel parcheggio dell'azienda e la collega al proprio computer, permettendo all'attaccante di infettare la rete aziendale.

Queste tecniche sfruttano la fiducia, la curiosità e la mancanza di consapevolezza delle vittime. Per difendersi, è importante mantenere sempre un alto livello di sospetto, verificare l'autenticità delle comunicazioni e seguire le migliori pratiche di sicurezza.

**Difendersi dagli attacchi di social engineering**

Per difendersi dagli attacchi di **social engineering**, è fondamentale adottare una serie di strategie preventive e pratiche di sicurezza che aiutano a riconoscere e bloccare i tentativi di manipolazione. Ecco alcune strategie efficaci:

**1. Formazione e sensibilizzazione**

* **Descrizione**: Il primo passo per prevenire gli attacchi è educare le persone sui rischi e le tecniche del social engineering. I dipendenti e gli utenti devono sapere come identificare i segnali di potenziali truffe e attacchi.
* **Strategia**: Organizzare corsi di formazione periodici e campagne di sensibilizzazione che insegnano a riconoscere phishing, vishing, tailgating, e altre tecniche. Testare regolarmente i dipendenti con attacchi simulati per valutare il livello di preparazione.

**2. Verifica dell'identità**

* **Descrizione**: Prima di condividere informazioni o accettare richieste, è importante verificare sempre l'identità della persona con cui si interagisce.
* **Strategia**: Richiedere una doppia verifica tramite un canale alternativo (ad esempio, chiamare direttamente un collega o un superiore per confermare una richiesta ricevuta via email). Usare l'autenticazione a due fattori (2FA) per proteggere gli account online.

**3. Utilizzo di password forti e gestione sicura delle credenziali**

* **Descrizione**: Molti attacchi di social engineering mirano a ottenere le password o altre credenziali. È essenziale proteggere questi dati.
* **Strategia**: Utilizzare password complesse e uniche per ogni account. Cambiare regolarmente le password e utilizzare un **password manager** per gestirle in modo sicuro. Implementare l'uso dell'autenticazione multi-fattore (MFA) per aggiungere un ulteriore livello di protezione.

**4. Diffidare delle richieste di informazioni sensibili**

* **Descrizione**: Gli attacchi di social engineering spesso coinvolgono richieste di informazioni personali o aziendali sotto pretesti falsi.
* **Strategia**: Non fornire mai informazioni sensibili come password, numeri di conto o dati personali senza aver verificato l'autenticità della richiesta. Le aziende e le istituzioni affidabili non chiedono mai informazioni sensibili via email o telefono senza una previa autorizzazione.

**5. Implementazione di controlli fisici di sicurezza**

* **Descrizione**: Gli attacchi come il **tailgating** si basano su una mancata attenzione alla sicurezza fisica.
* **Strategia**: Utilizzare badge, serrature elettroniche e telecamere di sicurezza per controllare gli accessi alle aree riservate. Incoraggiare i dipendenti a non far entrare persone sconosciute senza controllo, anche se sembrano legittime, e segnalare ogni comportamento sospetto.

**6. Segnalazione di incidenti e sospetti**

* **Descrizione**: Se qualcuno sospetta di essere stato vittima di un tentativo di social engineering, è fondamentale segnalarlo immediatamente.
* **Strategia**: Creare un sistema semplice e rapido per segnalare tentativi sospetti di attacco, con una risposta immediata da parte del team IT o di sicurezza. Le aziende dovrebbero adottare un approccio proattivo nel monitoraggio e rispondere velocemente agli incidenti.

**7. Evitare l'apertura di link o allegati sospetti**

* **Descrizione**: Molti attacchi di phishing cercano di far cliccare le vittime su link malevoli o di aprire allegati infetti.
* **Strategia**: Prima di aprire un allegato o cliccare su un link, controllare attentamente l'indirizzo del mittente e la coerenza del messaggio. Usare strumenti di scansione antivirus e anti-phishing, sia sui sistemi di posta elettronica che sui dispositivi personali.

**8. Implementazione di politiche di sicurezza aziendali**

* **Descrizione**: Le politiche di sicurezza strutturate possono aiutare a ridurre il rischio di social engineering, fornendo regole chiare su come trattare dati sensibili e reagire a possibili attacchi.
* **Strategia**: Definire linee guida precise su come gestire le comunicazioni e le interazioni esterne, l'uso di dispositivi USB, l'accesso a sistemi informatici, e stabilire protocolli di sicurezza per situazioni di emergenza. Promuovere il rispetto di queste regole in tutta l'azienda.

**9. Utilizzare filtri anti-phishing**

* **Descrizione**: I filtri anti-phishing possono rilevare e bloccare molti tentativi di phishing prima che raggiungano le vittime.
* **Strategia**: Implementare software di filtraggio email che identifichi e blocchi le email sospette. Utilizzare strumenti di sicurezza del browser che avvisano l'utente quando tenta di visitare siti web potenzialmente pericolosi.

**10. Backup regolari dei dati**

* **Descrizione**: Anche se un attacco riesce a compromettere un sistema, avere un backup riduce il danno e facilita il ripristino delle informazioni.
* **Strategia**: Creare backup regolari dei dati importanti e conservare queste copie in un ambiente sicuro, separato dal sistema principale. Questo garantisce che, anche in caso di compromissione, sia possibile recuperare i dati senza gravi perdite.

**11. Monitoraggio costante della rete e dei sistemi**

* **Descrizione**: Il monitoraggio in tempo reale dei sistemi e delle reti può aiutare a rilevare attività insolite causate da attacchi di social engineering.
* **Strategia**: Utilizzare strumenti di monitoraggio della sicurezza per rilevare comportamenti sospetti nei sistemi aziendali e reagire rapidamente a possibili compromissioni.

**Vulnerabilità più significative legate ai sistemi di infotainment dei veicoli Tesla**

**1. CVE-2023-32156 (ZDI-23-972)**

* **Descrizione**: Questa vulnerabilità riguarda il **Tesla Model 3** e consente a un attaccante, con accesso privilegiato, di eseguire codice arbitrario all'interno del sistema di infotainment. La falla sfrutta una cattiva gestione degli aggiornamenti firmware da parte del veicolo, in particolare dell'**ECU Gateway**. Se un attaccante riesce a manipolare l'aggiornamento, potrebbe compromettere il sistema, permettendo la modifica delle funzionalità principali del veicolo.
* **Dettagli tecnici**: L'attacco richiede un accesso fisico o remoto al veicolo e la capacità di interagire con il meccanismo di aggiornamento firmware. Una volta penetrato nel sistema, l'attaccante può eseguire codice arbitrario con privilegi elevati.
* **Soluzione**: Tesla ha risolto questa vulnerabilità con l'aggiornamento **firmware 2023.12**, che include misure di sicurezza più avanzate e una verifica più rigida durante il processo di aggiornamento ​([Zero Day Initiative](https://www.zerodayinitiative.com/advisories/ZDI-23-972/)).

**2. CVE-2022-3093**

* **Descrizione**: Questa vulnerabilità riguarda il meccanismo di aggiornamento firmware del sistema **ice\_updater** utilizzato sui veicoli Tesla. Il problema nasce dalla mancanza di una validazione appropriata del firmware fornito dall'utente, che potrebbe permettere a un attaccante fisico di installare un firmware malevolo ed eseguire codice arbitrario.
* **Dettagli tecnici**: Un attaccante con accesso fisico al veicolo potrebbe sfruttare il difetto per iniettare un firmware malevolo che non viene verificato correttamente, ottenendo accesso privilegiato al sistema e potenzialmente modificando il comportamento del veicolo.
* **Soluzione**: Tesla ha implementato un controllo più rigoroso sui pacchetti di aggiornamento firmware per garantire che solo firmware autenticato e firmato venga accettato dal sistema​ ([NVD](https://nvd.nist.gov/vuln/detail/CVE-2022-3093))​([MITRE CVE](https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=tesla)).

**3. CVE-2022-42431**

* **Descrizione**: Questa vulnerabilità permette l'escalation di privilegi sfruttando una falla nel driver **bcmdhd** utilizzato per la gestione della rete wireless. La mancanza di una corretta validazione della lunghezza dei dati forniti dall'utente prima di copiarli in un buffer può portare a un overflow del buffer stesso, permettendo l'esecuzione di codice arbitrario con privilegi root.
* **Dettagli tecnici**: L'attaccante deve prima ottenere la possibilità di eseguire codice nel contesto del sistema, ma una volta riuscito a sfruttare il difetto, può ottenere un controllo totale del sistema. Questa vulnerabilità può essere utilizzata per compromettere altri componenti del veicolo.
* **Soluzione**: Tesla ha rilasciato aggiornamenti per correggere la gestione del buffer nel driver **bcmdhd**, impedendo agli attaccanti di sfruttare questa vulnerabilità​ ([MITRE CVE](https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=tesla)).

**4. CVE-2022-23126**

* **Descrizione**: Riguarda TeslaMate, un sistema di monitoraggio e gestione delle Tesla. In una configurazione predefinita con Docker, gli attaccanti possono accedere alle API Tesla tramite Grafana e controllare il veicolo, inclusa l'apertura delle porte e l'avvio del veicolo in modalità Keyless Driving.
* **Dettagli tecnici**: Un attaccante che riesce a ottenere accesso al sistema Grafana, utilizzato per monitorare le Tesla, può sfruttare un'API vulnerabile per accedere alle funzioni principali del veicolo senza autenticazione adeguata.
* **Soluzione**: L'aggiornamento di TeslaMate alla versione 1.25.1 ha chiuso la falla e introdotto migliori meccanismi di autenticazione per impedire questo tipo di attacco ​([MITRE CVE](https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=tesla)).

**Considerazioni finali**

Molte delle vulnerabilità nei sistemi di infotainment di Tesla sono legate alla gestione inadeguata degli aggiornamenti firmware o a errori nella validazione dei dati, permettendo l'esecuzione di codice malevolo con privilegi elevati. Tesla ha affrontato queste vulnerabilità con aggiornamenti firmware regolari che includono controlli di sicurezza più rigorosi. Mantenere il software aggiornato è cruciale per garantire la sicurezza del veicolo.