

Tecniche di Social Engineering



In questa chat andremo ad analizzare le tecniche di social engineering utilizzate dagli attaccanti per manipolare le persone e ottenere informazioni sensibili o accesso non autorizzato a sistemi e dati. Per cominciare, quali sono le tecniche di social engineering più utilizzate (e più problematiche) nel 2024?



Nel 2024, le tecniche di social engineering sono sempre più sofisticate e mirate, sfruttando non solo le debolezze umane, ma anche l'accesso alla crescente quantità di dati personali e informazioni disponibili online. Ecco alcune delle tecniche più comuni e problematiche:

1. **Phishing avanzato:** I classici tentativi di phishing, via e-mail o messaggi, sono stati migliorati per risultare molto più personalizzati (spear phishing) e difficili da individuare. Con l'uso di AI e Big Data, gli attaccanti possono personalizzare i messaggi in base a dettagli specifici, rendendo le comunicazioni altamente credibili.
2. **Vishing e Smishing (Voice e SMS Phishing):** Questi attacchi, realizzati tramite chiamate telefoniche o messaggi SMS, sono in aumento, soprattutto ora che le tecnologie di spoofing rendono facile mascherare numeri di telefono per farli sembrare autentici. Con una finta urgenza, gli attaccanti chiedono dati personali o finanziari, soprattutto targettizzando utenti di piattaforme bancarie.
3. **Attacchi di impersonificazione sui social media:** Con la mole di informazioni personali accessibili sui social media, gli attaccanti sono in grado di impersonare amici, colleghi, o addirittura capi, richiedendo informazioni confidenziali o favori con pretesti credibili.
4. **Pretexting (Pretesto):** Qui, l'attaccante si presenta con una storia credibile o una specifica identità (ad esempio, fingendo di essere del team IT interno) per convincere la vittima a fornire informazioni riservate. Questo metodo è particolarmente efficace in ambienti aziendali e spesso usato per ottenere accessi fisici o a sistemi protetti.
5. **Baiting (Esca):** Questa tecnica fa leva sulla curiosità, come file USB lasciati in luoghi pubblici, che contengono malware o link a siti compromessi. Nel 2024, la versione digitale di questo attacco avviene anche tramite link di download in messaggi che offrono gratuitamente software o risorse "allettanti".
6. **Attacchi via QR code:** Con la diffusione dei QR code per molti servizi (ad esempio, nei pagamenti e nei biglietti), gli attaccanti li utilizzano per reindirizzare le vittime a siti fraudolenti. Vengono sovrapposti falsi QR code su quelli originali in luoghi pubblici, come stazioni e ristoranti.
7. **Deepfake e Video Call Phishing:** L'uso dei deepfake per creare video e audio realistici ha reso possibile nuovi attacchi di social engineering, in cui l'attaccante si finge una persona conosciuta

attraverso video call o messaggi vocali. Questi attacchi mirano spesso a ottenere autorizzazioni di pagamento o accessi di alto livello.

Misure di Difesa

Le difese migliori restano la consapevolezza e la formazione continua sugli ultimi metodi di attacco. Altre misure includono l'autenticazione a due fattori, l'uso di strumenti di rilevamento di phishing avanzato, la sensibilizzazione sul controllo delle fonti di messaggi e la verifica delle identità tramite canali secondari (ad esempio, chiamate dirette).



Molto bene. Per tutti e 7 i metodi di social engineering illustrati, fai un esempio realistico su come un attaccante potrebbe utilizzare quella tecnica e a quale scopo.



Ecco come un attaccante potrebbe utilizzare ciascuna delle sette tecniche di social engineering elencate:

1. Phishing avanzato

Esempio: Un dipendente di una grande azienda riceve un'email apparentemente da un fornitore di fiducia, che include dettagli precisi sui loro ultimi ordini. L'email sembra legittima e chiede al destinatario di cliccare su un link per "verificare la fattura" o "aggiornare il metodo di pagamento". La pagina di accesso a cui conduce è una copia del sito ufficiale, progettata per rubare le credenziali aziendali del dipendente.

Scopo: Rubare le credenziali del dipendente per accedere a risorse aziendali, come l'ERP o i dati finanziari.

2. Vishing e Smishing

Esempio: Un impiegato riceve una chiamata da una persona che si spaccia per un membro del dipartimento IT dell'azienda. Il finto operatore comunica all'impiegato che ci sono stati tentativi di accesso non autorizzati al suo account aziendale e che serve verificare l'identità tramite l'inserimento di un codice inviato via SMS. Tuttavia, il codice è in realtà un codice OTP (One-Time Password) inviato per confermare una transazione fraudolenta.

Scopo: Autorizzare transazioni o modificare credenziali di accesso, ottenendo così l'accesso a risorse aziendali sensibili.

3. Impersonificazione sui social media

Esempio: Un attaccante crea un profilo falso di un manager aziendale su LinkedIn o Facebook, utilizzando foto e dettagli personali accessibili pubblicamente. Poi invia un messaggio a un dipendente, richiedendo "in via confidenziale" informazioni su alcuni progetti in corso o chiedendo un aiuto finanziario temporaneo, suggerendo che non è stato possibile accedere a fondi aziendali.

Scopo: Estrarre informazioni riservate sui progetti in corso o sottrarre denaro con pretesti credibili.

4. Pretexting (Pretesto)

Esempio: Un attaccante si presenta come un rappresentante dell'assistenza clienti del fornitore di servizi IT della vittima, chiamando l'ufficio e dicendo di dover aggiornare i server. Per "verificare" le impostazioni attuali, chiede alla vittima le credenziali di accesso e l'indirizzo IP. La vittima, credendo sia una normale procedura, fornisce le informazioni.

Scopo: Ottenere l'accesso ai sistemi aziendali per rubare dati sensibili o installare malware.

5. Baiting (Esca)

Esempio: In un ufficio frequentato da dipendenti aziendali, un attaccante lascia una chiavetta USB con un'etichetta invitante come "Documenti finanziari" o "Rapporto sui bonus". La chiavetta contiene malware che infetta il computer non appena inserita, dando accesso all'attaccante alla rete aziendale.

Scopo: Infiltrare malware nella rete aziendale per esfiltrare dati, installare ransomware o ottenere accessi non autorizzati.

6. Attacchi via QR Code

Esempio: Un attaccante applica un falso QR code sopra quello reale su una locandina di un evento aziendale o in un ristorante frequentato da impiegati dell'azienda target. Il QR code indirizza le vittime a una pagina di login finta che replica il portale di un servizio comunemente usato, come Microsoft 365, per rubare le credenziali.

Scopo: Raccogliere credenziali di accesso per sfruttarle in un attacco successivo o venderle sul mercato nero.

7. Deepfake e Video Call Phishing

Esempio: Un dipendente del settore finanziario riceve una videochiamata apparentemente dal proprio direttore finanziario (CFO), che chiede con urgenza di autorizzare un pagamento verso un nuovo fornitore. Il deepfake è realistico, e l'urgenza convincente. Senza dubitare, il dipendente procede con la transazione.

Scopo: Indurre la vittima ad autorizzare un pagamento verso un conto controllato dall'attaccante.

Questi esempi evidenziano come la sofisticazione e la credibilità di ogni tecnica possano compromettere anche persone consapevoli dei rischi, sottolineando l'importanza di verifiche sempre più rigorose e multi-livello.



Poco fa hai menzionato i metodi di difesa. Oltre alla consapevolezza e alla formazione, quali sono le migliori tecniche di difesa? Illustra le tecniche di difesa per ogni tecnica di social engineering che hai illustrato.



Ecco le tecniche di difesa più efficaci contro ciascuna delle tecniche di social engineering descritte. Molte di queste includono strumenti tecnologici avanzati e best practices aziendali per limitare le vulnerabilità e migliorare la capacità dei dipendenti di riconoscere gli attacchi.

1. Difese contro il Phishing avanzato

- **Autenticazione Multi-Fattore (MFA):** Anche se un attaccante riesce a rubare le credenziali, l'uso di MFA rende più difficile il login, poiché richiede un secondo fattore di autenticazione.
- **Software di rilevamento del phishing:** I sistemi di e-mail aziendali dovrebbero includere un filtro anti-phishing avanzato, spesso basato sull'intelligenza artificiale, che analizza il contenuto, il mittente e gli allegati.
- **Politiche di verifica esterna dei link:** I dipendenti dovrebbero essere istruiti a verificare la destinazione di link sospetti e a evitare di inserire dati sensibili su pagine aperte da e-mail non verificate.

2. Difese contro il Vishing e Smishing

- **Politiche di verifica delle chiamate:** La formazione aziendale dovrebbe includere una politica che vieta di fornire informazioni sensibili su richiesta telefonica senza un protocollo di verifica dell'identità.
- **Protezione dei numeri aziendali e personali:** Limitare la diffusione dei numeri di telefono aziendali pubblicamente e informare i dipendenti sui rischi degli attacchi tramite SMS.
- **Autenticazione Out-of-Band:** Quando richiesto, confermare le richieste tramite un canale differente (ad esempio, email o tramite un'app aziendale sicura) per evitare che un attaccante possa condurre attacchi tramite telefonia.

3. Difese contro l'Impersonificazione sui social media

- **Monitoraggio dei social media aziendali:** Usare strumenti di monitoraggio per rilevare eventuali account falsi e segnalarli alle piattaforme.
- **Separazione delle informazioni personali e aziendali:** Incoraggiare i dipendenti a non pubblicare dettagli aziendali o relazioni di lavoro sui social, riducendo le informazioni a disposizione degli attaccanti.
- **Verifiche interne per richieste non abituali:** Se si riceve una richiesta di informazioni riservate o finanziarie, anche da colleghi conosciuti, è buona pratica verificarla direttamente con la persona, senza utilizzare i social media.

4. Difese contro il Pretexting

- **Politiche di autenticazione delle richieste interne:** Implementare protocolli di verifica interni per tutte le richieste di informazioni sensibili, soprattutto se provengono da fonti esterne o inusuali.
- **Autenticazione Multi-Fattore per accesso ai dati critici:** Rendere obbligatorio l'uso di MFA per accedere a dati e risorse aziendali di alto valore.
- **Consapevolezza del "principio del minimo privilegio":** Limitare l'accesso ai dati aziendali solo ai dipendenti che ne hanno effettivamente bisogno e sensibilizzare sull'importanza di non condividere informazioni al di fuori dei canali aziendali.

5. Difese contro il Baiting

- **Bloccare l'accesso automatico a dispositivi esterni:** Disabilitare il riconoscimento automatico di chiavette USB nei computer aziendali e richiedere che siano prima verificate tramite strumenti di sicurezza IT.
- **Campagne di sensibilizzazione sul rischio dei dispositivi sconosciuti:** Educare i dipendenti sui rischi di connettere dispositivi esterni non autorizzati e spiegare come verificare l'autenticità di un dispositivo.
- **Software di sicurezza endpoint:** Implementare soluzioni di protezione avanzata sugli endpoint (computer aziendali) per rilevare malware e attività sospette in caso di collegamento di dispositivi esterni.

6. Difese contro gli Attacchi via QR Code

- **Verifica manuale dei QR code:** Educare i dipendenti a verificare l'autenticità dei QR code, se possibile, accedendo al sito web dell'azienda direttamente tramite il browser invece di usare il QR code.
- **Scanner QR con protezione anti-phishing:** Fornire app per la scansione dei QR code con protezioni integrate contro i link malevoli.
- **Distribuzione sicura dei QR code aziendali:** Garantire che i QR code aziendali siano affissi in luoghi protetti e difficili da manomettere, evitando di posizionarli in luoghi pubblici o poco sorvegliati.

7. Difese contro i Deepfake e il Video Call Phishing

- **Verifica multi-fattoriale per richieste finanziarie:** Ogni richiesta di transazione dovrebbe richiedere conferme tramite più canali e coinvolgere più di una persona autorizzata per la verifica.
- **Utilizzo di tecnologie di rilevamento dei deepfake:** In caso di comunicazioni altamente sensibili, utilizzare software avanzati in grado di rilevare manipolazioni video e audio.
- **Politiche di riconferma interna:** Implementare una policy per verificare tutte le richieste di trasferimenti finanziari con il richiedente tramite un canale sicuro e diretto, come una chiamata telefonica.

Queste misure difensive, in combinazione con una solida cultura di sicurezza informatica, offrono un alto livello di protezione contro gli attacchi di social engineering e riducono significativamente il rischio di compromissione dei sistemi e delle informazioni aziendali.



Molto bene. Ora crea una presentazione che racchiude tutte le informazioni che mi hai fornito sul social engineering. Dividi la presentazione in 4 sezioni:

1. Che cos'è il social engineering e perché è una grande minaccia
2. Quali sono le tecniche di social engineering più diffuse e problematiche del 2024
3. Esempi pratici e realistici per ogni tecnica illustrata
4. Tecniche di difesa e best practice per ogni tecnica illustrata



Ecco una struttura per la presentazione sul social engineering:

Slide 1: Introduzione alla presentazione

- **Titolo:** Social Engineering: Tecniche, Esempi e Difese
 - **Sottotitolo:** Come proteggere dati e sistemi dalle minacce del social engineering nel 2024
 - **Obiettivi della presentazione:**
 - Comprendere cos'è il social engineering e perché è una minaccia crescente
 - Esplorare le tecniche di attacco più diffuse nel 2024
 - Analizzare esempi realistici di ogni tecnica
 - Apprendere le difese e le best practice contro questi attacchi
-

Sezione 1: Che cos'è il Social Engineering e Perché è una Grande Minaccia

- **Slide 2: Cos'è il Social Engineering?**
 - **Definizione:** Il social engineering è un insieme di tecniche manipolative utilizzate per ingannare le persone e ottenere informazioni sensibili o accesso non autorizzato a sistemi e dati.
 - **Obiettivi:** Rubare credenziali, accedere a sistemi interni, sottrarre denaro o informazioni riservate.
 - **Slide 3: Perché il Social Engineering è una Minaccia Maggiore nel 2024**
 - **Sofisticazione degli attacchi:** Utilizzo di AI, Big Data e tecnologie come i deepfake.
 - **Maggiore esposizione dei dati personali:** I social media e la condivisione online offrono agli attaccanti numerose informazioni per personalizzare gli attacchi.
 - **Costo per le aziende:** Violazioni di dati, perdite finanziarie, danni alla reputazione e costi di ripristino.
-

Sezione 2: Tecniche di Social Engineering più Diffuse e Problematiche nel 2024

- **Slide 4: Tecniche di Social Engineering nel 2024**
 - 1. Phishing avanzato
 - 2. Vishing e Smishing (Voice e SMS Phishing)
 - 3. Impersonificazione sui social media
 - 4. Pretexting (Pretesto)
 - 5. Baiting (Esca)
 - 6. Attacchi via QR Code
 - 7. Deepfake e Video Call Phishing
 - **Slide 5: Focus sulle Tecniche**
 - Descrizione sintetica di ciascuna tecnica con breve spiegazione di come funziona:
 - **Phishing avanzato:** Email personalizzate e altamente credibili
 - **Vishing e Smishing:** Chiamate e SMS falsificati che richiedono informazioni sensibili
 - **Impersonificazione:** Finti profili sui social per ottenere dati o denaro
 - **Pretexting:** Uso di pretesti credibili per ingannare le vittime
 - **Baiting:** Chiavette USB o file infetti per infiltrare malware
 - **QR Code:** QR falsificati per reindirizzare a siti compromessi
 - **Deepfake:** Video/audio manipolati per ottenere trasferimenti finanziari o dati
-

Sezione 3: Esempi Pratici e Realistici per Ogni Tecnica

- **Slide 6-7: Esempi Pratici di Attacchi**

- **Phishing avanzato:** Email da un fornitore "fidato" con link per accedere a una falsa pagina di login.
- **Vishing e Smishing:** Chiamata "dall'IT" che richiede un OTP per autorizzare una modifica di accesso.
- **Impersonificazione sui social:** Account falso di un manager che chiede informazioni confidenziali o supporto finanziario.
- **Pretexting:** Chiamata dal "fornitore IT" per ottenere credenziali e dettagli sulla rete.
- **Baiting:** Chiavetta USB "persa" contenente malware per accedere ai sistemi aziendali.
- **Attacchi via QR Code:** Falso QR in un ristorante che reindirizza a una pagina di phishing.
- **Deepfake:** Finto video del CFO che chiede un pagamento urgente verso un nuovo conto.

Sezione 4: Tecniche di Difesa e Best Practice per Ogni Tecnica

- **Slide 8: Difese Contro il Phishing Avanzato**

- **MFA:** Autenticazione a due fattori per proteggere gli accessi.
- **Software anti-phishing:** Filtri per rilevare e bloccare e-mail sospette.
- **Politiche di verifica dei link:** Verificare link e URL sospetti.

- **Slide 9: Difese Contro Vishing e Smishing**

- **Verifica delle chiamate:** Politiche di conferma dell'identità su richieste telefoniche.
- **Protezione dei numeri:** Limitare la condivisione dei numeri di telefono aziendali.
- **Autenticazione out-of-band:** Utilizzare canali alternativi per verificare le richieste.

- **Slide 10: Difese Contro l'Impersonificazione sui Social**

- **Monitoraggio dei social media:** Rilevamento di account falsi e impostazione di protocolli di segnalazione.
- **Separazione dati personali e aziendali:** Mantenere privata l'identità aziendale sui social.
- **Verifica interna per richieste non abituali:** Verificare ogni richiesta sensibile.

- **Slide 11: Difese Contro il Pretexting**

- **Autenticazione delle richieste interne:** Protocollo di verifica per richieste di informazioni sensibili.
- **MFA per dati critici:** Accesso con autenticazione avanzata a risorse sensibili.
- **Principio del minimo privilegio:** Limitare l'accesso ai dati solo al personale autorizzato.

- **Slide 12: Difese Contro il Baiting**

- **Bloccare l'accesso automatico a USB:** Disabilitare l'accesso automatico a dispositivi esterni.
- **Campagne di sensibilizzazione:** Informare sui rischi di dispositivi esterni sconosciuti.
- **Protezione endpoint:** Software avanzato per il rilevamento di malware.

- **Slide 13: Difese Contro Attacchi via QR Code**

- **Verifica dei QR:** Insegnare a verificare manualmente l'autenticità dei QR code.
- **Scanner QR protetto:** Fornire strumenti di scansione sicuri contro i link fraudolenti.
- **Distribuzione sicura:** Posizionare i QR in ambienti protetti.

- **Slide 14: Difese Contro Deepfake e Video Call Phishing**

- **Verifica per richieste finanziarie:** Richiedere la conferma di ogni richiesta finanziaria su più canali.
 - **Rilevamento deepfake:** Software per individuare manipolazioni video e audio.
 - **Politiche di riconferma interna:** Controllo diretto con la persona per confermare richieste di trasferimenti.
-

Slide 15: Conclusioni

- **Sintesi:** Il social engineering sfrutta le vulnerabilità umane per accedere a dati e sistemi.
 - **Strategie di difesa:** Combina tecnologie di sicurezza avanzate con consapevolezza e formazione.
 - **Best practice:** Monitorare le tendenze e aggiornare continuamente le misure di difesa.
 - **Q&A:** Domande e risposte per chiarimenti.
-

Questa struttura organizza i contenuti in modo chiaro e permette di guidare il pubblico attraverso le minacce, esempi pratici e difese, rendendo facile comprendere sia i rischi che le soluzioni.

ChatGPT può commettere errori. Considera di verificare le informazioni importanti.