**Mattia Montis**

# Social Engineering e Tecniche di difesa

## 1. Comprendere il Social Engineering

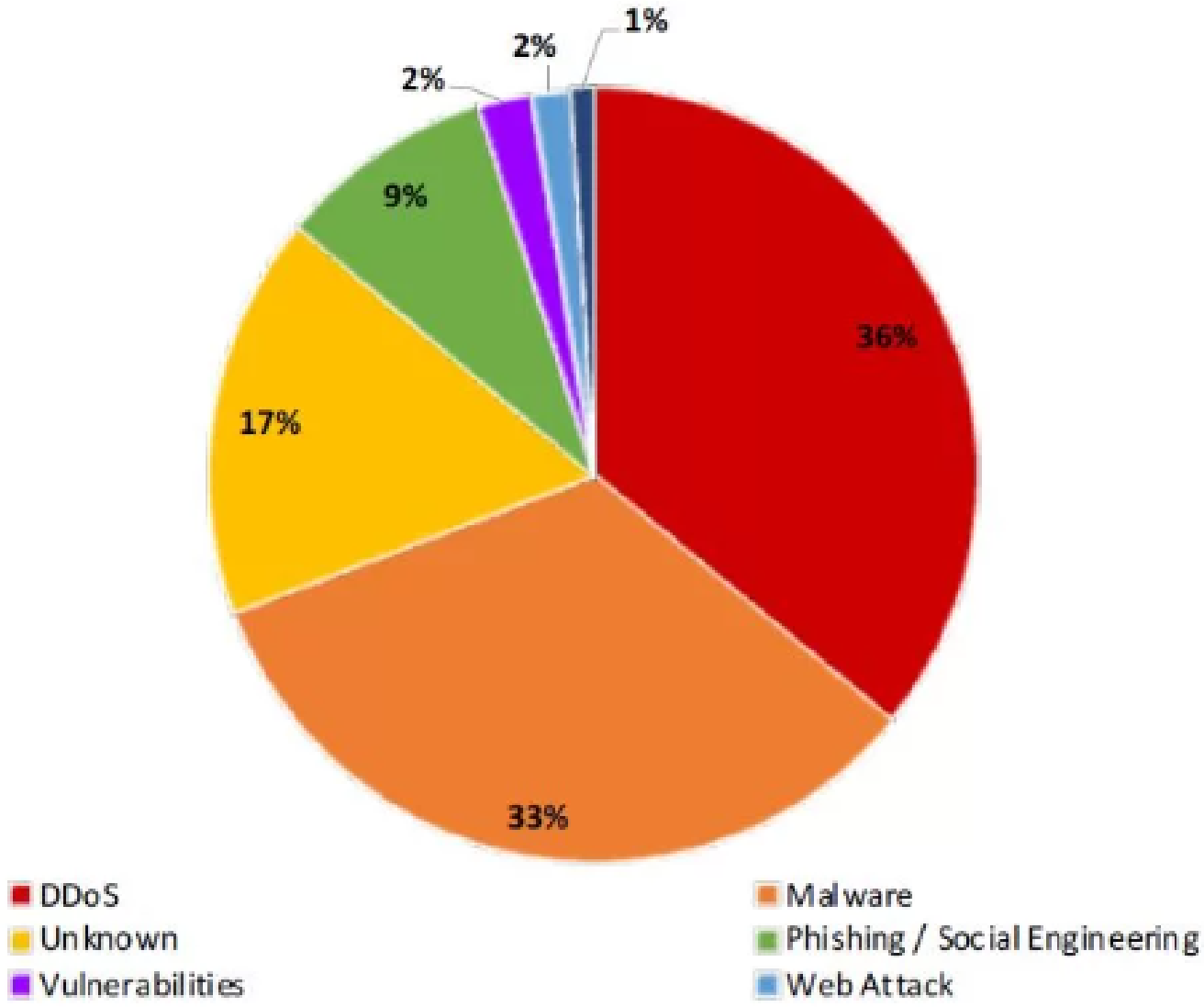
Il social engineering è una pratica di manipolazione psicologica che mira a persuadere le persone a rivelare informazioni sensibili o compiere azioni dannose. Gli attaccanti sfruttano la fiducia, la paura o la pressione psicologica per ottenere accesso a dati o sistemi.

Prompt per approfondire:

**"ChatGPT, potresti descrivere in dettaglio le tecniche di social engineering più comuni, come phishing, pretexting, baiting, quid pro quo e tailgating, con esempi pratici di come vengono utilizzate dagli attaccanti?"**

Tecniche principali:

- **Phishing:** Simula comunicazioni ufficiali (come email o SMS) per ottenere credenziali o installare malware.
- **Spear Phishing:** Variante mirata del phishing, diretta a persone o organizzazioni specifiche.
- **Pretexting:** L'attaccante si inventa una storia (pretesto) per ottenere informazioni sensibili, ad esempio fingendosi un tecnico di assistenza.
- **Baiting:** Offerta di "esche" (come premi falsi) per indurre l'utente a cliccare su link o scaricare file dannosi.
- **Quid Pro Quo:** L'attaccante si offre di risolvere un problema tecnico in cambio di credenziali, oppure finge di fare un favore per ottenere accesso.
- **Tailgating:** Accesso fisico a un'area protetta seguendo qualcuno che ha il permesso di entrare.




## 2. Strategie di Difesa

Difendersi dagli attacchi di social engineering richiede consapevolezza e l'adozione di pratiche difensive mirate. Essere in grado di riconoscere i segnali di allerta e adottare misure preventive sono aspetti essenziali per ridurre il rischio.

Prompt per approfondire le strategie difensive:

**"ChatGPT, quali sono le migliori pratiche per difendersi dalle tecniche di social engineering? Potresti elencare strategie preventive per ogni tipo di attacco, come phishing, pretexting e tailgating?"**

Suggerimenti di difesa:

- **Formazione e sensibilizzazione:** Impara a riconoscere email e comportamenti sospetti. La formazione regolare è cruciale per mitigare phishing e pretexting.
- Verifica e autenticazione: Utilizza l'autenticazione a più fattori (MFA) per ridurre il rischio di accessi non autorizzati.

- **Politiche aziendali rigorose:** Sviluppa protocolli per evitare la condivisione di informazioni sensibili senza verifica.
- **Segnalazione delle minacce:** Crea l'abitudine di segnalare comportamenti o richieste sospette.
- **Accesso controllato:** Limita l'accesso fisico a spazi riservati con badge e controlli per prevenire tailgating.
- **Test periodici:** Sottoponiti a simulazioni di phishing per allenarti e migliorare la tua risposta agli attacchi.


## 3. Esplorazione dei CVE (Common Vulnerabilities and Exposures)

I CVE sono identificatori che descrivono vulnerabilità di sicurezza in software e sistemi operativi. Analizzare i CVE ti permette di comprendere le debolezze di un sistema e di applicare le patch necessarie per mitigare i rischi.

Scelta del Software o Sistema Operativo:

- Seleziona un sistema operativo o software di cui vuoi approfondire le vulnerabilità (come Windows 10, WordPress o Apache HTTP Server).

Prompt per ottenere informazioni dettagliate sui CVE:

**"ChatGPT, potresti fornirmi una lista di CVE rilevanti per [nome del software o sistema operativo]? Mi servirebbero dettagli su alcune delle vulnerabilità più critiche, come**

**descrizione, rischi associati e metodi di mitigazione."**

Cosa includere nelle informazioni sui CVE:

- **Descrizione:** La natura della vulnerabilità e le sue implicazioni.
- **Rischi:** Scenari di sfruttamento, ad esempio accesso non autorizzato o esecuzione di codice remoto.
- **Soluzioni di mitigazione:** Patch ufficiali, aggiornamenti software e raccomandazioni pratiche per ridurre il rischio.


## Strutturazione della Relazione Finale

Struttura suggerita:

1. **Introduzione al Social Engineering:** Definizione e importanza di essere preparato a difendersi da attacchi di social engineering.
2. **Tipologie di Attacchi:** Descrizione delle tecniche di social engineering con esempi pratici.
3. **Strategie di Difesa:** Migliori pratiche per prevenire attacchi come phishing e pretexting.
4. **Analisi dei CVE per Software Specifico:** Approfondimento su alcune vulnerabilità rilevanti, con spiegazioni e raccomandazioni.
5. **Conclusioni e Raccomandazioni:** Sintesi delle tecniche, strategie di difesa e importanza dell'aggiornamento sulle vulnerabilità.

# Social Engineering: Tecniche di Attacco