

Utilizzo di ChatGPT per avere informazioni riguardo le Tecniche di Ingegneria Sociale

- Richiesta di informazioni riguardo le tecniche di Ingegneria Sociale usate dagli attaccanti.

### 1) Phishing.

Consiste nell'inviare messaggi fraudolenti che **imitano comunicazioni ufficiali** per indurre la vittima a:

- cliccare su un link maligno,
- scaricare un allegato infetto,
- inserire le proprie credenziali su un sito truffa (clonato).

Il Phishing può avere più varianti:

- **Spear phishing**: mirato a una persona o azienda specifica.
- **Whaling**: prende di mira figure di alto livello (es. CEO).
- **Smishing**: phishing via SMS.
- **Vishing**: phishing via chiamate vocali.

### 2) Tailgating

Questa tecnica consiste nell'**accedere fisicamente a un'area riservata** seguendo una persona autorizzata, approfittando della sua cortesia. Ad esempio:

- Un attaccante si presenta con le mani occupate davanti a una porta con badge, aspettando che qualcuno gliela apra.
- Si finge un corriere, un tecnico o un nuovo impiegato.

### 3) Pretexting

L'attaccante inventa un **falso pretesto o identità** per ottenere informazioni. Potrebbe fingersi un addetto all'IT, un collega, un fornitore o un'autorità (es. polizia, ispettore fiscale).

#### 4) Baiting

Offre qualcosa di **allettante (una “esca”)** per convincere la vittima a prendere un’azione. Un classico esempio è:

- Una chiavetta USB lasciata in un parcheggio aziendale: la vittima, curiosa, la inserisce nel PC e attiva un malware.

#### 5) Quid Pro Quo

Offre un **vantaggio in cambio** di informazioni o accesso. Un esempio può essere un falso supporto tecnico che chiama la vittima promettendo aiuto in cambio dell’accesso al computer.

Le strategie migliori per difendersi dagli attacchi possono essere:

- Formazione e sensibilizzazione del personale
- Politiche di sicurezza fisica
- Autenticazione forte
- Simulazioni di phishing
- Diffidenza verso richieste inusuali

**Utilizzando Windows 11** ho scelto di chiedere a ChatGPT i CVE relativi ad esso e mi ha riportato i seguenti:

#### **Principali CVE relativi a Windows 11:**

- **CVE-2025-24076** – Vulnerabilità di tipo DLL hijacking nel componente Mobile Devices, consente elevazione dei privilegi.
- **CVE-2025-24985** – Integer overflow nel driver Fast FAT che può portare all'esecuzione di codice locale.
- **CVE-2025-24054** – Spoofing tramite NTLM, sfruttabile in attacchi di rete.
- **CVE-2025-24993** – Buffer overflow nello stack NTFS, utilizzabile per esecuzione di codice arbitrario.

- **CVE-2024-6769** – DLL hijacking con manipolazione della cache di attivazione, permette bypass dell'UAC.
- **CVE-2024-6768** – Vulnerabilità nel driver CLFS.sys che causa crash del sistema (BSOD).
- **CVE-2024-38063** – RCE nel sottosistema IPv6 dello stack TCP/IP.
- **CVE-2024-21302** – Permette il rollback di file di sistema per ripristinare vulnerabilità precedenti, aggirando misure di sicurezza come VBS.