Nel **2024 Data Breach Investigations Report** (DBIR), phishing e social engineering sono identificati come minacce principali con un impatto notevole sugli incidenti di sicurezza informatica. Ecco i principali dettagli:

Phishing

- **Phishing** è uno dei principali vettori di attacco nel 31% degli incidenti legati al social engineering. Gli attaccanti sfruttano email, messaggi e siti web per ottenere credenziali o altre informazioni personali.
- Più del **50% delle violazioni** in cui sono coinvolte tecniche di social engineering riguardano il furto di credenziali. Queste credenziali vengono poi utilizzate per accedere a sistemi o piattaforme sensibili (2024-dbir-data-breach-i…).
- Le tecniche di phishing, in particolare lo **spear-phishing**, sono state utilizzate nel 62% degli attacchi che prevedono l'invio di allegati malevoli, mentre i **link di phishing** hanno rappresentato il 33% (Rapporto_Clusit_2024_web) (Rapporto_Clusit_2024_web).

Social Engineering

- **Pretexting**, una sottocategoria del social engineering, resta una delle principali modalità di attacco, rappresentando il **40% degli incidenti**. Gli attaccanti utilizzano email già esistenti per convincere le vittime a fornire informazioni sensibili o effettuare operazioni fraudolente, come nel caso di attacchi **Business Email Compromise (BEC)** (2024-dbir-data-breach-i…).
- L'ingegneria sociale è efficace perché sfrutta la natura umana, rendendo le persone vulnerabili rispetto a sistemi tecnologici che sono più facilmente rafforzabili (2024-dbir-data-breach-i…).

In conclusione, phishing e social engineering sono tra i metodi più comuni e pericolosi utilizzati dagli attaccanti per compromettere le organizzazioni, evidenziando la necessità di difese tecnologiche e una maggiore consapevolezza tra gli utenti.