/LIBRAESVA

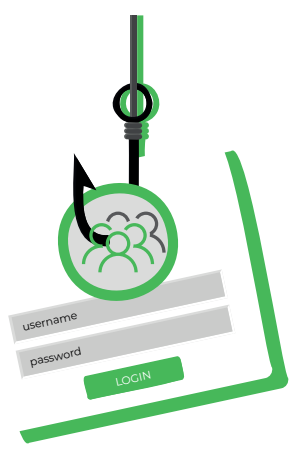
SOCIAL ENGINEERING

ATTACCHI DIFFUSI VIA EMAIL

IMPERSONATION

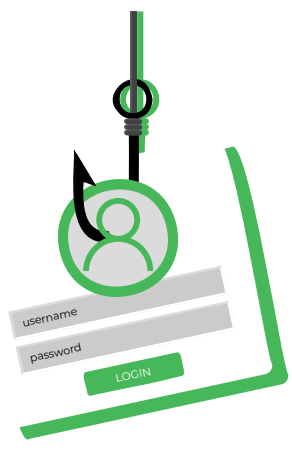
Utilizzare una falsa identità è il punto di partenza di un attacco di Social Engineering. Attraverso tattiche di **persuasione psicologica**, si mira a conquistare la totale fiducia del malcapitato, per indurlo a compiere un'azione immediata.

TIPOLOGIE DI ATTACCO



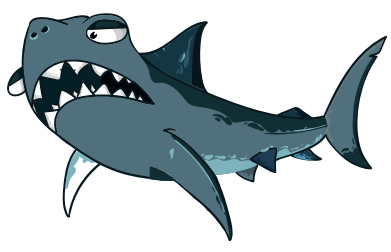
PHISHING

Invio di email massive contenenti link o allegati malevoli da parte di un soggetto che si finge una fonte affidabile, con lo scopo di indurre la vittima a fornire informazioni personali



SPEAR PHISHING

Email malevola progettata specificamente per una determinata vittima, con l'obbiettivo di ottenere un trasferimento di denaro o indurla a rivelare informazioni confidenziali a fini concorrenziali, di ricatto, per arrecare un danno o per screditare la vittima o la sua organizzazione



BUSINESS EMAIL COMPROMISE

Variante dello spearphishing in cui il criminale tenta di impersonare un CEO, un dirigente o un fornitore. L'attacco fa leva sull'autorità del mittente apparente e contiene un ordine di pagamento apparentemente legittimo o la richiesta di informazioni confidenziali. Questa forma di attacco è conosciuta anche come Frode del CEO o Whaling. A volte il criminale si inserisce in uno scambio email legittimo.