L’ingegneria sociale è una tecnica di manipolazione atta a trarre in inganno una o più persone nel tentativo di ottenere informazioni personali da queste(ad esempio, dati del conto corrente o delle carte di credito, credenziali di un account, ecc.), oppure di diffondere un malware. Vengono usate diverse tecniche psicologiche come, autorevolezza, urgenza, desiderio, consenso, senso di colpa, ecc. È molto importante essere consapevoli e saper riconoscere questo tipo di minacce per proteggere se stessi e i propri dati.
Tra i vari tipi di attacco di ingegneria sociale il più frequente è il phishing. Esso è una forma di truffa, perpetrata tramite mail, con lo scopo di ottenere informazioni personali della vittima o di farle eseguire una determinata azione, come cliccare su un link o scaricare un allegato.
L’attacco si svolge in questo modo:

-Invio della mail truffa da parte del malintenzionato;
-Apertura del messaggio da parte della vittima;
-Accesso al falso sito e inserimento dei dati;
-Invio delle informazioni al truffatore.

Per raggiungere i loro scopi, i criminali informatici si avvalgono di strumenti in grado di creare delle email che sembrano legittime, magari copiando anche il logo della compagnia. La vittima, tramite il click su un link nella email, viene reindirizzata in un sito falso simile a quello originale del fornitore del servizio oppure indotta a scaricare un allegato contenente un malware.
Il phishing può essere molto insidioso e gli attacchi di questo tipo diventano sempre più sofisticati. È importante dunque tenersi aggiornati e formare il personale.
I dipendenti delle aziende devono saper distinguere una email legittima da una falsa. Adesso che abbiamo chiaro il concetto di ingegneria sociale e di phishing possiamo capire come difenderci.
La regola numero uno in questo caso è: nessuno può tutelare le nostre informazioni meglio di noi stessi. Per questo è necessario creare e gestire i dati con cura e diffonderli il meno possibile. Non bisogna condividere le informazioni personali con nessuno, tantomeno scriverle su un pezzo di carta e lasciarlo incustodito da qualche parte.
Ma come possiamo capire se un’email è falsa o no?
Per distinguerle possiamo controllare i seguenti dettagli:

-Controllare che l’URL o il link siano corretti;
-Controllare eventuali errori ortografici, poiché spesso sono scritte da un software e presentano errori grammaticali;

-Controllare attentamente l’indirizzo email del mittente e il dominio, poiché in genere differiscono da quello reale dell’azienda/compagnia (per esempio invece di google.com potrebbe essere google.web, oppure invece di facebook potrebbe apparire come facebok);
-Controllare le richieste, dato che è molto improbabile che la vostra banca, agenzia governativa o qualsivoglia social vi richieda soldi o informazioni personali.

Grazie ad un tool come GoPhish è possibile simulare una campagna di attacco phishing, eseguire quindi un test di sicurezza sulle applicazioni aziendali ed effettuare una sessione di formazione pratica in cyber security al proprio personale.
Per ingannare il personale al meglio si possono adottare le tecniche più usate come ad esempio email che creano allarmismi, come per esempio scrivere sulla email che se non si effettua un controllo entro 48 ore altrimenti viene bloccato l’account, oppure c’è un pagamento in sospeso.