



Un programma di Cyber Security Awareness evoluto oltre a descrivere le varie tecniche di attacco, utilizzando una comunicazione efficace e comprensibile anche da persone inesperte in sicurezza informatica, dovrà analizzare il **fattore umano** nel contesto della Cyber Security, attingendo a contributi multidisciplinari per esempio le scienze sociali, la psicologia e la sociologia.

Nello specifico dovrà da un lato essere in grado di trasformare concretamente gli Atteggiamenti e i Comportamenti degli utenti di fronte alle crescenti minacce Cyber e dall'altro descrivere le dinamiche che intercorrono tra l'attaccante e la vittima, evidenziare quindi sia il modo di pensare della vittima sia quello di operare dell'attaccante.

Come dice Sun Tzu:

"Se conosci il nemico e te stesso non dovrai temere il risultato di cento battaglie."

Ma cosa significa analizzare un argomento di Cyber Security dal punto di vista psicologico?



Significa rendere l'utente consapevole che gli hacker, sfruttando le nostre emozioni, ci spingono ad agire d'istinto, senza utilizzare quella parte più razionale e logica del nostro cervello e creano dei meccanismi per ingannare il modo in cui il nostro cervello prende delle decisioni.

Inoltre gli hacker utilizzano momenti di disattenzione, come il lunedì mattina quando l'utente controlla l'email che ha ricevuto nel fine settimana, oppure 5 minuti prima della pausa pranzo, oppure potrebbe utilizzare la fine della giornata lavorativa quando l'utente si sta preparando per terminare le attività lavorative.

Le principali caratteristiche che dovrebbe avere un innovativo programma di Cyber Security Awareness per essere efficace e di successo:



**La nostra Missione è passare
dall'Informazione alla Trasformazione**

