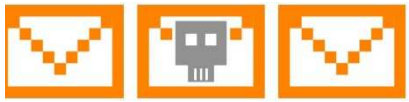
# SECURITY AWARENESS TESTING

*"**It's not if but when a cyber security attack will happen**": si tratta della frase che accomuna tutti gli ultimi rilevamenti statistici che calcolano la numerosità degli attacchi cyber subiti dalle organizzazioni a livello mondiale.*

*La tecnologia di attacco innovativa attualmente più utilizzata e che costituisce un vero e proprio incubo per le società si chiama **APT** (Advanced Persistent Threats) e si installa generalmente aprendo o facendo clic su allegati o collegamenti fraudolenti in un messaggio email, un messaggio in chat, un post in ambiente social network o un altro sito Web. Potrebbe entrare nel sistema persino durante la semplice visita di un sito Web appositamente creato.*

*Si tratta di un malware molto sofisticato che **elude i tradizionali sistemi di difesa** (Advanced); si insidia nel computer **senza essere rilevato** ed attende le istruzioni del suo creatore /attaccante (Persistent). Con qualche centinaio di dollari si possono acquistare al mercato nero rendendoli sfruttabili anche senza avere la minima conoscenza tecnica. I più diffusi attualmente sono i ransomware Locky, Cerber, Teslacrypt, Petya e le numerose varianti di **CryptoLocker**.*

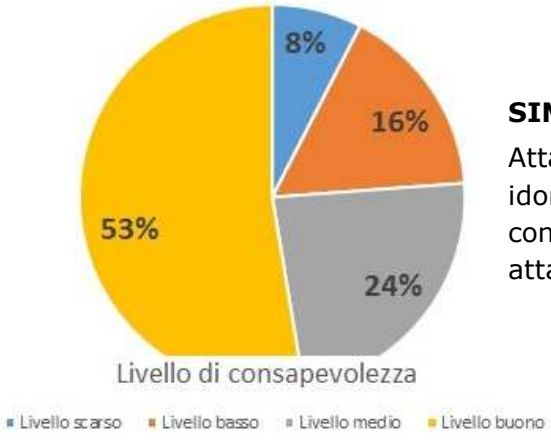
L'azione più efficace per ridurre il rischio di attacchi APT è la sensibilizzazione del personale a queste forme di attacco.



1. **MISURAZIONE**: valutare la consapevolezza del personale attraverso simulazioni di attacchi che rilevino la propensione delle persone ad utilizzare gli strumenti informatici in maniera pericolosa, avventata o ingenua.
2. **MITIGAZIONE**: definire una strategia di awareness che sia in linea con quanto misurato nella fase precedente e che contribuisca efficacemente e velocemente all'innalzamento della sensibilità del personale alle tematiche di sicurezza.

## SIMULAZIONE DI PHISHING

Attacchi di phishing simulati, a complessità crescente, idonei a tracciare il comportamento del personale e valutarne di conseguenza il livello di consapevolezza. Tale verifica può essere condotta sia attraverso la spedizione di mail sia attraverso la spedizione di messaggi chat o messaggi social.


## SIMULAZIONE DI APT ATTACK

Attacchi APT simulati, anch'essi a complessità crescente, idonei a tracciare la reazione del personale e valutarne di conseguenza la predisposizione a cadere nei tranelli degli attacchi mirati, decisamente più subdoli di quelli di phishing.


XECURITY S.R.L.
VIA GALLARATE, 156
20151 MILANO
WWW.XECURITY.IT