



# Cyber Guru

## Cyber Guru Phishing add-on

**ESTENSIONI FUNZIONALITÀ**

PHISHPRO



Cyber Guru Phishing, grazie all'esclusivo e innovativo modello di Machine Learning progettato in maniera specifica per la formazione e l'addestramento, è in grado di offrire un approccio personalizzato e, soprattutto, adattivo e automatico, che rende il training formativo molto più efficace e funzionale per affrontare le nuove tecniche di attacco cyber.

È proprio per addestrare gli utenti a diverse tecniche di attacco cyber, che Cyber Guru offre l'Add-on **PhishPro** che estendere le simulazioni di attacco a due componenti digitali particolarmente interessanti per il cyber crime, le **Chiavette USB** e i **QR code**. L'Add-On offre inoltre una formazione anti-phishing adattiva con la funzionalità **Adaptive Learning Remediation**.



**SIMULAZIONE  
ATTACCO USB**



**SIMULAZIONE  
ATTACCO QR CODE**



**ADAPTIVE LEARNING  
REMEDATION**



# Simulazione attacco USB

Utilizzando questa particolare tipologia di simulazione sarà possibile ampliare l'addestramento anti-phishing e formare il personale ad un uso consapevole dei dispositivi USB.

## L'estensione di attacco con chiavetta USB consente ai supervisor di:

- Creare una chiavetta USB contenente un file Microsoft Word "malevolo".
- Accedere a un report, presente nella Dashboard di Remediation e alimentato ad ogni apertura del file Word, che evidenzierà il numero di volte che il Word è stato aperto.
- Analizzare quanti utenti, oltre a inserire la chiavetta USB nel dispositivo, hanno anche accettato di eseguire la macro Word, un'azione particolarmente pericolosa per la sicurezza che esporrebbe l'organizzazione a un ulteriore livello di rischio cyber.

# Simulazione attacco QR code

Utilizzando questa particolare tipologia di simulazione sarà possibile ampliare l'addestramento anti-phishing e formare il personale sui rischi che potrebbero nascondersi dietro un QR code malevolo.

## L'estensione di attacco QR code consente di realizzare campagne di simulazione così organizzate:

- I supervisor potranno creare dei QR code "malevoli", stamparli e distribuirli all'interno dell'organizzazione.
- Gli utenti che effettueranno la scansione e accetteranno di aprire il link presente nel QR code saranno reindirizzati a una landing page dedicata dove verrà chiesto loro di fornire informazioni sensibili come ad esempio nome e email.
- Ogni QR code scansionato andrà ad alimentare un report presente nella Dashboard di Remediation, dove verranno evidenziati quanti QR Code sono stati scansionati e chi ha inviato le ulteriori informazioni richieste.

# Adaptive Learning Remediation

Con questa particolare tipologia di Remediation adattiva sarà possibile effettuare delle azioni di formazione personalizzate verso quegli utenti che necessitano di contenuti didattici dedicati e finalizzati al riconoscimento della minaccia di cui sono caduti vittima.

Dalla Dashboard di Remediation, i supervisor potranno pertanto assegnare dei contenuti formativi dedicati a quella tipologia di utenti definiti "weak" o che soddisfano criteri simili, fornendo così una formazione specifica e finalizzata al riconoscimento della minaccia di phishing.