Cyber Guru

Cyber Guru Phishing add-on

PHISHPRO

ESTENSIONI FUNZIONALITÀ

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

PHISHPRO

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 supervisori 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 supervisori potranno creare dei QR code "malevoli", e distribuirli all'interno dell'organizzazione attraverso due modalità:

- Il QR Code potrà essere stampato e distribuito. La scansione e l'apertura del link relativo al QR Code e l'eventuale immissione di informazioni aggiuntive inserite nella landing page a cui il link del QR Code porta, verranno tracciate.
- Il QR Code potrà essere distribuito attraverso le usuali mail di phishing di Cyber Guru Phsihing.

Adaptive Learning Remedation

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 supervisori 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.