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 tre componenti digitali particolarmente interessanti per il cyber crime: la **simulazione attacco video/deepfake**, le **chiavette USB** e i **QR Code**.
L'Add-On offre inoltre una formazione deepfake anti-phishing adattiva, con la funzionalità **Adaptive Learning Remediation**.

- SIMULAZIONE ATTACCO USB
- SIMULAZIONE ATTACCO QR CODE
- ADAPTIVE LEARNING REMEDIATION
- SIMULAZIONE ATTACCO VIDEO

PHISHPRO

Simulazione **attacco video**

Questa estensione consente di simulare l'identità di persone fidate, sfruttando il senso di urgenza e la familiarità per spingere gli utenti a condividere informazioni sensibili o ad agire d'impulso, senza la necessaria riflessione.

Potenzia la formazione anti-phishing aumentando la consapevolezza sugli attacchi video/deepfake, offrendo ai supervisori la possibilità di:

- Accedere a script di esempio per la realizzazione di video deepfake simulati.
- Utilizzare template email specifici per scenari di attacco video/deepfake.
- Monitorare i risultati tramite report dettagliati e dashboard dedicate.

Simulazione **attacco USB**

Questa simulazione rafforza la formazione anti-phishing sensibilizzando gli utenti all'uso sicuro dei dispositivi USB.

Grazie all'estensione per l'attacco USB, i supervisori possono:

- Creare una chiavetta USB contenente un file Microsoft Word "malevolo" simulato.
- Monitorare ogni apertura del file tramite la Remediation Dashboard.
- Verificare quanti utenti hanno collegato la chiavetta e quanti hanno attivato la macro – un'azione rischiosa che aumenta l'esposizione ai cyber attacchi.

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.

I supervisori possono creare codici QR "malevoli" realistici e condividerli in due modalità:

- **Stampati** – Posizionati in vari punti del luogo di lavoro. Una volta scansionati, è possibile monitorare le azioni dell'utente, come l'apertura del link o l'invio di informazioni.
- **Via email** – Inviati attraverso le email di phishing simulate di Cyber Guru.

Adaptive **Learning Remediation**

Fornisce una formazione personalizzata agli utenti che sono caduti vittima di attacchi di phishing simulati. Grazie alle informazioni fornite dalla Remediation Dashboard, i supervisori possono assegnare contenuti personalizzati agli utenti considerati vulnerabili.
La formazione è mirata, pertinente e rafforza la consapevolezza proprio dove è più necessaria.