Cyber Guru

Cyber Guru Phishing add-on

PHISHPRO

EXTENSIONES DE FUNCIONALIDAD

Cyber Guru Phishing, gracias al exclusivo e innovador modelo de Machine Learning diseñado específicamente para la formación y entrenamiento, es capaz de ofrecer un enfoque personalizado y, sobre todo, adaptativo y automático, que hace que el entrenamiento sea mucho más efectivo y funcional para enfrentar las nuevas técnicas de ataque cibernético.

Es precisamente para entrenar a los usuarios en diferentes técnicas de ataque cibernético, que Cyber Guru ofrece el complemento PhishPro, que amplía las simulaciones de ataques a tres componentes digitales particularmente interesantes para la ciberdelincuencia: la **simulación de ataques** de **vídeo/deepfakes**, las **memorias USB** y los **códigos QR**.
El complemento también ofrece una formación anti-phishing adaptativa con la funcionalidad de **Aprendizaje Adaptativo** de **Remediación**.

- **SIMULACIÓN DE ATAQUE USB**
- **SIMULACIÓN DE ATAQUE DE CÓDIGO QR**
- **REMEDIACIÓN DE APRENDIZAJE ADAPTATIVO**
- **SIMULACIÓN DE ATAQUE VÍDEO/DEEPFAKE**

PHISHPRO

Simulación de **ataque vídeo/deepfake**

Esta extensión permite simular la identidad de personas de confianza, aprovechando el sentido de urgencia y la familiaridad para incitar a los usuarios a compartir información sensible o a actuar impulsivamente, sin la reflexión necesaria.

Refuerza la formación anti-phishing sensibilizando sobre ataques con vídeo/deepfake y ofrecer a los supervisores la posibilidad de:

- Acceder a guiones de ejemplo para crear tus propios vídeos.
- Utilizar plantillas de correo electrónico adaptadas a escenarios de ataque con vídeo/deepfake.
- Monitorear los resultados a través de informes detallados y paneles de control especializados.

Simulación de **ataque USB**

Utilizando este tipo particular de simulación, será posible ampliar el entrenamiento anti-phishing y capacitar al personal en el uso consciente de los dispositivos USB.

La extensión de ataque con llave USB permite a los supervisores de:

- Crear una memoria USB que contenga un archivo de Microsoft Word “malicioso”.
- Acceder a un informe, presente en el Panel de Remediación.
- Analizar cuántos usuarios, además de insertar la memoria USB en el dispositivo, también han aceptado ejecutar la macro de Word, una acción particularmente peligrosa para la seguridad que expondría a la organización a un nivel adicional de riesgo cibernético.

Simulación de **ataque de código QR**

Esta simulación refuerza la formación y sensibiliza sobre los riesgos ocultos en códigos QR maliciosos.

Los supervisores podrán crear códigos QR "maliciosos" y distribuirlos dentro de la organización a través de dos métodos:

- El código QR podrá ser impreso y distribuido. La escaneada y apertura del enlace relacionado con el código QR y la evvventual introducción de información adicional en la página de destino a la que dirige el enlace del código QR serán rastreadas.
- El código QR podrá ser distribuido a través de los correos electrónicos de phishing habituales de Cyber Guru Phishing.

Remediación de **aprendizaje adaptativo**

Ofrece una formación personalizada a los usuarios que han caído en ataques de phishing simulados. Con la información proporcionada por el Panel de Remediación, los supervisores pueden asignar contenidos específicos a los usuarios considerados vulnerables.
La formación es precisa, relevante y refuerza la concienciación exactamente donde más se necesita.