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 ataque a dos componentes digitales particularmente interesantes para el cibercrimen, los **dispositivos 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

PHISHPRO

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 y alimentado cada vez que se abre el archivo Word, que destacará el número de veces que éste ha sido abierto.
- 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

Utilizando este tipo particular de simulación, será posible ampliar el entrenamiento anti-phishing y capacitar al personal sobre los riesgos que podrían esconderse detrás de un código QR malicioso.

La extensión de ataque de código QR permite realizar campañas de simulación de manera organizada.

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 eventual 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

Con esta particular tipología de Remediación adaptativa será posible realizar acciones de formación personalizadas hacia aquellos usuarios que necesitan contenidos didácticos dedicados y enfocados al reconocimiento de la amenaza de la cual han sido víctimas.

Desde el Panel de Remediación, los supervisores podrán asignar contenido de formación dedicado a aquellos usuarios definidos como “débiles” o que cumplan criterios similares, proporcionando así una formación específica y orientada al reconocimiento de la amenaza de phishing.