Cyber Guru

Cyber Guru Phishing add-on

PHISHPRO

EXTENSIONS DE FONCTIONNALITES

Cyber Guru Phishing, grâce à son modèle exclusif et innovant d'apprentissage automatique spécifiquement conçu pour la formation et l'entraînement, est capable de proposer une approche personnalisée et surtout adaptative et automatique, ce qui rend la formation beaucoup plus efficace et fonctionnelle pour faire face aux nouvelles techniques d'attaque cyber.

C'est précisément pour former les utilisateurs à différentes techniques d'attaque cyber que Cyber Guru propose l'Add-on **PhishPro**, qui étend les simulations d'attaque à trois composants numériques particulièrement intéressants pour les cybercriminels, la **simulation d'attaques vidéo/deepfakes**, les clés **USB** et les **codes QR**. L'Add-on offre également une formation anti-hameçonnage adaptative avec la fonctionnalité **Adaptive Learning Remediation**.

- **SIMULATION D'ATTAQUE USB**
- **SIMULATION D'ATTAQUE QR CODE**
- **ADAPTIVE LEARNING REMEDIATION**
- **SIMULATION D'ATTAQUE VIDÉO/DEEPFAKE**

PHISHPRO

Simulations d'attaque vidéo/deepfake

Cette extension permet de simuler l'identité de personnes de confiance, en exploitant le sentiment d'urgence et la familiarité pour inciter les utilisateurs à partager des informations sensibles ou à agir de manière impulsive, sans la réflexion nécessaire.

Renforcez la formation anti-phishing en augmentant la sensibilisation aux attaques vidéo/deepfake, en offrant aux superviseurs la possibilité de :

- Accéder à des scripts d'exemple pour la réalisation de vos vidéos.
- Utiliser des modèles d'e-mail spécifiques pour les scénarios d'attaque vidéo/deepfake.
- Surveiller les résultats grâce à des rapports détaillés et des tableaux de bord dédiés.

Simulation d'attaque USB

Cette simulation renforce la formation anti-phishing en sensibilisant les utilisateurs à l'utilisation sécurisée des périphériques USB.

Grâce à l'extension pour la connexion USB, les superviseurs peuvent :

- Créer une clé USB contenant un fichier Microsoft Word « malveillant » simulé.
- Surveiller chaque ouverture de fichier via le tableau de bord de remédiation.
- Vérifier combien d'utilisateurs ont connecté la clé et combien ont activé la macro, une action risquée qui augmente l'exposition aux cyberattaques.

Simulation d'attaque QR code

En utilisant ce type particulier de simulation, il sera possible d'élargir la formation anti-phishing et de former le personnel aux risques potentiellement cachés derrière un code QR malveillant.

Les superviseurs peuvent créer des codes QR « malveillants » réalistes et les partager de deux manières :

- **Imprimés** – Placés à différents endroits du lieu de travail. Une fois scannés, il est possible de surveiller les actions de l'utilisateur, telles que l'ouverture du lien ou l'envoi d'informations.
- **Par e-mail** – Envoyés via les e-mails de phishing simulés de Cyber Guru.

Adaptive Learning Remediation

Offre une formation personnalisée aux utilisateurs ayant été victimes d'attaques de phishing simulées. Grâce aux informations fournies par le tableau de bord de remédiation, les superviseurs peuvent attribuer des contenus personnalisés aux utilisateurs considérés comme vulnérables.
La formation est ciblée, pertinente et renforce la prise de conscience là où elle est le plus nécessaire.