Cyber Guru

Cyber Guru Phishing add-on

PHISHPRO

FUNKTIONSERWEITERUNGEN

Cyber Guru Phishing verwendet ein einzigartiges Modell für maschinelles Lernen, das speziell auf die Schulung und Ausbildung zugeschnitten ist. Dies bietet einen personalisierten Ansatz, der sowohl adaptiv als auch automatisiert ist und die Effektivität des Trainings gegen neue Cyber-Angriffstechniken erhöht.

Gerade um Benutzer auf verschiedene Cyber-Angriffsvektoren zu trainieren, bietet Cyber Guru das PhishPro Add-on an, das die Angriffssimulationen auf drei digitale Komponenten erweitert, die für Cyber-Kriminelle immer attraktiver werden: **Video-/Deepfake**, **USB-Sticks** (USB Baiting) und **QR-Codes** (Quishing). Das Add-On bietet ausserdem ein adaptives Anti-Phishing-Training durch die Adaptive Lernhilfe-Funktion.

USB ANGRIFF SIMULATION

SIMULATION EINES QR-CODE-ANGRIFFS

ADAPTIVE LERNHILFE

VIDEO ANGRIFF SIMULATION

PHISHPRO

Simulation eines **Videoangriffs**

Diese Erweiterung ermöglicht es, die Identität vertrauenswürdiger Personen zu simulieren, indem sie das Gefühl von Dringlichkeit und Vertrautheit ausnutzt, um Benutzer dazu zu bringen, sensible Informationen preiszugeben oder impulsivzu handeln, ohne die notwendige Überlegung.

Sie verbessert das Anti-Phishing-Training, indem sie das Bewusstsein für Video/Deepfake-Angriffe erhöht und den Verantwortlichen die Möglichkeit bietet:

- Auf Beispielskripte zur Erstellung simulierten Deepfake-Videos zuzugreifen.
- Spezifische E-Mail-Vorlagen für Video-/Deepfake-Angriffszenarien zu verwenden.
- Die Ergebnisse über detaillierte Berichte und spezielle Dashboards zu überwachen.

Simulation eines **USB-Angriffs**

Durch den Einsatz dieser besonderen Art von Simulation kann die Anti-Phishing-Schulung verbessert und das Personal zum bewussten Umgang mit USB-Geräten ausgebildet werden.

Die USB-Angriffserweiterung erlaubt es Aufsichtsbehörden:

- Erstellen eines USB-Sticks mit einer «bösartigen» Microsoft Word-Datei.
- Über das Dashboard auf Berichte zuzugreifen, die bei jedem Öffnen der Datei aktualisiert werden.
- Analysieren Sie, wie viele Benutzende nicht nur den USB-Stick in das Gerät gesteckt haben, sondern auch das Word-Makro ausgeführt haben – eine besonders gefährliche Aktion für die Sicherheit, die das Unternehmen einem zusätzlichen Cyber-Risiko aussetzen würde.

Simulation eines **QR-Code-Angriffs**

Diese spezielle Simulation verbessert das Anti-Phishing-Training und sensibilisiert Mitarbeitende für die Risiken bösartiger QR-Codes.

Mit der QR-Code-Angriffserweiterung können Vorgesetzte simulierte Kampagnen durchführen, indem sie „bösartige“ QR-Codes auf zwei Wegen verteilen:

- Als Ausdruck innerhalb der Organisation. Scans, Link-Aufrufe und Dateneingaben werden nachverfolgt.
- Über reguläre Phishing-E-Mails von Cyber Guru.

Adaptive **Lernhilfe**

Bietet personalisiertes Training für Nutzer, die auf simulierte Phishing-Angriffe hereingefallen sind. Dank der Informationen aus dem Remediation-Dashboard können Aufsichtsführende gezielt Inhalte an als gefährdet eingestufte Nutzende zuweisen.
Die Schulung ist zielgerichtet, relevant und stärkt das Bewusstsein genau dort, wo es am nötigsten ist.