Cyber Guru

Cyber Guru Phishing add-on

PHISHPRO

FUNCTIONALITY EXTENSIONS

Cyber Guru Phishing uses a unique Machine Learning model tailored for training and education. This offers a personalised approach that's both adaptive and automated, enhancing the effectiveness of training against emerging cyber attack techniques.

It is precisely to train users to different cyber attack vectors that Cyber Guru offers the PhishPro Add-on, which extends the attack simulations to three digital components that become increasingly attractive to cyber criminals: **video attacks/deepfake, USB keys** (USB baiting) and **QR Codes** (Quishing). The Add-On also provides adaptive deepfake phishing emails training through the **Adaptive Learning Remediation** feature.

- **USB ATTACK SIMULATION**
- **QR CODE ATTACK SIMULATION**
- **ADAPTIVE LEARNING REMEDIATION**
- **VIDEO ATTACKS SIMULATION**

Video Attacks Simulation

PHISHPRO

This simulation extension lets you impersonate trusted individuals, playing on urgency and familiarity to manipulate people into sharing sensitive info or act quickly without taking time to think. It enhances anti-phishing training by raising awareness to video attacks/deepfakes, allowing supervisors to:

- Unlock sample scripts for specific deepfake videos, helping them create their own fake videos.
- Access vdeo attack/deepfake-specific email templates.
- Track performance through reports and dashboards.

USB Attack Simulation

This simulation enhances anti-phishing training by raising awareness to safe USB device usage.

With the USB attack extension, supervisors can:

- Create a USB stick with a mock “malicious” Microsoft Word file.
- Track each time the file is opened via the Remediation Dashboard.
- See how many users plugged in the USB device and how many enabled the macro - a risky action that increases cyber exposure.

QR Code Attack Simulation

This simulation helps users spot the hidden risks behind malicious QR Codes.

Supervisors can create realistic "malicious" QR Codes and share them in two ways:

- **Printed** - Place them around the workplace. When scanned, user actions like opening the link or submitting info are tracked.
- **Email** - Send them via Cyber Guru’s phishing emails.

Adaptive Learning Remediation

Provide tailored training for users who’ve fallen for simulated phishing attacks.
Using insights from the Remediation Dashboard, supervisors can assign personalised content to those flagged as vulnerable.
Training is focused, relevant, and reinforces awareness for those that need it the most.