Cyber Guru Phishing add-on

FUNCTIONALITY EXTENSIONS

PHISHPRO

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 two digital components that become increasingly attractive to cyber criminals: **USB keys** (USB baiting) and **QR codes** (Quishing). The Add-On also provides adaptive anti-phishing training through the **Adaptive Learning Remediation** feature.

USB ATTACK SIMULATION

QR CODE ATTACK SIMULATION

ADAPTIVE LEARNING REMEDATION

USB attack simulation

By using this particular type of simulation, it will be possible to enhance anti-phishing training and educate personnel on the conscious use of USB devices.

The USB attack extension allows supervisors to:

- Create a USB key containing a "malicious" Microsoft Word file.
- Access a report, present in the Remediation Dashboard and updated every time the Word file is opened, which will highlight the number of times the Word has been opened.
- Analyse how many users, in addition to inserting the USB key into the device, have also agreed to execute the Word macro, a particularly dangerous action for security that would expose the organization to an additional level of cyber risk.

QR code attack simulation

By using this particular type of simulation, it will be possible to enhance anti-phishing training and educate personnel about the risks that may be hidden behind a malicious QR code.

The QR code attack extension allows simulation campaigns to be realised in this way:

- The supervisors will be able to create "malicious" QR codes, print them, and distribute them within the organization.
- Users who scan and agree to open the link in the QR code will be redirected to a dedicated landing page where they will be asked to provide sensitive information such as name and email.
- Every scanned QR code will contribute to a report in the Remediation Dashboard, where it will be highlighted how many QR codes have been scanned and who has sent the additional requested information.

Adaptive Learning Remedation

With this particular type of adaptive remediation, it is possible to carry out personalized training actions towards those users who need dedicated educational content aimed at recognizing the threat they have fallen victim to.

From the Remediation Dashboard, supervisors are able to assign dedicated training content to those types of users defined as "weak" or who meet similar criteria, thus providing specific and targeted training for recognizing phishing threats.