Cyber Guru

Cyber Guru Phishing

EXPERIENTIAL TRAINING TO TRANSFORM HUMAN BEHAVIOURS

Cyber Guru Phishing is the anti-phishing experiential training programme delivered by our platform. Thanks to the exclusive and **innovative Machine Learning model** specifically designed for training, Cyber Guru Phishing is able to offer a personalized and, above all, automatic and adaptive approach to simulated campaigns, which makes training much more effective and functional in dealing with new cyber attack techniques.

The training operates in three specific areas:

- The perception of danger
- The promptness in acting correctly
- The awareness of the threat

The effectiveness of automation

Thanks to our innovative Machine Learning model, Cyber Guru Phishing offers a completely adaptive training capable of reducing management costs to zero. Our ML Engine can automatically adapt all simulation campaigns based on the behavioural profile of each individual user, following the logic of "**Personal Training**".

The model, continuously enriching itself with information, is able to send personalized phishing simulations, taking into account the likelihood that a person may fall victim to a phishing attack. The adaptive process is essentially based on some macro-variables:

- **The user profile**: that is, the specific level of resistance to attacks based on thematic preferences, time slots, or digital habits.
- **The templates ranking**: that is, the level of difficulty of the attack, calculated on parameters that are both static and dynamic, taking into account the specificity of the organization.

Transforming the phishing experience into effective training

To transform phishing experiences into effective training opportunities, each simulation campaign must be unique and personalised, and this should be achieved without any human intervention. The learning algorithms of our ML model are in fact able to select the most suitable attack templates to ensure maximum training effectiveness.

When a user fails a simulation by performing the deceptive action outlined in the template, they immediately receive personalised educational content related to the specific deception used in the attack template.

Cyber Guru Phishing offers the possibility to carry out phishing attack campaigns via email and SMS. With the **PhishPro Add-on**, it is also possible to carry out simulations of phishing attacks with **USB keys** (USB baiting) and **QR codes** (Quishing), and to perform personalized training actions with the **Adaptive Learning Remediation** functionality.

Advanced reporting

The reporting, available on a unified dashboard, does more than just measure the average click-rate. Using advanced metrics, it allows users to assess the actual risk and track its mitigation throughout the programme's progression.

Features of Cyber Guru Phishing

EXPERIENTIAL TRAINING

- Continuous training
- Instant error training
- Remediation policies
- Reporting procedure
- Multilingual format

ENGAGEMENT OF THE LEARNER

- Adaptive process
- Custom simulations
- Risk groups
- Difficulty levels
- Localised templates
- Simulations on USB-QR codes

ENGAGEMENT OF THE LEARNER

- SaaS platform
- Turnkey service
- Automated campaigns
- Pre-loaded templates
- Comprehensive reporting