
Cyberattacks:
Awareness is
no longer optional
Cyber
Guru

Introduction

The human factor is now the most crucial element in cybersecurity, used by cybercrime to creep into organisations with increasingly sophisticated offensive strategies. It is precisely the users, whose behaviour is not adapted to the complexity of the challenge, who unwittingly open the door to the attackers.

Analysing the various reports concerning the state of cybersecurity, the picture that emerges is one of unstoppable growth in cyberattacks. Among the various attack techniques used, those growing the fastest are characterised by the human factor.

The news is full of successful cyberattacks. Attacks that affected organisations from all sectors and of all sizes. Both prestigious and lesser-known brands have seen their production activities halted and their reputations compromised. Make no mistake, a cyber war is taking place and the attackers have an unquestionable advantage. Crucially, the first line of defence consists of unaware users who, in most cases, don't even realise that they are being attacked.

Therefore, launching effective and innovative Cyber Security Awareness programmes, capable of adapting human behaviour and turning users into the organisations' first line of defence, is no longer an option.

Cyber Guru's Cyber Security Awareness platform increases resistance to cyberattacks. Continuous learning programmes develop people's ability to operate with safe behaviour guided by increased awareness. A constantly implemented platform that uses the most advanced technologies, production processes and pedagogical methodologies to ensure maximum user involvement and protection against cyber risks.

Michel Ruefenacht
VP Marketing

The scenario

Unfortunately, trends in cyberattacks in recent years show a steadily increasing curve. One of the main causes is undoubtedly the increased use of digital technologies, considered to be the driving force behind real economic growth. However, this growth has not been matched by adequate digital literacy among users. Accelerating the trend are the effects of the pandemic, with the massive shift to remote working and increased use of digital applications and services.

Unfortunately, despite the considerable efforts made by organisations in cybersecurity, what emerges is that the weakest link in any organisation's defence chain is still the human factor, and in particular digital users. It is now established that more than 90 per cent of cyberattacks can be traced back to human error, to inappropriate behaviour.

90% of cyberattacks start with a click on a malicious email

Barclays Bank

95% of cyberattacks are attributable to human error

IBM Cyber Security Intelligence Index Report

A chain is only as strong as its weakest link

An organisation's resistance to cyberattacks therefore depends on the resilience of the Human Factor, today's real weakest link in the chain.

The development of the digital society, with its risks, forces all organisations to invest consistently in the human factor, in people's awareness.

An investment that has become necessary to bridge the cultural gap that the effects of pandemic and rapid digital transformation have exacerbated.

“In 2021, data breaches cost organisations $45 billion.”

Panda Security

“The number of ransomware attacks increased by 13% between 2020 and 2021.”

Verizon Data Breach Investigations Report

“Global cybercrime costs to reach $10.5 trillion by 2025.”

Cybersecurity Ventures

The methodology

Launching effective and innovative Cyber Security Awareness programmes, capable of affecting human behaviour and turning users into the organisations' first line of defence, is no longer an option.

The Cyber Guru platform is designed to maximise learning processes by developing 3 defensive characteristics of the individual: **knowledge, perception of danger, and readiness to respond**.

This requires advanced training programmes, based on innovative ongoing training and engagement methodologies, which can minimise the impact on those conducting staff training and cybersecurity management. Only this way will it be possible to keep pace with the continual progress of increasingly sophisticated attack strategies.

3 TRAINING COURSES

Cognitive

Knowledge is managed through a cognitive training process based on a mainly didactic approach.

Inductive

The perception of danger is stimulated through inductive training that acts on the more emotional component of our brain.

Experiential

Practising alertness is essential if we want to act quickly and adopt the right behaviour when danger arises.

A complete cyber security awareness platform

The platform is designed to transform the behaviour of the workforce of any public or private organisation, whatever its size or product category, thanks to:

3 HIGHLY SYNERGISTIC TRAINING COURSES

Cyber Guru Awareness

A cognitive educational programme delivered on an e-learning basis that ensures the gradual development of awareness through knowledge about network threats and the behavioural pattern to be adopted to prevent attacks.

Cyber Guru Channel

An inductive training programme that generates learning thanks to the strength of storytelling and video production. Following a narrative pattern typical of TV series, the learner learns by identifying with the situations narrated in the different episodes.

Cyber Guru Phishing

An experiential training programme that trains individuals to resist various types of phishing attacks. The programme, which is automatic and adaptive, allows for customised training based on individual experience and individual level of resistance to attacks.

Cyber Guru Awareness

Cyber Guru Awareness is designed to engage the entire organisation in an educational and stimulating learning pathway, characterised by its steady and gradual release (Smart-School) approach. The course consists of self-consistent training modules, each dedicated to a specific topic, with monthly activation, covering a period of 12/24/36 months. Each module consists of 3 video lessons of 5 minutes duration. The main features are effective cognitive learning, maximum learner involvement, and zero-impact supervision.

- **Self-consistent training modules with monthly activation**
- **A minimum weekly commitment, compatible with any job role**
- **Video micro-lessons in multimedia format**
- **Use of professional actors with coach roles**
- **Highly informative language**
- **An interactive approach with continuous alternation between micro lessons and tests**
- **Multiple-choice assessment tests**
- **Gamification methodology, with team organisation**
- **A multilingual platform**
- **Additional and continually updated content**

Cyber Guru Channel

The inductive methodology is based on the user's immersion within a real situation and a process of self-identification with the cyber threat, which then takes a concrete form. The user gains awareness not by being given information, but through a narrative, which first targets the perception of danger, and then provides factual knowledge, thereby bypassing a very dangerous afterthought: "it couldn't happen to me". The three main features are effective inductive learning, maximum learner involvement, and zero-impact supervision.

- **Ongoing training**
- **Advanced video productions**
- **Multiple video formats with different storytelling**
- **Short episodes**
- **A high-paced narrative**
- **Self-identification in realistic situations**
- **A Netflix-like approach**
- **In-depth documentation for each episode**
- **Comprehensive reporting on the level of use**
- **Automatic student caring functions, to motivate participation**

Cyber Guru Phishing

Cyber Guru Phishing is designed to train the workforce to resist phishing attacks, through simulated attack campaigns. These are customised based on the behavioural profile of the individual user, using an automatic and adaptive process, guided by the artificial intelligence technologies. The learner increases their resistance to attacks by gaining experience, both negative by making mistakes, and positive by learning to recognise attacks when they happen. The three main features are effective experiential training, personalised training, and zero-impact supervision.

- **Effective and continuous experiential training**
- **Personalised training through an adaptive process**
- **Levels of difficulty and custom simulations**
- **Automated attack campaigns**
- **Error > Instant training**
- **Reporting procedure**
- **Pre-built templates**
- **Analytical and managerial reporting through an advanced dashboard**
- **Risk groups**
- **Remediation policies**

Cyber Guru

Security Awareness Training That Works!

Follow us on LinkedIn | Youtube

Learn more at Cyber Guru
cyberguru.it/en/

Become our partner
cyberguru.it/en/partner/

Are you interested in a live demo of our solutions?

Book a 30-minute appointment with an Awareness Training Specialist

BOOK NOW