TRAINING COURSE

Security Awareness 2025

YOUR COMPANY IS UNIQUE:
CUSTOMIZE YOUR TRAINING PATH

securitylab ACADEMY | eLearning atelier

“Security is not a product, but a process. And it all starts with awareness.”

Bruce Schneier, cybersecurity expert

Defend your digital world!

Modular architecture: freedom to build

The **Security Awareness 2025** course introduces an innovative **autonomous block** structure. Each module lives independently and can be delivered separately from the others.

This architecture offers training managers the freedom to compose tailor-made paths, calibrating content based on the specific risk profiles of various departments.

The independence of modules also allows for strategic temporal distribution, transforming cybersecurity from one-time training into a continuous process that keeps attention alive over time.

A flexible approach that responds to different business needs and adapts to the constant evolution of digital threats.

Intelligent training path

Adaptive training on the Moodle platform
Our course introduces a personalized learning system: each module is preceded by an assessment test that evaluates the user's level of knowledge on the 15 fundamental topics of modern cybersecurity. Based on the results, the path automatically adapts, showing only the content necessary to fill the actual knowledge gaps.

Flexible delivery method: This adaptive mode is one of the available options. The course's modular architecture also allows for traditional, complete delivery or customized paths based on specific organizational needs.

Strategic benefits for the company:

- ↗ **Intelligent Assessment:** Unlike solutions that use generic fake phishing, our tests, delivered on the Moodle platform and processed with AI, determine the user's real knowledge with greater reliability.
- ↗ **Automated Management:** No need to manually define who sees which content – the system automatically determines the optimal path for each user.
- ↗ **Training Efficiency:** Drastic reduction in downtime and a focus on actual skill gaps.
- ↗ **Complete Traceability:** Detailed monitoring of individual progress and acquired skills.

- **Automatic Compliance:** Punctual documentation of the training path for audits and certifications.
- **Reinforced Company Protection:** Employees trained specifically on the risks related to their role and sector.
- **Incident Reduction:** Targeted prevention of the most critical human vulnerabilities for the organization.

From basic cybersecurity to scams involving artificial intelligence, every employee receives the exact training they need. A smart approach that transforms mandatory training into strategic professional growth, ensuring optimal company protection and significantly reducing exposure to cyber risks.

Security is essential in work and daily life

In today's digital landscape, every click can represent a risk, both in the office and at home. Cyber threats evolve at an impressive speed: criminals continuously refine their strategies, making attacks increasingly difficult to detect.

The **Security Awareness 2025** course has been completely renewed to address the most recent challenges.

Based on real cases, it provides concrete tools to:

- Immediately recognize phishing and social engineering attempts
- Effectively protect sensitive personal and corporate data
- Implement security measures for mobile devices and smart homes
- Defend against advanced scams using artificial intelligence
- Safeguard personal privacy and digital identity

Awareness is the first and most powerful line of defense against cyber threats. This course goes beyond corporate security, offering essential skills to also protect private digital life, family, and personal information in an increasingly connected world.

Discover the keys to security: a comprehensive path

The **Security Awareness 2025** course offers a structured training path that covers all dimensions of modern digital security. Each module has been designed to address specific threats with a practical and immediately applicable approach.

From social engineering to scams based on artificial intelligence, from password protection to smart working security, this course provides concrete tools to safely navigate the complex current digital landscape.

The modules that make up the training path have been developed by analyzing hundreds of real cases of cyber attacks, with particular attention to the international context.

The defense techniques presented have been selected for their effectiveness and simplicity of implementation, ensuring immediate results in both professional and personal contexts.

The fifteen course modules

1.

Introduction to Cybersecurity

This fundamental module explores the basic principles of computer security and its growing importance in daily life. It analyzes the main threats in today's digital landscape, from data theft to espionage, highlighting how the human factor often represents the weakest link in the security chain. The course delves into the objectives of cyber attacks and the malicious use of stolen personal data, debunking the myth that only large companies are targets of criminals. Through real cases and concrete scenarios, participants acquire solid awareness of the need to protect their digital presence, developing a proactive approach to cybersecurity.

2.

Social engineering: the art of deception

This module explores the psychological manipulation techniques used by cybercriminals to induce people to disclose confidential information or perform risky actions. It analyzes the psychological mechanisms exploited, such as the art of deception and human weaknesses, along with the most commonly used techniques by scammers. The course teaches how to recognize manipulation attempts and presents practical defense strategies both personal and corporate, with the goal of developing a true security culture.

3.

Phishing: the perfect deception

The module delves into phishing in all its forms, from traditional versions to more sophisticated techniques. It examines email phishing and fake sites along with their psychological mechanisms, then moves to targeted attacks like spear phishing and whaling against executives. It analyzes modern variants like smishing (SMS), vishing (phone) and QRishing (QR codes), in addition to advanced techniques such as typosquatting, calendar phishing and IM phishing. The course also addresses the dangers of artificial intelligence integration in phishing and provides effective defense and recognition techniques.

4.

E-mail: basic rules for protection

This module analyzes emails as the main vector of cyber attacks, exploring vulnerabilities, types of threats and best practices for secure communication. It examines emails as gateways to the digital world, BEC (Business Email Compromise) scams in corporate environments and mass attacks with "spray-and-pray" techniques. It explains the danger of malicious attachments and provides basic rules and effective defense strategies in the age of artificial intelligence.

5.

Password: the first line of defense

The module explores authentication systems, from correct use of traditional passwords to modern authentication technologies. It teaches techniques for creating secure passwords and proper access management, the advantages and use of password managers, and passphrases as an effective alternative. The course debunks false myths about password security, explains multi-factor authentication (MFA) with its different types and introduces passkeys as the future of passwordless authentication.

6.

Protected browsing

This module illustrates the risks of online browsing and the necessary precautions to protect your data. It analyzes the differences between HTTP and HTTPS and their security implications, how to verify website authenticity and the limits of the HTTPS padlock that can create false senses of security. It highlights the risks of advanced phishing even on HTTPS sites and provides practical techniques for safe daily browsing.

7.

Mobile: opportunities and risks

The module focuses on mobile device security, analyzing specific risks and protection strategies for smartphones and tablets. It examines opportunities and dangers of mobile devices, how to recognize malware and spyware, app security and permission management. It addresses digital payments with their risks, cloud data protection, and security on social media and messaging apps, with particular attention to the most common scams on WhatsApp and other platforms.

8.

Digital Footprint: digital traces

This module explores the concept of digital footprint, analyzing how our online activities create permanent traces. It explains what digital footprint is and how it forms, its impact on personal and professional life, with particular attention to risks for minors. It illustrates threats related to data exposure, techniques for cleaning and managing your online presence, and how to build a positive and professional digital footprint.

9.

Ransomware: the art of digital extortion

The module analyzes the ransomware threat in detail, explaining attack mechanisms, consequences and prevention and response strategies. It defines what ransomware is and how it works, its action mechanisms and infection vectors, the short and long-term impact of attacks. It presents effective prevention strategies, the importance of backup and recovery plans, and actions to take in case of attack.

10.

Smart Working: working safely

This module addresses the specific security challenges of remote work, offering practical strategies to protect data and communications outside the corporate environment. It analyzes home office risks and hidden vulnerabilities, how to protect privacy during remote work, and manage IT emergencies from home. It discusses physical workspace security, secure communications during videoconferences and messaging, the balance between productivity and security, and protection of mobile devices in work contexts.

11.

Scams with Artificial Intelligence

The module explores new frontiers of scams powered by artificial intelligence, analyzing emerging techniques and defense strategies. It examines deepfake video calls and how to recognize them, voice cloning and advanced phone scams, and methods to identify AI-generated content. It provides daily good practices against these scams, verification and protection tools, and techniques for safeguarding your biometric data.

12.

Smart Home: protecting devices

This module focuses on the security of connected devices in domestic and personal environments, addressing vulnerabilities and protection measures. It examines risks and vulnerabilities of smart home devices, protection of cameras, voice assistants and other connected devices, and the importance of secure configuration and updates. It illustrates conscious use of IoT devices, home network protection, and privacy management with always-connected devices.

13.

Fake news: recognizing and defending against them

The module teaches how to verify the authenticity of online information, providing practical tools to recognize false news and manipulated content. It explains what fact checking is and why it's essential in digital security, the psychology behind disinformation and the ESCAPE method for quick verification. It presents accessible digital tools to verify images and news, how to recognize false or manipulated content, the importance of fact checking during emergencies and crises, and how to protect family and friends from disinformation.

14.

External storage: data security in motion

This module analyzes risks related to portable storage devices and strategies to protect sensitive data during transport. It examines the dangers of device variety and diffusion, intrinsic vulnerabilities of physical media and risks of uncontrolled data transfer. It addresses concrete threats like loss, theft, degradation and damage to media, and unauthorized data access. The course provides practical strategies for effective protection through encryption, access control, physical device management and secure usage policies, in addition to presenting advanced strategies and secure alternatives for structured backup.

15.

Wearable devices: practical protection

The module focuses on wearable device security and strategies to protect personal data collected by these increasingly widespread tools. It examines effective methods to limit data collection, correctly manage companion app permissions and create digital boundaries for your privacy. It analyzes techniques to protect sensitive data through account security, Bluetooth transmission protection and physical device security. The course illustrates secure configurations, the importance of regular updates and separation of usage contexts, along with strategies for periodic permission verification and data minimization techniques.

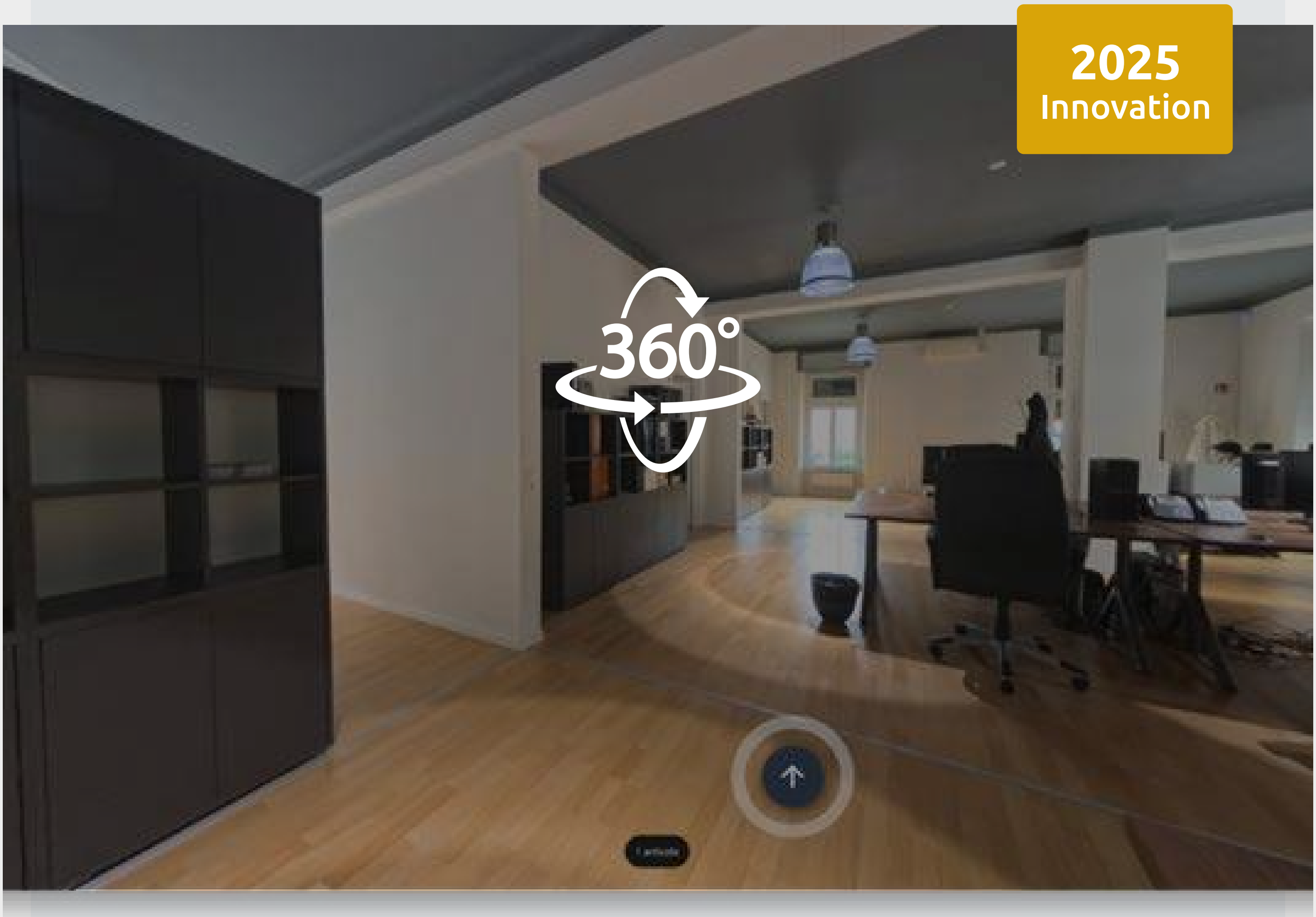
Phishing Detective: Interactive exercise

This interactive module offers a practical learning experience where users can test their abilities to recognize phishing emails. By hovering over suspicious links and sender addresses, it’s possible to analyze in real time the authenticity of URLs and sender details to determine if they are legitimate communications or fraud attempts.

Through realistic examples and immediate feedback, this simulation develops concrete skills to identify even the most sophisticated deception techniques, transforming theory into practical daily digital defense abilities.

Office 360°: immersive risk simulation

INTERACTIVE MODULE



2025
Innovation

This module offers a **3D interactive experience** where users explore a realistic office environment to identify security risks. Navigating the virtual space, participants must identify vulnerabilities such as unattended devices, unprotected sensitive information, visible passwords and other physical threats. For each discovered element, the system provides explanations about the risk and suggests practical solutions.

This immersive simulation transforms theoretical concepts into practical skills, developing the ability to quickly recognize potential threats in your daily work environment.

Who is the course for?

The **Security Awareness 2025** course has been designed to meet the security needs of a diverse audience.

In professional settings

The course is aimed at managers and executives who must protect sensitive corporate information, employees at all levels who use digital tools daily, and administrative teams who manage critical data and important communications.

In personal settings

The course is aimed at everyone who wants to improve their security in the digital world. The course offers practical tools and essential knowledge to navigate safely in cyberspace, regardless of technological competence level.

No advanced technical skills required

The course has been developed with clear language and concrete examples, making computer security accessible to everyone.

Innovative Learning Experience

The **Security Awareness 2025** course has been developed using cutting-edge educational technologies to ensure an engaging and effective learning experience:

Intelligent and personalized navigation

The course is structured with an interactive interface that allows free navigation between contents. Each module is organized in interconnected thematic sections: a simple click allows direct access to the topic of interest, enabling a personalized learning path based on your needs and priorities.

Accessible multimedia content

Each slide is enriched with professional audio commentary that guides users through fundamental concepts. Synchronized subtitles guarantee full content accessibility and facilitate understanding and memorization of key information, making the training experience complete and inclusive.

Tailored learning

The modular structure and rich multimedia equipment allow adaptation of learning pace to your needs. Whether it's intensive training or a path spread over time, the platform supports different learning strategies, always maintaining high attention through alternating theoretical and practical elements.

Integrated formative assessment

Each module concludes with a calibrated test that allows verification of understanding of fundamental concepts. The peculiarity of this system lies in the articulated feedback that accompanies each answer: targeted commentary that deepens the topic, clarifies any doubts and consolidates learning. This methodological approach transforms the evaluation moment into an additional growth opportunity, favoring deep and lasting understanding of the course's essential contents.

Learning monitoring and analysis

The course is supported by a sophisticated monitoring system that allows a complete view of the training path. For training managers and HR teams, the platform offers intuitive dashboards with detailed reports on individual and collective progress. It's possible to view module completion rates, usage times, test performance and level of interaction with contents. This data, exportable in different formats, allows evaluation of training effectiveness, identification of potential improvement areas and customization of future training interventions. Integrated analysis provides objective metrics on training investment return, transforming training from cost to measurable strategic investment.

Protect your Company

Request a free demo of the **Security Awareness 2025** course

info@elearningatelier.ch ↗

securitylab ACADEMY | eLearning atelier

www.elearningatelier.ch

eLearning Atelier - Corso Enrico Pestalozzi 21A, 6900 Lugano, Switzerland