

PHISHED x THE SECURITY FACTORY

Build your human firewall with Phished

Change behavior, reduce human error and prevent
cyber incidents - all with a holistic approach to
security awareness training



The only metric that matters in cybersecurity is a zero-incident rate

A holistic approach is the only truly effective way to keep your company cybersecure. Phished combines hyper-realistic phishing simulations with frequent training sessions. This is the only way to drive real behavioral change and prevent cyber incidents caused by human error. Furthermore, the new NIS2 directive mandates that healthcare institutions provide regular cybersecurity training to both management and staff.

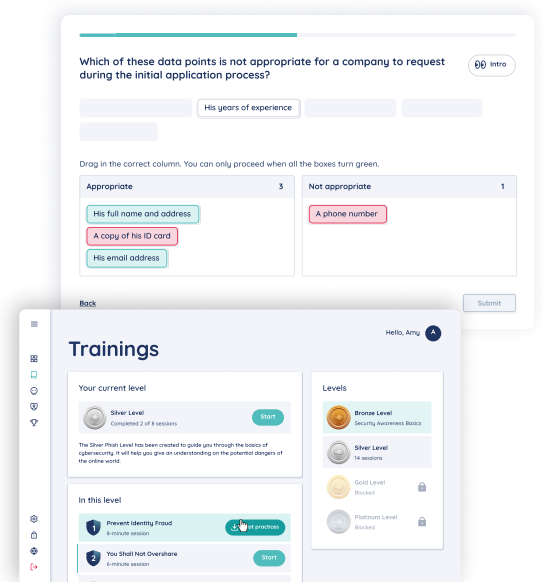
Cybersecurity training for managers & IT teams - COMPLIANT WITH ART.21 OF NIS2.

The Phished training for C-level and IT teams covers a wide range of topics related to regulations such as NIS2 and GDPR. The training sessions include templates, checklists, and certificates to demonstrate compliance.

Cybersecurity training for employees - COMPLIANT WITH ART.21 OF NIS2.

Phished is a comprehensive training platform that opens your employees' eyes to every kind of cyber threat. So they can go from being innocent targets to vigilant defenders of your organization.

- ✓ **AI-driven phishing simulations with microlearnings**
Practicing how to recognize and report attacks (such as phishing) is a key requirement under NIS2. With Phished, employees learn to detect and report malicious emails through AI-driven phishing simulations, personalized to their individual skill level and reinforced with targeted microlearnings.
- ✓ **Gamified Cyber Resilience Training**
Frequent, bite-sized training sessions on topics like incident response, access control, HR, AI and deepfakes, ... With certification levels ranging from Bronze to Platinum. These regular trainings are designed to drive lasting behavioral change across the organization, in line with NIS2.
- ✓ **Repeat Offender Training for high-risk users**
Zero Incident Mail™ delivers targeted training in a safe environment to protect high-risk users, such as first-time clickers, repeat offenders, new hires, and those who enter sensitive data.
- ✓ **1-minute video training for apps & devices**
Training on the secure use of apps and devices is linked to NIS2's obligation. Phished provides targeted training for allowlisted apps and devices, helping employees easily optimize their privacy and security settings.
- ✓ **Real-time Threat Alerts**
A cyber defense team informs your employees on the latest cyber threats with quick guides showing them how to respond.



The difference between **cybersecurity training** and traditional security awareness training



OTHER SOLUTIONS

- **Science-based**, holistic curriculum, designed to drive behavioral change.
✓ NIS2 COMPLIANT
- **Performance-based certification** ranging from Bronze to Platinum.
- **Gamified training for users** aligned with familiar workflows, updated monthly.
✓ NIS2 COMPLIANT
- **Tailored training for management** and IT teams, focused on key compliance topics like NIS2, GDPR, ISO27001, SOC2, ...
✓ NIS2 COMPLIANT
- **Simulations** tailored to each employee's skill level, language, and context.
✓ NIS2 COMPLIANT
- **Designed by ethical hackers** to replicate real-world phishing attacks.
- Integrated training for **repeat offenders**.
✓ NO RISK OF DATA BREACHES
- **Fully automated** simulations and training sessions.
✓ NIS2 COMPLIANT

- **Massive content libraries** with no clear learning path.
x INSUFFICIENT FOR BEHAVIORAL CHANGE
- **Participation-only certificates** with no assessment or skill validation.
- **Static training** not tied to real work scenarios.
x INSUFFICIENT FOR BEHAVIORAL CHANGE
- **Lack of tailored management** or IT training, and no coverage of critical frameworks like NIS2, GDPR, ISO27001, and SOC2.
x INSUFFICIENT FOR NIS2 COMPLIANCE
- **Generic, uniformly applied simulations** reused across regions.
✓ NIS2 COMPLIANT
- **Predictable content** that misses real-world threat tactics.
x INSUFFICIENT FOR BEHAVIORAL CHANGE
- **No targeted training** for high-risk users.
x CRITICAL RISK OF DATA BREACHES
- Campaigns and training **require significant manual effort** from IT.
✓ NIS2 COMPLIANT

A Behavioral Risk Score™ to track & quantify your resilience

The Behavioral Risk Score™ gives admins a concrete way to measure how vulnerable their workforce is to phishing attacks. So you can close awareness gaps and watch your employees' efforts pay off.

