

resp^onsu

By



Leading IT Security Awareness Training Platform

Build a Strong Cybersecurity Culture through Employee Training



Solution for small, medium, and large enterprise-level companies



Responsu IT security training platform empowers companies to build a strong cybersecurity culture by enabling employees to recognize common cyber threats.

The solution makes it easy to implement an ongoing training program across the entire organization and comply with GDPR, ISO 2700 regulations.

Responsu helps companies of all sizes and industries turn their employees into human firewalls, reduce costs, simplify training administration and strengthen IT security posture.

Benefits



Company

- Stronger IT security
- GDPR, ISO 27001 compliance
- Branding and customization
- Cost-savings



Administrator

- Centralized user management
- Real-time reports
- Automatization
- Tests & certificates



User

- Localized real-life examples
- Micro-modules and interactivity
- 24/7 availability
- Localized content

Modules

- Introduction to information security
- A short GDPR guide
- Mobile device security
- Social engineering
- Wi-Fi security
- Phishing
- Secure work from home
- Social networks
- Vishing
- Physical security
- Passwords
- "Clean table" policy
- Your suggestion



Finance



Government



Transportation



Healthcare

100% Deployment Flexibility



Cloud-Hosted

- Hosted on the cloud
- Training administration control



As-a-Service

- Hosted on the cloud
- Dedicated training administrator



On-Premise

- Hosted on your own server(s)
- Training administration control

Our Customers



Siauliai district municipality

Responsu has helped a significant number of our employees refresh their IT security awareness. Interactive content, localized examples, and visual elements enabled them to grasp tough cybersecurity topics almost effortlessly.

Jurgita Mickūnė

Legal and Personnel Administration Division Officer, Šiauliai District Municipality



Exceeded our expectations! Our team was contented to obtain hands-on skills which they can apply in professional and personal setup. We have already recommended the training to our partners.

Rasa Butkuvienė

CEO, Easy Dept Service

Choose a package	Basic	Standard	Premium
● Access to trainings	●	●	●
● Phishing simulations		●	●
● Professional services	●	●	●
● Customization			●

Contact Us

- info@responsu.com
- +37068881450
- www.responsu.com



responsu



A brief overview of online courses

Physical security

- Why is Physical Security awareness important when it comes to preventing cyber hacking in your organization?
- What steps should be taken if fraud is suspected?

A short GDPR guide

- What is GDPR?
- What are the principles of personal data processing?
- How can we apply GDPR in practice?
- What rights do we have as data subjects?

Passwords

- Why is it important to use strong passwords?
- What does a proper password actually mean?
- How can we create and remember proper passwords?

"Clean table" policy

- What does "a messy workplace" mean according to IT security standards?
- To what we should pay special attention in the workplace?
- How can we identify misplaced information or items?
- How can we protect our workplaces?

Wi-Fi security

- Why and when using a wireless network (Wi-Fi) can put information on your smart device at risk?
- What rules should we follow to protect information when using public Wi-Fi?

Safe work from home

- What are the tactics cybercriminals use?
- What are the most common cyber threats that employees face when working from home?
- How can we identify and prevent these dangers?

Mobile device security

- What are the most common cyber threats related to mobile devices?
- How can we protect information on a mobile device?
- How can we reduce the chance of a mobile device being hacked?

Vishing

- What information shouldn't we disclose when talking on the phone?
- What strategies do criminals use?
- What should you do if you got a suspicious call?

Phishing

- Why has email fraud been so successful for years?
- How can each of us recognize a suspicious email?
- What should you do if you received a fraudulent email?