



---

**First-line Incident  
Response training  
for general IT  
specialists**

**2022**

# **Cybersecurity for IT Online**

**kaspersky**

Free trial: [cito-training.com](https://cito-training.com)

# Cybersecurity for IT Online (CITO)

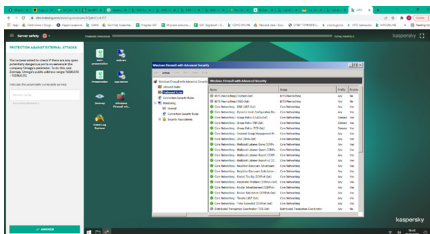
**Interactive training that builds strong cybersecurity and first-level incident response skills for general IT specialists**

## Training format

Training is completely online. Trainees only need Internet access and the Chrome browser on their PC. Each of 6 modules consists of a short theoretical overview, practical tips and between 4 and 10 exercises covering specific skills teaching students how to use IT security tools and software in everyday work.

Study is intended to be spread over the course of a year. The recommended rate of progress is 1 exercise per week – each exercise takes between 5 and 45 minutes to complete.

**The current edition of the training is targeted at the Windows corporate environment.**



## Training delivery method:

Cloud or SCORM format

Creating a strong corporate cybersecurity posture is impossible without the systematic education of all relevant employees. Most enterprises provide cybersecurity education and training on two levels – expert training for IT security teams and security awareness for non-IT employees. Kaspersky offers a comprehensive set of products for both. But what's missing? For IT teams, service desks, and other technically advanced staff, standard awareness programs are not enough. However, they don't need to become cybersecurity experts – it's too expensive and too time-consuming.

## First-line incident response

Kaspersky is launching first-on-the-market online skills training for generalist enterprise IT professionals. It consists of 6 modules:

- Malicious software
- Potentially unwanted programs and files
- Investigation basics
- Phishing incident response
- Server security
- Active Directory Security

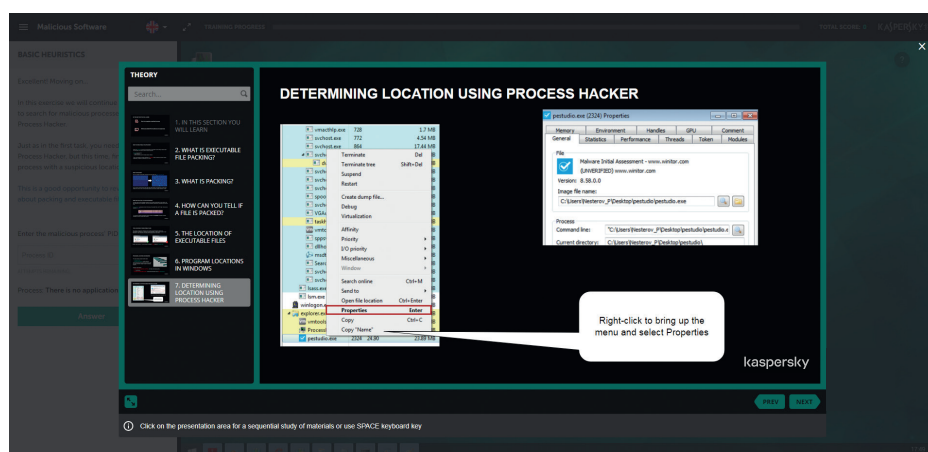
The program equips IT professionals with practical skills to recognize a possible attack scenario in a seemingly benign incident, and how to collect incident data for handover to IT security. It also creates a passion for hunting out signs of malicious activity, cementing the role of all IT team members as the first line of security defense.

## Why is CITO training effective?

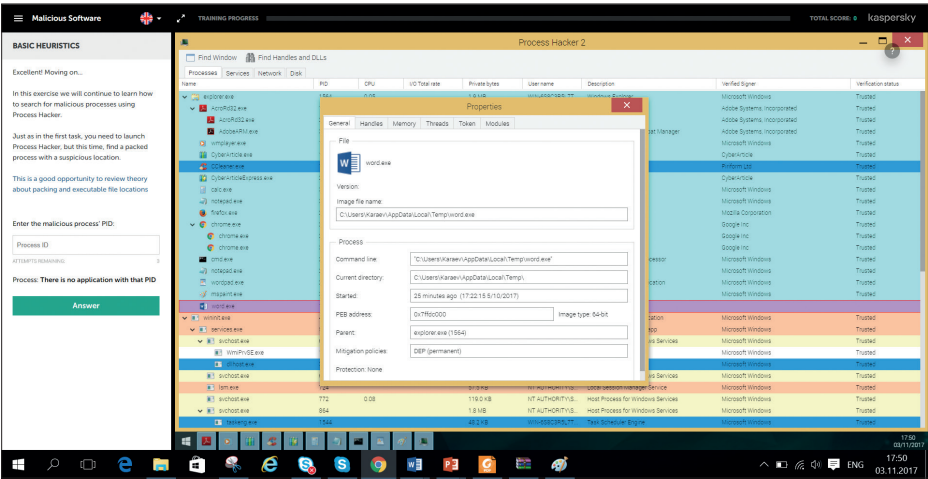
- Interactive: the stimulation of real processes without any risk to the computer
- Creates skills as well as knowledge: learning by doing
- Intuitive learning process: convenient navigation and hints
- Covers all the main IT security topics and problems that general IT staff face in their work

## Learning process

Each learning exercise block consists of two parts: education and practice, with tasks simulating real processes related to previous explanations.



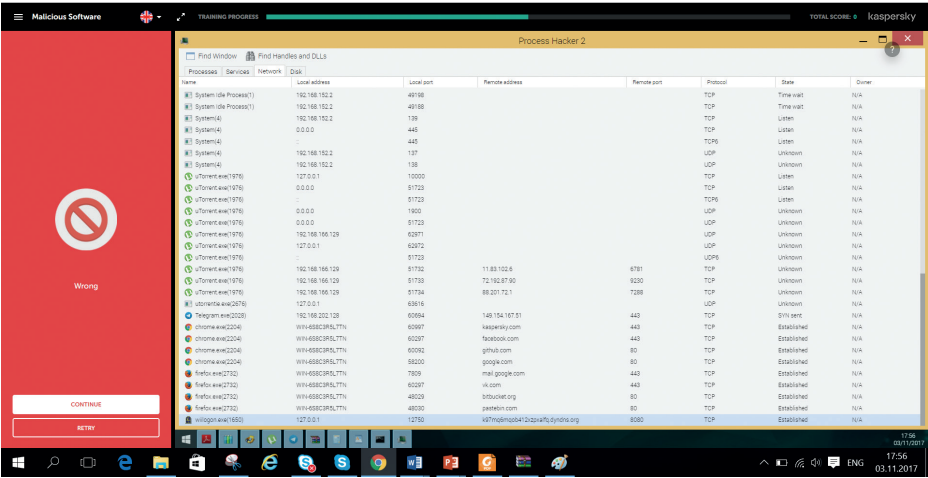
If you didn't manage to execute the task correctly, you will be prompted to attempt and pass the educational part again.



If you did well, you will be directed to the next exercise block.

Certificates

Personal certificates are available for employees after the completion of each module



Who is this training for?

This training is recommended for all IT specialists within the organization, especially service desks and system administrators. But most non-expert IT security team members will benefit from this course too.



## Training topics and outcomes

| Module name                                           | Target audience                                                                                                            | Knowledge gained                                                                                                                  | Personal attitude                                                                                                                                                                                                                                                                       | Skills gained                                                                                                                                                                      | Practice given in module                                                                                                                                                                                                                                        |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Malicious Software</b>                             | Users with administrated rights on servers and/or workstations                                                             | Malware techniques and classification<br><br>Malicious and suspicious software actions and signs<br><br>Heuristic analysis basics | Malware can exist anywhere on the computer<br><br>Malware can steal data in multiple non-trivial ways<br><br>It is mandatory to report all suspicious potential incidents to the security team                                                                                          | Verification of the existence or absence of a malware-related incident                                                                                                             | Using ProcessHacker, Autoruns, Fiddler, Gmer tools for detecting malware                                                                                                                                                                                        |
| <b>Potentially unwanted programs and files (PuPs)</b> | Users with the rights to install additional software, and users who actively evaluate/open files received from the outside | The basics of statistical and dynamic analysis of software samples and suspicious documents                                       | Documents (pdf, docx) can contain exploits<br><br>Unsigned files can contain malware or riskware<br><br>All unsigned executables should be checked for possible infection<br><br>A digital signature does not guarantee that the file doesn't contain malicious functionality           | Working with system and sandbox event monitors<br><br>Using statistical engines<br><br>Removing PuPs                                                                               | Static (signature) and statistical (virustotal) analysis of the software samples<br><br>Using procmon, to search for exploits and malicious behavior of software<br><br>File analysis with Cuckoo sandbox<br><br>Creating scripts for malware removal using AVZ |
| <b>Investigation basics</b>                           | IT employees involved in the forensic or incident response activities led by the security team                             | The Incident Response process<br><br>Methods of log analysis<br><br>Specifics of storing digital information                      | If you suspect a cybersecurity incident, immediately report it to the security team and collect digital evidence<br><br>Analysis should be done under the supervision of and in co-operation with the security team                                                                     | Collecting digital evidence<br><br>NetFlow traffic analysis<br><br>Timeline analysis<br><br>Event log analysis                                                                     | Collecting volatile and non-volatile data (FTK-imager)<br><br>Log analysis to find the source and the links of the attack (eventlogexplorer)<br><br>Lateral movement investigation by NetFlow analysis (ntop)<br><br>Disk analysis using Autopsy                |
| <b>Phishing and Open source intelligence (OSINT)</b>  | IT employees involved in forensic or incident response activities                                                          | Modern phishing methods<br><br>Methods of analysis for email headers                                                              | Phishing can be very sophisticated, making it hard to discover, but it can always be detected by manual investigation<br><br>Phishing emails need to be deleted from user' mailboxes                                                                                                    | Phishing email analysis and deleting obfuscated phishing emails from users' mailboxes<br><br>Open source intelligence for understanding what hackers know about your company       | Search and removal of the phishing emails in Exchange Mailbox<br><br>Using Recon-ng for web reconnaissance                                                                                                                                                      |
| <b>Server security</b>                                | Server administrators                                                                                                      | Analyze the network environment<br><br>Server hardening<br><br>Analyze PowerShell logs to detect attacks                          | Network perimeter compromise is one of the major attack vectors. It's impossible to close all vulnerabilities - you need to reduce the attack surface to make it as hard as possible for an attack to succeed. Even if it doesn't stop an intruder, it will buy you time for detection. | Search for vulnerable and non-standard network services<br><br>Configure systems according to the 'default deny' principle<br><br>Search for signs of an attack in PowerShell logs | Use Nmap to find vulnerable network services<br><br>Configure Software Restriction Policies for program control and Windows Firewall for network control<br><br>Analyze events using Event Log Explorer                                                         |

| Module name                      | Target audience                 | Knowledge gained                                                     | Personal attitude                                                                              | Skills gained                                                             | Practice given in module                                                       |
|----------------------------------|---------------------------------|----------------------------------------------------------------------|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| <b>Active Directory Security</b> | Active Directory administrators | Use an API to check passwords in a database of compromised passwords | Default Active Directory configuration is not optimal from security point of view.             | Safely check for password hashes in a database                            | Use the Have I Been Pwned? API to search the database of compromised passwords |
|                                  |                                 | Configure domain policies according to recommendations               | Attacker can elevate their privileges in many ways.                                            | Search for inconsistencies between recommended and actual domain policies | Use Policy Analyzer to compare current domain policies with best practices     |
|                                  |                                 | Methods for analyzing Active Directory domain security               | Study security recommendations, use tools which provide better visibility for Active Directory | Assess the security of Active Directory settings                          | Use Ping Castle reports                                                        |
|                                  |                                 |                                                                      |                                                                                                |                                                                           |                                                                                |

## Contact us

To arrange a demo, price inquiries and delivery information please contact your Kaspersky manager, or email [awareness@kaspersky.com](mailto:awareness@kaspersky.com)

# Kaspersky Security Awareness – a new approach to mastering IT security skills

### Key program differentiators



#### Substantial cybersecurity expertise

20+ years' experience in cybersecurity transformed into a cybersafety skillset that lies at the heart of our products



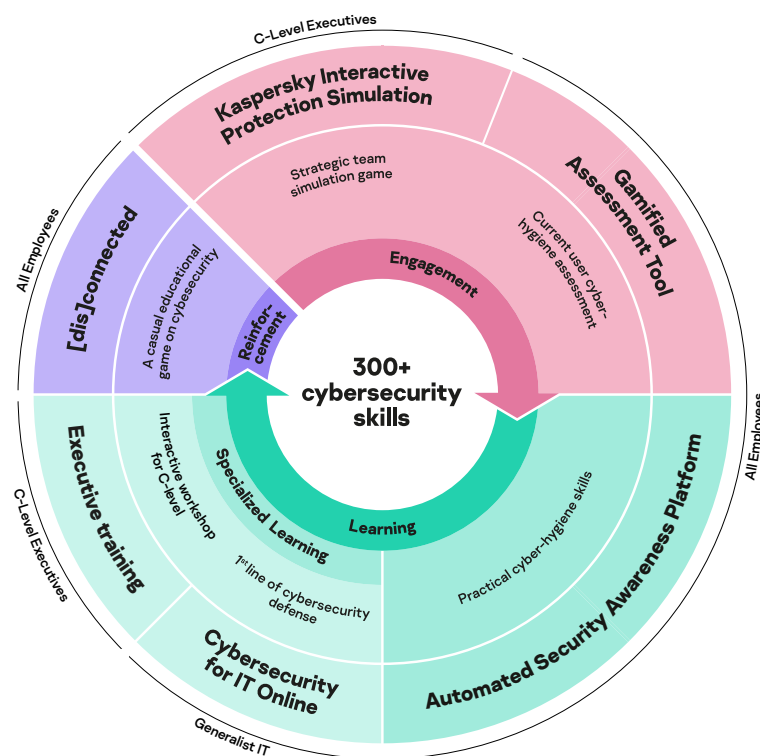
#### Training that changes employees' behavior at every level of your organization

Our gamified training provides engagement and motivation through edutainment, while the learning platforms help to internalize the cybersecurity skillset to ensure that learnt skills don't get lost along the way.

Kaspersky Security Awareness offers a diverse range of solutions covering all the cybersafety-specific needs of enterprises, and teaches the skills everyone needs using the latest learning techniques and technologies.

### One flexible training solution for all

Choose a single solution that addresses a specific security need, or let us provide packages that make it easy for you to launch and target training according to all your needs and priorities. You can find more information about packages here: [kaspersky.com/awareness](https://kaspersky.com/awareness)



Enterprise Cybersecurity: [www.kaspersky.com/enterprise](https://www.kaspersky.com/enterprise)  
Kaspersky Security Awareness: [www.kaspersky.com/awareness](https://www.kaspersky.com/awareness)

[www.kaspersky.com](https://www.kaspersky.com)

**kaspersky** **BRING ON  
THE FUTURE**