CYBERSECURITY EDUCATION

Leverage Kaspersky Lab's knowledge, experience and intelligence in the area of cybersecurity through this innovative education program.

Cybersecurity awareness and education have become critical requirements for enterprises faced with an increasing volume of constantly evolving threats. Improving and enabling information security employee skills in advanced security techniques is a key component of effective enterprise threat management and mitigation strategy.

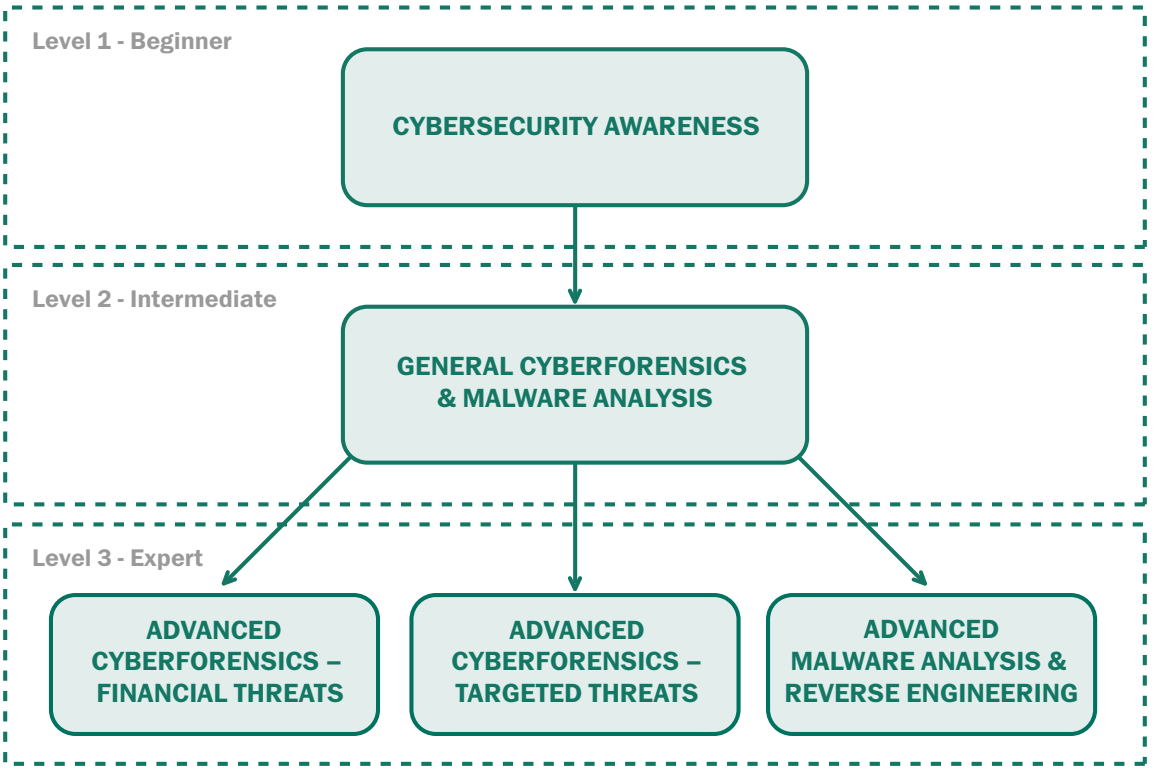
Developed specifically for any business looking to promote the role of cybersecurity in its operations to better protect its infrastructure and intellectual property. Kaspersky Lab's Cybersecurity Education program offers a broad curriculum and certification ranging from basic to expert cybersecurity topics and techniques.

IMPROVE YOUR IT SECURITY SKILLS TODAY:

Real hands-on experience – Kaspersky Lab's program is unique, providing hands-on experience with the latest attacks and malware – an immense benefit not available through other training providers.

Beginner, intermediate or expert? – The program is well structured and useful for a broad range of attendees.

A comprehensive offering – All training courses are offered in English and are available either in-class at a local or regional Kaspersky Lab office, or on-demand at a customer premises. The courses are designed to include both theoretical and practical classes (labs). Attendees are provided with all required training materials and laptops for labs. Upon completion of the course, all attendees will be able to pass a certification program to validate their knowledge on the course subjects.



Course Description	Course Duration	Course Audience
LEVEL 1 – CYBERSECURITY AWARENESS **Day 1:** Cyberthreats and Attacks in the Modern World **Day 2:** Protecting Against Cyberthreats and Attacks	2 days	Staff employees and executives from a broad range of organizations
LEVEL 2 – GENERAL CYBERFORENSICS & MALWARE ANALYSIS **Day 1:** Course Introduction **Day 2:** Cyberthreats for Businesses – Real Examples **Day 3:** Labs – Malware Analysis Fundamentals **Day 4:** Labs – Malware Analysis Real Examples **Day 5:** Labs – Cyberforensics Basics / Mobile Infection Examples *Upon course completion, all attendees will be able to pass a certification program to validate their knowledge.*	5 days	Employees and executives with intermediate knowledge of IT security
LEVEL 3 – ADVANCED CYBER FORENSICS – FINANCIAL THREATS **Day 1:** Course Introduction **Day 2:** Types of Financial Cyberfraud **Day 3:** Labs – Cyberforencics Methodology of Financial Threats in Depth **Day 4:** Labs – Cyberforensics Techniques in Depth - Real-world online banking attack examples will be used in labs. **Day 5:** Labs – ATM Threats / Mobile Financial Fraud Investigation Examples - Real-world ATM & mTAN hijacking attacks will be used in labs. *Upon course completion, all attendees will be able to pass a certification program to validate their knowledge.*	5 days	Employees with advanced level knowledge of IT security who need to gain expertise in the cyberforensics of financial threats
LEVEL 3 – ADVANCED CYBERFORENSICS – TARGETED THREATS **Day 1:** Course Introduction **Day 2:** Targeted Attacks Introduction **Day 3:** Labs – Cyberforencics Methodology of Targeted Threats in Depth **Day 4:** Labs – Cyberforencics Techniques of Targeted Threats in Depth **Day 5:** Labs – Attack Timeline Analysis & Incident Response – Real-world online banking attack examples will be used in labs. *Upon course completion, all attendees will be able to pass a certification program to validate their knowledge.*	5 days	Employees (mostly from governmental agencies or CERTs) with advanced knowledge of IT security who need to gain expertise in the cyberforensics of targeted threats
LEVEL 3 – ADVANCED MALWARE ANALYSIS & REVERSE ENGINEERING **Day 1:** Course Introduction **Day 2:** Assembler Basics, Windows OS Internals **Day 3:** PE Format / Malware Analyst's Toolset **Day 4:** Compilers: Visual Studio; MFC; Visual Basic, .NET **Day 5:** Compilers: Delphi, GCC **Day 6:** Reverse Engineering – Object Files, Linker, PE Resources **Day 7:** Reverse Engineering – Network Analysis **Day 8:** Reverse Engineering – Malware Protection Techniques **Day 9:** Reverse Engineering – System Drivers Analysis, Rootkits and Bootkits **Day 10:** Reverse Engineering – Vulnerabilities and Exploits / Alternative OS / Web Application Analysis *Upon course completion, all attendees will be able to pass a certification program to validate their knowledge.*	10 days	Employees (mostly from governmental agencies or CERTs) with high level of knowledge of IT security and programming skills who need to gain expertise in malware analysis and reverse engineering

For more information on Cyber Security Education or other Kaspersky Services, please contact us via intelligence@kaspersky.com today!

TO LEARN MORE VISIT: **WWW.KASPERSKY.COM**