

KASPERSKY SECURITY INTELLIGENCE SERVICES. CYBERSECURITY TRAINING

CYBERSECURITY TRAINING

Leverage Kaspersky Lab's cybersecurity knowledge, experience and intelligence through these innovative training programs.

Cybersecurity awareness and education are now critical requirements for enterprises faced with an increasing volume of constantly evolving threats. Security employees need to be skilled in the advanced security techniques that form a key component of effective enterprise threat management and mitigation strategies, while all employees should have a basic awareness of the dangers and how to work securely.

Kaspersky Lab's Cybersecurity Training courses have been developed specifically for any organization looking to better protect its infrastructure and intellectual property. All training courses are offered in English.

CYBERSECURITY TRAINING

Cybersecurity Awareness It Staff Security Education

THE COURSES

NON-IT AWARENESS

IT SECURITY EDUCATION

Employees	Level 1 - Beginner		
ONLINE TRAINING PLATFORM	CORE SECURITY FUNDAMENTALS Basic IT knowledge PRACTICAL SECURITY FUNDAMENTALS WITH LABS Basic IT knowledge		
Line Managers	Level 2 - Intermediate		
CYBERSAFETY GAMES	DIGITAL FORENSICS System Administrator skills required MALWARE ANALYSIS & REVERSE ENGINEERING Programming skills required		
Business Managers	Level 3 - Advanced		
CYBERSAFETY CULTURE ASSESSMENT	ADVANCED DIGITAL FORENSICS System Administrator advanced skills required ADVANCED MALWARE ANALYSIS & REVERSE ENGINEERING Assembler skills required		

CYBERSECURITY AWARENESS

Online interactive training modules and on-site cybersafety game training for all employees who use computers or mobile devices at work, and those who manage them.

Around 80% of all cyber incidents are caused by human error. Companies are spending Millions on the cybersecurity awareness programs, but few CISOs are really satisfied with the results. What's wrong?

Most cybersecurity awareness training is too long, technical and essentially negative. This does not play to people's core strengths - their decision-making principles and learning abilities - and as a result can render training ineffectual.

So organizations are seeking more sophisticated behavioral support approaches (such as corporate culture development) that deliver a quantifiable and worthwhile return on their investment in security awareness.

Kaspersky Lab Cybersecurity Awareness courses work by:

- Changing behavior stimulating the individual's commitment to working securely, building a corporate environment where "Everybody else cares about cybersafety, so I do, too".
- Combining a motivational approach, gamification learning techniques, simulated attacks and in-depth interactive cybersecurity skills training.

HOW IT WORKS

Comprehensive but straightforward	Training covers a wide range of security issues – from how data leaks occur to internet based malware attacks and safe social networking, through a series of simple exercises.
	We use learning techniques – group dynamics, interactive modules, cartoons and gamification to make the learning process engaging.
Continuous motivation	We create teachable moments - by gamification and competition, and then re-inforce these training moments throughout the year via online simulated attack exercises, assessment and training campaigns.
Changing beliefs	We teach people that it is human beings, not machines, who are the primary targets of cybercriminals. We show how, through working in a more safety-conscious manner, individuals can avoid becoming victims and exposing themselves and their workplace to attack.
Building a corporate cybersafety culture	We train management to become security advocates; a culture where cybersecurity becomes second nature is best achieved through management commitment and example, and cannot simply be imposed by IT.
Positive and collaborative	We demonstrate how security practices make a positive contribution to business efficiency, and promote more effective cooperation with other internal departments, including the IT Security team.
Measurable	We provide tools to measure employee skills, along with corporate-level assessments analyzing staff attitudes to cybersecurity in their daily work.

IT STAFF SECURITY EDUCATION

These courses offer a broad curriculum in cybersecurity topics and techniques and assessment ranging from basic to expert. All are available either in-class on customer premises or at a local or regional Kaspersky Lab office, if applicable.

Courses are designed to include both theoretical classes and hands-on 'labs'. On completion of each course, attendees will be invited to complete an evaluation to validate their knowledge.

BEGINNER, INTERMEDIATE OR EXPERT?

The program covers everything from security fundamentals to advanced digital forensics and malware analysis, allowing organizations to improve their cybersecurity knowledge pool in three main domains:

- Fundamental knowledge of the topic
- Digital Forensics and Incident Response
- Malware Analysis & Reverse Engineering

SERVICE BENEFITS

LEVEL 1 – Core Security Fundamentals

Equip IT and Security Administrators and Managers with a basic understanding of the latest thinking on practical IT security measures from an industry leader.

LEVEL 1 – Practical Security Fundamentals

Benefit from a in-depth understanding of security though practical exercises using modern securityrelated tools.

LEVELS 2-3 – Digital Forensics

Improve the expertise of your in-house digital forensics and incident response team.

LEVELS 2-3 – Malware Analysis & Reverse Engineering

Improve the expertise of your in-house malware analysis and reverse engineering team.

HANDS-ON EXPERIENCE

From a leading security vendor, working and learning alongside our global experts who inspire participants through their own experience at the 'sharp end' of cybercrime detection and prevention.

PROGRAM DESCRIPTION

TOPICS	Duration	Skills gained
LEVEL 1 - CORE SECURITY FUNDAMENTALS		
 Cyberthreats & underground market overview Spam & phishing, email security 	2 days	Recognize security incidents and take decisions to resolve them
 Fraud protection technologies Exploits, mobile and advanced persistent threats Investigation basics using public web tools Securing your workplace 		 Reduce the load on Information Security departments
		 Increase the security level of each employer's workplace with additional tools
		Perform simple investigations
		Analyze phishing mails
		Recognize infected or fake websites

TOPICS	Duration	Skills gained			
LEVEL 1 – PRACTICAL SECURITY FUNDAMENTALS					
Security basics Open-source intelligence	5 days	Provide basic investigations, using public resources, specialist search engines and social networks			
Enterprise network security		Create a secure network perimeter			
Application security & exploit prevention		Basic penetration testing skills			
• DDoS attacks & banking threats		Inspect traffic for different types of attack			
Wireless LAN security & global mobile network		Ensure secure software development			
Banking & mobile threats		Identify malicious code injection			
Cloud and virtual environment security incident response		Undertake basic malware analysis and Digital forensics			
LEVEL 2 – GENERAL DIGITAL FORENSICS					
• Introduction to Digital Forensics	5 days	Build a Digital Forensics lab			
Live response and evidence acquisition		 Collect digital evidence and deal with it properly 			
Windows registry internals		Reconstruct an incident and use time stamps			
Windows artifacts analysisBrowsers forensics		• Find traces of intrusion based on artifacts in Windows OS			
• Email analysis		 Find and analyze browser and email history 			
		Be able be apply with the tools and instruments of digital forensics			
LEVEL 2 – GENERAL MALWARE ANALYSIS & REV	/ERSE ENGIN	NEERING			
Malware Analysis & Reverse Engineering goals and techniques	5 days	Build a secure environment for malware analysis: deploy sandbox and all necessary tools			
• Windows internals, executable files, x86 assembler		Understand principles of Windows program			
Basic static analysis techniques (strings extracting,		execution			
import analysis, PE entry points at a glance, automatic unpacking, etc.)		 Unpack, debug and analyze malicious object, identify its functions 			
Basic dynamic analysis techniques (debugging,		• Detect malicious sites through script malware analysis			
monitoring tools, traffic interception, etc.)		 Conduct express malware analysis 			
.NET, Visual Basic, Win64 files analysis					
 Script and non-PE analysis techniques (Batch files; Autoit; Python; Jscript; JavaScript; VBS) 					
LEVEL 3 – ADVANCED DIGITAL FORENSICS					
Deep Windows Forensics	5 days	Be able to perform deep file system analysis			
Data recovery		Be able to recover deleted files			
Network and cloud forensics		Be able to analyze network traffic			
Memory forensics		Reveal malicious activities from dumps			
Timeline analysis		Reconstruct the incident timeline			
Real world targeted attack forensics practice					
LEVEL 3 – ADVANCED MALWARE ANALYISIS & F	REVERSE EN	GINEERING			
Malware Analysis & Reverse Engineering goals and	5 days	Use the world best practices in reverse engineering			
techniques		Recognize anti-reverse engineering techniques			
Advanced static & dynamic analysis techniques		(obfuscation, anti-debugging)			
(manual unpacking)		Apply advanced malware analysis for Rootkits/Bootkits			
Deobfuscation techniques		Analyze exploit shellcode, embedded in different file			
• Rootkit & bootkit analysis		types			
Exploits analysis (.pdf, .doc, .swf, etc.)		Analyze non-Windows malware			
Non-Windows malware analysis (Android, Linux, Mac OS)					

