

Building your personal brand and strengthening your reputation as a cyber pro

Here's why developing cyber skills can increase your value to your employer



It's said you must practice something for 10,000 hours to master it. Most of us, however, don't have that kind of time. Our families, jobs and social lives dictate our learning capacity, and so we settle for competence instead of mastery, learning smart rather than at length. In security this isn't a bad thing. Upskilling for 10,000 hours would likely put you among the industry's elite, but the relevance of your knowledge would quickly decline. You couldn't just stop upskilling and stay a ninja, because in a year's time you'd encounter tools and techniques totally alien to you. Learning continuously is therefore far more important.

This need for continuous upskilling exists because cyber moves quickly and bad actors innovate constantly. It's why patch Tuesday – when companies release fixes for emerging vulnerabilities – is practiced religiously by Microsoft, which sometimes addresses [100 or more issues](#) simultaneously. When mitigating one risk another fast emerges, making cyberthreats to businesses what the hydra was to Heracles.

Having people with the skills to address these evolving threats couldn't be more important, but this is proving one of the great dilemmas of modern business. In 2022, for example, there was a cybersecurity skills shortage in [nearly 700,000 UK businesses](#), meaning those responsible for security weren't confident executing the tasks laid out in the government's [Cyber Essentials](#) scheme. This lack of demonstrable expertise puts companies at risk, but for ambitious employees, it also creates opportunity.

Why is there a cyber skills gap?

Historically, investment in security technology has dwarfed investment in human capability. This is likely down to the way leaders view traditional training methods and certifications; are the skills taught, for example, relevant to their business's specific risk profile? Are they good value for money? As long as these questions are up for debate, people will remain an afterthought.

Right now, then, it's clear that maximizing the effectiveness of human capability is front and center in staying resilient in the face of adversaries. And because security skills are in short supply, there is scope for those in small-to-medium sized businesses (SMBs) to step up and be counted – whether they are coming from IT, engineering or even a non-technical department.

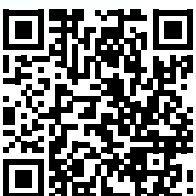
That's because people with the aptitude for cybersecurity (think persistence, ingenuity and problem solving) need only the right tools to begin realizing their potential. Prior experience isn't necessary.

How you can help plug the cyber skills gap

You might be considering upskilling but wondering whether it's worth it. If your company has a security solution installed, after all, what can you add? Well, a robust cybersecurity posture unites technology, process and people – there is no silver bullet. The world's best security team is useless without technology, just as technology is useless without someone to implement it.

Download our [step-by-step guide to mitigating cyber risk in the business](#)

now



Our research shows that **90% of employees** overestimate their existing cybersecurity capability.

Respond to modern cybersecurity challenges resourcefully.

Security simplified: a step-by-step guide to mitigating cyber risk in the business

kaspersky BRING ON THE FUTURE

Cybersecurity training may be low on the agenda of your business if it has a limited IT function, but an organization's people are its frontline, so its entire staff should have a grounding in security. The ability to spot techniques that leverage human error – take phishing, for example, which [accounts for 83% of UK cyberattacks](#) – is crucial.

If you're part of IT, you work on service desks or are somewhat technical, upskilling is even more important, and you should be developing your capability **beyond** standard security awareness. Equally important is training for your personal brand and career development.

What, and how, you'll learn with Kaspersky Endpoint Security Cloud Pro

Cyber training that needs people to attend a certain venue on set days isn't conducive to creativity, and it fails to factor in something we all crave: a good work-life balance. Kaspersky Endpoint Security Cloud Pro's bespoke training modules are available on demand with no registration required. You can upskill on your own terms and at a cadence that suits you. (We recommend continuous upskilling, because unlike computer games where each boss beatdown gets you closer to 100%, there's no endgame in security.)

By choosing Kaspersky Endpoint Security Cloud Pro as your technical security solution, your business will automatically be investing in its human potential. And this is crucial right now, considering the following challenges when hiring and retaining advanced security talent:

- High compensation demands
- Your business's bespoke skill requirements
- Recruitment costs
- Candidates' work-life balance concerns

We're of course hopeful that our customers, who benefit from [100% ransomware protection](#), won't need the skills they learn from our experts – but any vendor promising invincibility is lying. People must work in tandem with technology to protect an organization, and our easy-to-use training interface is designed to help you defend your organization from day one.

Module	knowledge you'll gain	skills you'll learn
Malicious software	<ul style="list-style-type: none"> • Malware techniques and classification • Malicious and suspicious software actions and signs • Heuristic analysis basics 	<ul style="list-style-type: none"> • Verification of the existence or absence of a malware-related incident
Potentially unwanted programs and files (PUPs)	<ul style="list-style-type: none"> • The basics of statistical and dynamic analysis of software samples and suspicious documents 	<ul style="list-style-type: none"> • Working with system and sandbox event monitors • Using statistical engines • Removing PUPs
Investigation basics	<ul style="list-style-type: none"> • The Incident Response process • Methods of log analysis • Specifics of storing digital information 	<ul style="list-style-type: none"> • Collecting digital evidence • NetFlow traffic analysis • Timeline analysis • Event log analysis
Phishing and open source intelligence (OSINT)	<ul style="list-style-type: none"> • Modern phishing methods • Methods of analysis for email headers 	<ul style="list-style-type: none"> • Phishing email analysis and deleting obfuscated phishing emails from users' mailboxes • Open source intelligence for understanding what hackers know about your company
Server security	<ul style="list-style-type: none"> • Analyze the network environment • Server hardening • Analyze PowerShell logs to detect attacks 	<ul style="list-style-type: none"> • Search for vulnerable and non-standard network services • Configure systems according to the "default deny" principle • Search for signs of an attack in PowerShell logs
Active Directory security	<ul style="list-style-type: none"> • Use an API to check passwords in a database of compromised passwords • Configure domain policies according to recommendations • Methods for analyzing Active Directory domain security 	<ul style="list-style-type: none"> • Safely check for password hashes in a database • Search for inconsistencies between recommended and actual domain policies • Assess the security of Active Directory settings



Whenever you complete a module you'll be awarded a **Kaspersky certificate**, so you can prove your increasing value to your employer. Better still, you'll learn using practical methods that build muscle memory in preparation for the real thing, getting hands-on with threats based on exclusive Kaspersky research.

If you'd like to test-run our training and start increasing your own value, share this link with the decision-maker in your organization today so they can see all the benefits of Kaspersky Endpoint Security Cloud Pro.

[Learn more](#) about training with Kaspersky and reducing cyber risk in the business.

"The thing I liked most of all is the virtual lab environment. Thanks to it, you can immediately start solving exercises without the need to install any software"


[Kaspersky cybersecurity training user](#)




Cyberthreats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise
Threat Intelligence Portal: opentip.kaspersky.com
Interactive Portfolio Tool: kaspersky.com/int_portfolio

www.kaspersky.com

© 2023 AO Kaspersky Lab.
Registered trademarks and service marks are the property of their respective owners.



We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.



Proven. Transparent. Independent.

Know more at kaspersky.com/about/transparency