# Kaspersky launches new training courses to bolster cybersecurity in healthcare and supply chains



Kaspersky has announced a significant enhancement to its Kaspersky Automated Security Awareness Platform (ASAP) with the introduction of three specialised training courses aimed at bolstering cybersecurity skills across various sectors. This initiative addresses the rising tide of cyberattacks, particularly those targeting critical areas such as healthcare, supply chains, and executive levels within businesses.

As highlighted by the Kaspersky IT Security Economics report, 2023 has marked a shift towards focusing on supply chain resilience as a priority for IT security teams, with many organisations acknowledging the pressing need for improved oversight of their suppliers. Reports indicate that certain healthcare institutions are experiencing an alarming rate of cyber incidents, averaging 18 per year, in a sector noted for its low security maturity and funding.

The first of the new courses, titled "Attacks on top managers and on behalf of top managers: whaling and its impact," educates executives on sophisticated phishing schemes specifically targeting high-ranking officials. This training highlights how cybercriminals meticulously prepare these attacks to exploit the resources and authority of top management before impersonating them to extract sensitive information from employees.

The second course, "Information security in healthcare," addresses the sector's unique cybersecurity challenges. By emphasising the critical nature of data protection in safeguarding lives, this training covers foundational security principles along with practical guidance on secure medical data handling and compliance with legal requirements.

The third course, "Supply chain attacks," focuses on the vulnerabilities associated with external vendors and suppliers. It provides organisations with strategies to identify risks and implement necessary safeguards to protect interconnected systems from these increasingly common cyber threats.

Tatyana Shumaylova, Senior Product Marketing Manager at Kaspersky Security Awareness, commented, "As cyber threats evolve, so must our strategies to counter them. By equipping employees with both the knowledge and practical tools to mitigate these risks, we empower organisations to stay one step ahead of attackers." She underscored that enhancing employee cybersecurity skills is essential to any organisation's broader defence strategy.

In parallel developments within the financial sector, J.P. Morgan Payments unveiled its new biometric payment terminals, the J.P. Morgan Paypad™ and J.P. Morgan Pinpad™, at the NRF 2025 retail conference. These innovative all-in-one devices incorporate facial and palm biometric recognition, tailored to provide seamless transaction experiences across various industries including retail and hospitality. According to Jean-Marc Thienpont, Managing Director of Omnichannel & Biometric Solutions at J.P. Morgan Payments, these terminals are fundamental in transforming commerce, providing a frictionless solution that enhances customers' trust.

Scheduled for a pilot launch later this year, the Paypad and Pinpad are engineered to streamline payment processes while ensuring a high level of security, accommodating multiple payment methods including biometric authentication.

As preparations for Identity Week Europe 2025 continue, the focus shifts towards the evolving landscape of Identity and Access Management (IAM) in retail. This event, set for June 2025 in Amsterdam, aims to provide valuable insights into how retailers can maintain security while delivering seamless and personalised services. Notable discussions will include harnessing cloud-based IAM architecture and advancing towards a passwordless authentication future.

The digital identity space is also experiencing advancements, as evidenced by the establishment of the Humanity Foundation, which aims to foster the adoption of decentralised identity technologies. The foundation will support the Humanity Protocol, a blockchain-based identity system that utilises privacy-preserving biometrics to establish human uniqueness.

In a noteworthy collaboration, GLEIF (Global Legal Entity Identifier Foundation) has partnered with the UK's Companies House to enhance the identifiability of businesses through Legal Entity Identifiers (LEIs). This new initiative simplifies the process for LEI data users to access vital business registration data, subsequently improving due diligence practices.

Additionally, Italy has made strides in its immigration policies, now mandating biometric data for long-term visa applicants, a move seen as enhancing security despite potential delays in the processing times for applicants.

The government's focus on artificial intelligence (AI) has gained prominence recently, as Keir Starmer articulated his vision of the UK emerging as a global leader in AI innovation. Pledging significant investment in AI growth, Starmer envisions a future where AI technologies enhance public services and drive economic growth, signalling an ambitious effort to place the UK at the forefront of AI development.

In the technology sector, Relx has pivoted towards AI-powered fraud detection, emphasising automated identity verification processes that are becoming increasingly essential in financial transactions.

Finally, the growing threats posed by deepfakes on surveillance and security systems signal a pressing need for innovation in protective measures. The integration of advanced AI and blockchain technologies could bolster the integrity of security footage, highlighting the critical intersection between enhanced security measures and emerging technologies.

In summary, these trends across various sectors illustrate a collective move towards leveraging emerging technologies, such as AI and biometrics, to cope with evolving digital challenges, enhance security protocols, and foster a more resilient business environment.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

* <https://www.kaspersky.co.za/about/press-releases/kaspersky-automated-security-awareness-platform-expands-its-courses-with-three-new-cybersecurity-topics> - Corroborates the introduction of three new specialised training courses in the Kaspersky Automated Security Awareness Platform, focusing on attacks on top managers, information security in healthcare, and supply chain attacks.
* <https://www.kaspersky.co.za/about/press-releases/kaspersky-automated-security-awareness-platform-expands-its-courses-with-three-new-cybersecurity-topics> - Supports the information on the rising tide of cyberattacks, particularly those targeting healthcare, supply chains, and executive levels, as highlighted by the Kaspersky IT Security Economics report.
* <https://www.kaspersky.com/small-to-medium-business-security/security-awareness-platform> - Provides details on the Kaspersky Automated Security Awareness Platform, including its features and the importance of enhancing employee cybersecurity skills.
* <https://www.kaspersky.com/about/press-releases/kasperskys-award-winning-security-awareness-now-offered-on-premises> - Explains the on-premises model of the Kaspersky Automated Security Awareness Platform and its benefits for companies requiring high levels of confidentiality and compliance.
* <https://www.kaspersky.co.za/about/press-releases/kaspersky-automated-security-awareness-platform-expands-its-courses-with-three-new-cybersecurity-topics> - Quotes Tatyana Shumaylova, Senior Product Marketing Manager at Kaspersky Security Awareness, on the importance of evolving strategies to counter cyber threats.
* <https://www.kaspersky.co.za/about/press-releases/kaspersky-automated-security-awareness-platform-expands-its-courses-with-three-new-cybersecurity-topics> - Details the specific courses, including 'Attacks on top managers and on behalf of top managers: whaling and its impact,' 'Information security in healthcare,' and 'Supply chain attacks.'
* <https://www.kaspersky.com/about/press-releases/kasperskys-award-winning-security-awareness-now-offered-on-premises> - Highlights the significance of supply chain resilience and the low security maturity and funding in the healthcare sector.
* <https://www.kaspersky.co.za/about/press-releases/kaspersky-automated-security-awareness-platform-expands-its-courses-with-three-new-cybersecurity-topics> - Discusses the strategies and practical tools provided in the new courses to mitigate cyber risks and enhance cybersecurity skills.
* <https://www.kaspersky.com/small-to-medium-business-security/security-awareness-platform> - Explains the features of the Kaspersky Automated Security Awareness Platform, including simulated phishing attacks and detailed reporting.
* <https://www.kaspersky.com/about/press-releases/kasperskys-award-winning-security-awareness-now-offered-on-premises> - Mentions the importance of digital literacy and the need for cybersecurity training across all employee levels in various sectors.
* <https://news.google.com/rss/articles/CBMia0FVX3lxTFA4MHg4WlJueGNRNXF1RjhhNldvQUNZTjNUdUlZYkpfUXNQNnlUZUxyaUZjb0gtN0YxNVdscnN4SGVqMm5mMk0zUWVBTWZhd1NYM2JYLUQ3a1BCZ0ZnUnlsbmxUUlpTNnBJdHBz?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data
* <https://news.google.com/rss/articles/CBMiZ0FVX3lxTE9hOVJlZkdYYU91c3k4aDg4WWVFLWJoVDlfLWVleGxpcTJUcXRYME9YQ0szUzQ3MVV5MmVDckpQUDM2b2xUaG9JYTI2cDI2WnpZelAwODEyNWNpenVQalNyVEtsdk5nV0E?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data