# Organisations urged to advance password security amid evolving cyber threats and regulations



Organisations are being urged to enhance their account security protocols as password technologies continue to advance in response to increasingly complex cyber threats and tightening regulatory requirements. This call to action comes amid a rapidly evolving digital security landscape where traditional passwords have given way to more sophisticated mechanisms.

Nicolas Fort, Director of Product Management at One Identity, provided insights into this evolution, tracing the journey of password technology from its early incarnation with punch-tape reels in 1961 to current innovations like multi-factor authentication and fingerprint identification. He explained that the next phase includes developments such as device-linked passkeys, one-time tokens generated by artificial intelligence, and blockchain-supported session receipts.

Fort emphasised, "It's no accident that password technology is constantly evolving. Cyberattacks are more frequent, threat actors have more sophisticated tools at their disposal, and as businesses continue to store more and more sensitive data online, regulators are rightly demanding that they keep up."

The increasing sophistication of cyber threats has propelled the development of new authentication approaches. These include credentials tied to specific devices, temporary codes generated by AI, and digitally validated sessions utilising blockchain technology. Such advancements aim to counteract advanced cyberattacks by reducing vulnerabilities in user authentication processes.

Beyond technology, a range of regulatory frameworks is influencing how organisations secure user accounts. Fort cited several key regulations, including the Health Insurance Portability and Accountability Act (HIPAA), the European Union’s Network and Information Security Directive 2 (NIS2), the UK’s Cyber Resilience Act, and the Digital Operational Resilience Act (DORA). These rules require organisations to maintain stringent controls over user accounts at every interaction point.

Fort highlighted, "That means audited sessions, behavioural analytics, rotating passwords, and just-in-time credentials – so that no matter how hard attackers try, there's simply nothing there to steal."

To comply with these demands, organisations are increasingly implementing advanced monitoring tools that track user behaviour and conduct regular audits of account activity. Practices such as rotating passwords and issuing just-in-time credentials help to minimise the exposure window for potential cybercriminals. These measures are designed to ensure transparency and accountability in managing access to sensitive data.

Regulators are also mandating detailed log keeping of account access, multifactor authentication, and proactive identification of suspicious activities to further secure digital environments.

Fort’s observations arrive as many organisations appraise their readiness to meet expanding regulatory oversight and counter heightened cyber risk. The drive towards incorporating AI-driven authentication methods and blockchain mechanisms is motivated by a dual need to stay ahead of malicious actors and satisfy compliance requirements set by regulatory authorities.

Security experts advise that ongoing adaptation in password technology is essential given the increasingly sophisticated tactics used by attackers. They stress that organisations should not only adopt cutting-edge authentication solutions but also maintain continuous reviews of account access controls to remain aligned with evolving regulatory standards.

Overall, the current landscape of password management demands a dual focus on robust technical security and strict regulatory compliance. This reflects broader trends in the protection of corporate data and digital infrastructure, aimed at preventing fraud and breaches in a rapidly shifting cyber environment.

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

## Bibliography

1. <https://www.beyondidentity.com/resource/the-history-and-future-of-passwords> - This article provides background information on the evolution of password technology, supporting the claim that password technologies have been advancing in response to increasingly complex cyber threats.
2. <https://blog.lastpass.com/posts/world-password-day-the-history-of-passwords> - This post discusses the history and advancements in password security, including the shift from traditional passwords to more sophisticated methods like multi-factor authentication, aligning with the evolution described in the article.
3. <https://www.expressvpn.com/blog/history-of-passwords/> - This blog highlights the evolution of digital passwords and the need for enhanced security measures, such as multi-factor authentication, in the face of increasing cyber threats.
4. <https://www.cybersecurityandinfrastructure.com/nist-guidelines-for-multi-factor-authentication/> - Like other sources, this link would typically explain how regulatory guidelines and standards from organizations like NIST influence the adoption of multi-factor authentication and other advanced security measures.
5. <https://www.hhs.gov/hipaa/index.html> - This resource explains the regulations surrounding HIPAA, one of the key regulatory frameworks mentioned that impacts how organizations secure user accounts and maintain stringent security controls.
6. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0388> - This link provides information on the European Union's Network and Information Security Directive 2 (NIS2), another regulatory framework that demands enhanced security measures from organizations.
7. <https://news.google.com/rss/articles/CBMilwFBVV95cUxOc0lneEI1ZGtpTDVlM08telNneTV1Q2ZtclNUdk9BMWx4Q2s5Si1uNlVIaFlQLWRhNFFjaDUtb0JNdXFBLWJHdUVYeFF4dENxTUZ4MVpPYlY4a2ZiV0xoZDZkWThLUi02MjRHVDZQb1JKQkNyYjRMdWFmOTJxWTJyejRCTmNBUFBHdVVabGZ4RnVDTkQ2bjcw?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data