# Concerns over social media security grow among younger generations



Recent research conducted by Yubico, a provider of hardware authentication security keys, indicates significant concerns among younger generations regarding the security of their social media accounts. As stated in findings reported by BetaNews, nearly half of Generation Z (47 per cent) and Millennials (46 per cent) have experienced instances of their social media account passwords being hacked.

The survey underscores a noticeable shift in attitude towards traditional password usage, with a marked inclination towards adopting hardware security keys, indicative of a growing scepticism surrounding conventional digital authentication methods. This reflects a wider trend among respondents, where 42 per cent question whether organisations are adequately safeguarding their data.

Particularly noteworthy is the heightened vigilance among Gen Z respondents, with 73 per cent voicing concerns over the potential of AI-powered cyberattacks. The implications of artificial intelligence in the context of cybersecurity appear to resonate strongly, as 72 per cent of all survey participants believe that online scams and phishing attacks have evolved to be more sophisticated due to AI technologies. Furthermore, 66 per cent acknowledge that such attacks have become more effective because of AI, while 58 per cent express worry regarding AI's impact on the security of both personal and business accounts.

The authors of the report stress the importance of a cohesive cybersecurity strategy that unifies personal and professional security measures. They suggest that organisations must take proactive steps to educate employees on best practices and encourage the adoption of more secure authentication methods, such as hardware security keys and passkeys. The need for consistent training and application of security protocols among all employees is seen as vital for fostering "phishing-resistant users."

As the digital landscape continues to evolve, with increasing threats stemming from advancements in technology, the embrace of emerging solutions like hardware security keys is positioned as essential for maintaining the security of digital identities and the systems on which businesses depend. For those interested in further details, the comprehensive findings of the 2024 State of Authentication Survey can be accessed on the Yubico website, along with an illustrative infographic summarising the key insights.

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

## Bibliography

1. <https://www.yubico.com/blog/state-of-global-authenticageion-a-look-at-cybersecurity-habits-by-generations/> - Corroborates the findings that nearly half of Gen Z (47%) and Millennials (46%) have had their social media account passwords hacked, and highlights the shift towards hardware security keys and concerns about AI-powered cyberattacks.
2. <https://www.yubico.com/blog/state-of-global-authenticageion-a-look-at-cybersecurity-habits-by-generations/> - Supports the trend of growing skepticism towards traditional password usage and the increased adoption of hardware security keys among younger generations.
3. <https://www.yubico.com/blog/state-of-global-authenticageion-a-look-at-cybersecurity-habits-by-generations/> - Confirms that 42% of respondents question whether organizations are doing enough to protect their data.
4. <https://www.yubico.com/blog/state-of-global-authenticageion-a-look-at-cybersecurity-habits-by-generations/> - Highlights Gen Z's heightened vigilance, with 73% concerned about AI’s role in cyberattacks and their increased use of MFA compared to other generations.
5. <https://www.yubico.com/blog/2024-global-state-of-authentication-survey-qa-with-yubico-vp-derek-hanson-on-a-passkey-future/> - Discusses the broader impacts and trends on individuals and businesses, emphasizing the need for a cohesive cybersecurity strategy and the adoption of more secure authentication methods like hardware security keys and passkeys.
6. <https://www.yubico.com/blog/state-of-global-authenticageion-a-look-at-cybersecurity-habits-by-generations/> - Supports the importance of educating employees on best practices and encouraging the adoption of more secure authentication methods to foster 'phishing-resistant users'.
7. <https://www.yubico.com/blog/state-of-global-authenticageion-a-look-at-cybersecurity-habits-by-generations/> - Emphasizes the evolving digital landscape and the increasing threats from advancements in technology, highlighting the necessity of embracing emerging solutions like hardware security keys.
8. <https://blog.lastpass.com/posts/a-look-into-online-security-through-the-ages> - Provides additional context on Gen Z's password practices, noting that despite their confidence in online security, many have poor password hygiene.
9. <https://secureframe.com/blog/password-statistics> - Supports the general trend of poor password practices, including the reuse of passwords and the susceptibility of Gen Z to credential-stuffing cyberattacks.
10. <https://www.yubico.com/blog/state-of-global-authenticageion-a-look-at-cybersecurity-habits-by-generations/> - Highlights the difference in beliefs about effective cybersecurity methods between generations, such as the reliance on usernames and passwords.
11. <https://www.yubico.com/blog/2024-global-state-of-authentication-survey-qa-with-yubico-vp-derek-hanson-on-a-passkey-future/> - Provides further details on the 2024 State of Authentication Survey and the importance of unified personal and professional security measures.
12. <https://betanews.com/2025/01/07/almost-half-gen-z-and-millennials-have-had-their-social-media-passwords-hacked/> - Please view link - unable to able to access data