Global State of Authentication Survey 2025

Perceptions Vs. Reality: Gaps In Authentication Security

Insights by Yubico

yubico

Table of Contents

Introduction

Cybersecurity threats present an ever-evolving danger to enterprises of all sizes, but many organizations are slow to react to new and emerging risks. Indeed, many employees and companies now believe that legacy security protocols are as effective today as they were months or even years ago. Unfortunately, this perception does not match reality.

Rising threats from artificial intelligence (AI) -powered attacks, combined with outdated cybersecurity guidelines and high-risk employee habits, have left countless organizations vulnerable to security breaches. Yubico's survey explored individuals' cybersecurity habits in both their workplace and personal lives. It also examined the dangers of weak security practices and evaluated the growing concerns around emerging technologies like AI and their implications for both organizational and individual security.

Executive Summary

Yubico commissioned a global survey of 18,000 employed adults from Australia, India, Japan, France, Germany, Singapore, Sweden, the United Kingdom, and the United States, revealing fundamental failings in organizational security, driven by a misalignment between what employees and their companies perceive as secure and the reality of their vulnerability to modern cyber threats.

Close to half of those surveyed have never received cybersecurity training and are still utilizing authentication methods that, while once considered secure, are now easily bypassed by sophisticated attacks like phishing. Passwords, SMS-based verification, and even basic multi-factor authentication (MFA) are increasingly vulnerable and present weak spots for cybercriminals to target.

Perhaps more telling, personal security habits are undermining protection protocols of enterprises as well, with 50% of employees using personal accounts on work devices, and vice versa. Further, nearly one-third of respondents do not utilize MFA in any form outside of work, setting the stage for hackers to potentially leverage personal information in attempts to target enterprises.

The rapid growth and adoption of AI by bad actors has dramatically quickened the pace at which new threats emerge. Our findings indicate that those surveyed are aware of this new reality, with 76% concerned that their accounts are now at a much higher risk of attack — a large increase over the 58% that felt this way in a similar 2024 report.

18,000+

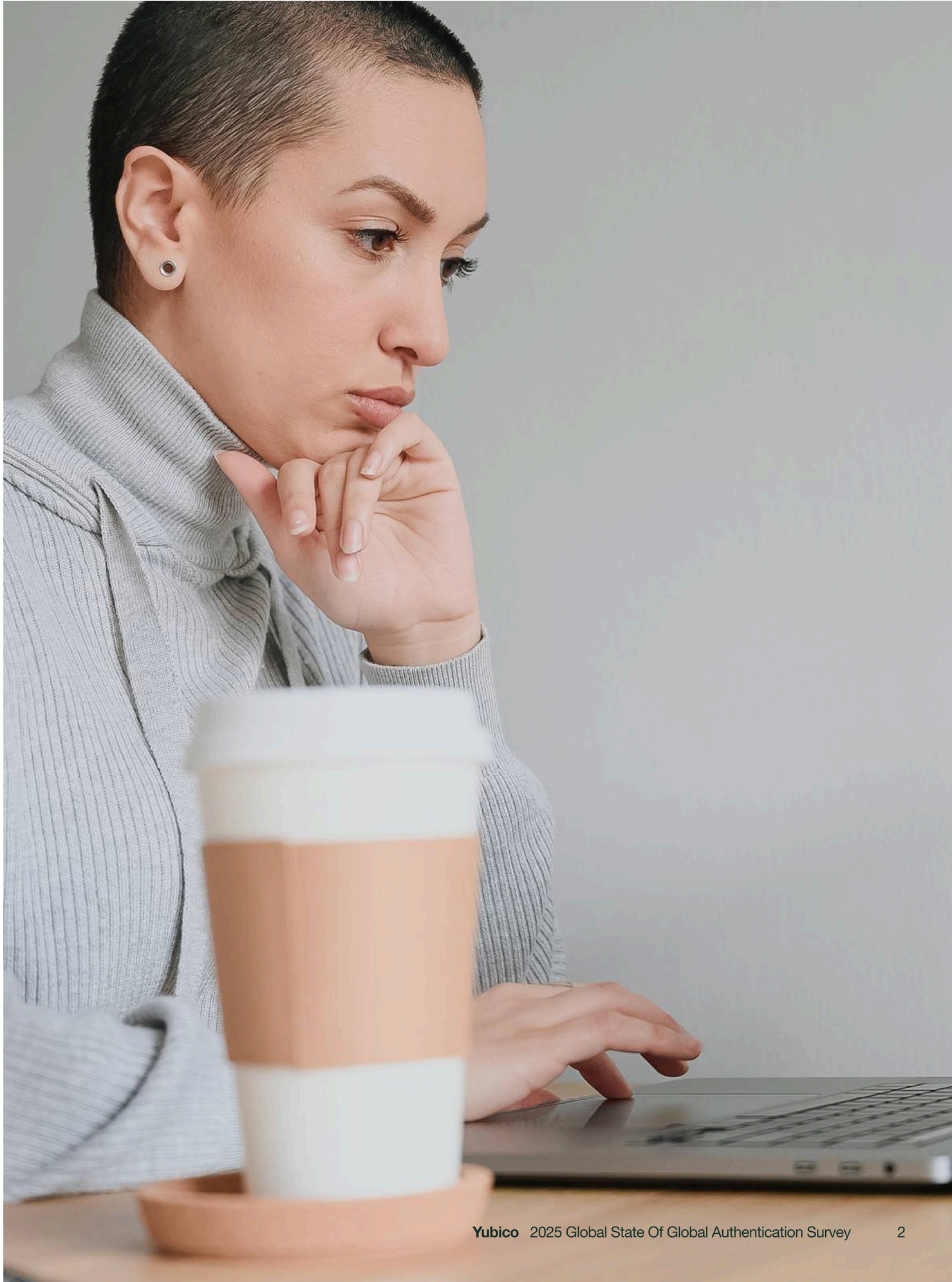
Responses

9

Countries

I.

The New Cyber Landscape



A Global Cybersecurity Wake-Up Call

Our research finds that 4 in 10 (40%) employees have never received training on cybersecurity in any form. Furthermore, 44% of companies wait longer than 3-5 months to update their cybersecurity policies.

These two statistics suggest that close to half of employees were never introduced to their company's security guidelines in the first place, and roughly half of those that were given cybersecurity training are operating on outdated information.

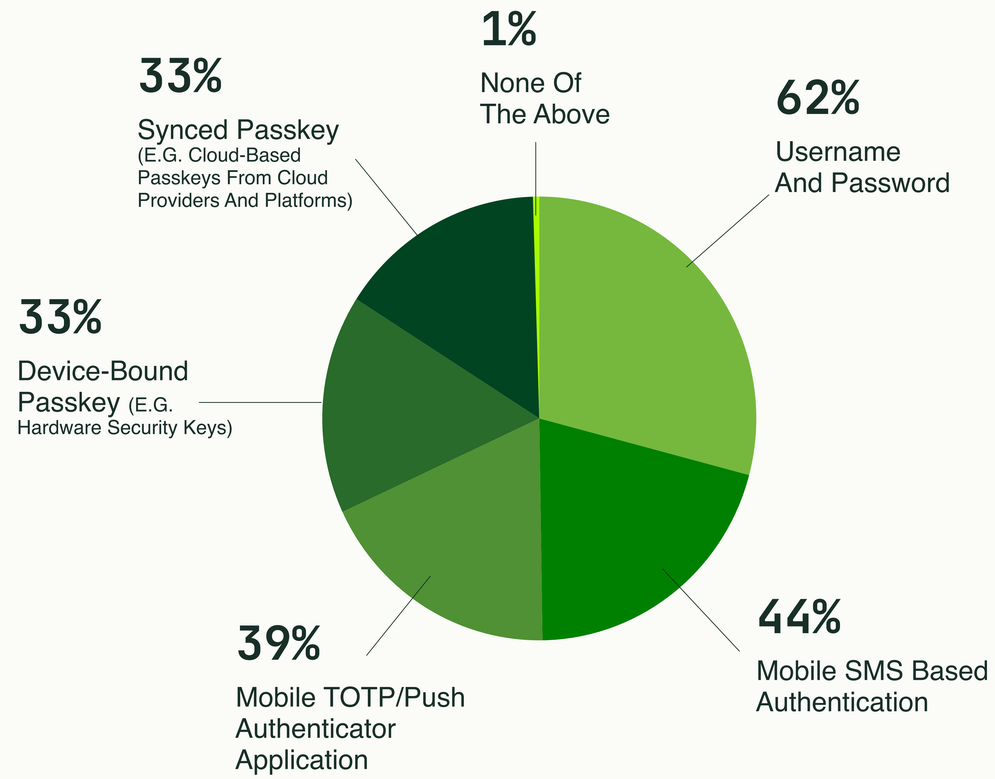
With new attack techniques emerging on a near-constant basis and the rise of AI-based threats, inconsistent cybersecurity training habits leave many organizations and their workforce in a constant state of vulnerability.

Inconsistent Authentication

Further complicating the risk profile of modern enterprise systems is how they inconsistently use authentication. Companies that provide employees with multiple types of authentication to apps and services create a weaker defense against potential vulnerabilities.

Perhaps more eye-opening, 62% of organizations still rely primarily on username/password credentials despite the vast evidence that this outdated technology is increasingly vulnerable. Another 44% of companies utilize SMS-based one-time passwords (OTPs), which are susceptible to SIM swapping attacks and social engineering that, thanks to AI, is now more sophisticated.

Which forms of authentication does your company use across different applications/ programs used by the company?



Perceptions vs. Reality

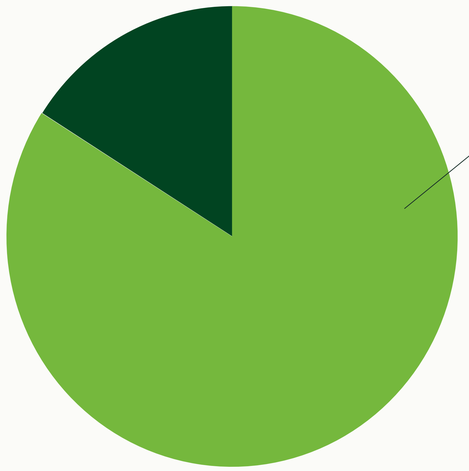
Our findings show that employees consistently **underestimate** risks to their secure login information and **overestimate** the capabilities of the systems meant to protect them.

In our research, SMS authentication was perceived to be the most secure method by 41% of respondents, while 33% considered time-sensitive OTPs through dedicated mobile apps to be the most secure. While these methods are better than nothing, they are highly vulnerable to threats ranging from social engineering to SIM swapping and even mobile device theft. Surprisingly, over a quarter (26%) of respondents still believe passwords, which are highly susceptible to phishing attacks, are the most secure.

Device-bound passkeys, like those on hardware security keys, were perceived as the most secure by just 30% of respondents, despite being highly effective against a variety of attack types. These misconceptions influence both individual security choices as well as overarching organizational policies, increasing vulnerability across an entire enterprise.

Despite these vulnerabilities, 84% of respondents whose companies' security measures differ based on role still believe their company's cybersecurity is as secure as it needs to be, showing misplaced confidence as all levels of an organization need to be treated the same for cybersecurity tools to be effective.

Despite vulnerabilities, 84% of respondents whose companies' security measures differ based on role and requirement still believe their company's cybersecurity is as secure as it needs to be, showing overconfidence.



84%

still believe their company's cybersecurity is as secure as it needs to be

What Is The Most Secure Method Of Authentication?

Hardware security keys are widely regarded as the most secure form of authentication. These small, physical devices must be in your possession to verify your identity–making them highly effective at preventing phishing attacks and identity theft. Device-bound passkeys, a type stored on a hardware security key, are considered the "gold standard."

Personal Habits Jeopardize Enterprise Security

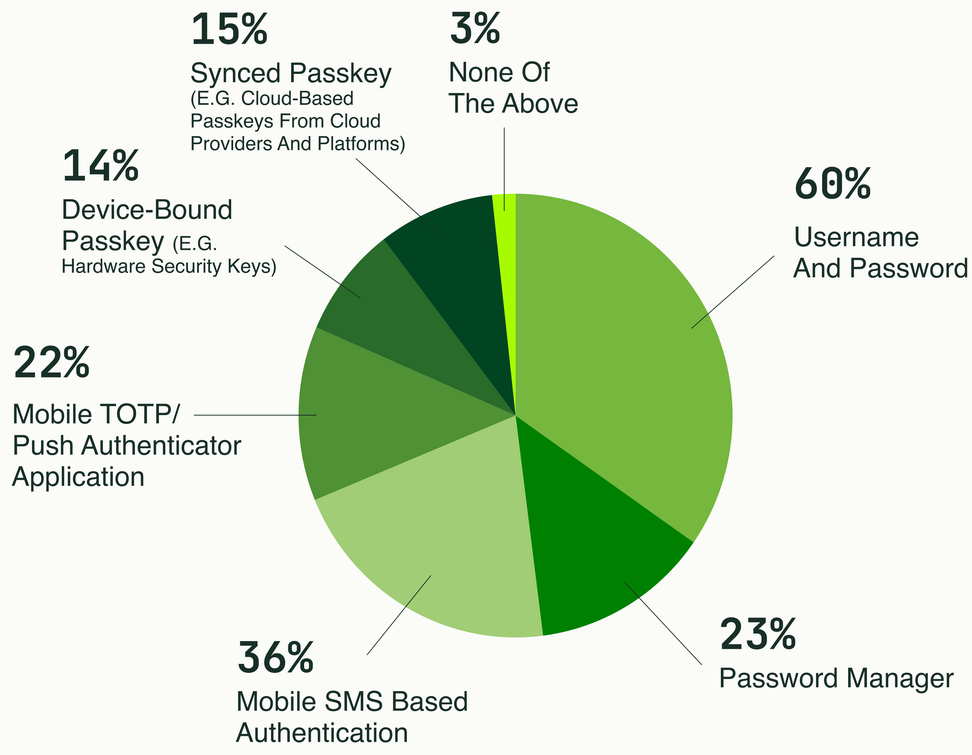
The line between personal and professional lives is increasingly blurred, and the cybersecurity habits of workers at home can quickly create risks for employers. Our findings reveal a strong overlap between personal and professional device usage, with 40% of employees utilizing their work devices to check personal email accounts and an equally troubling 40% accessing their work email from their personal devices. These habits create multiple pathways for attackers to breach professional accounts without directly attacking a corporate target.

Considering that 29% of respondents do not utilize MFA options on their personal email accounts, this creates weak points that can be exploited by bad actors to access professional systems, conduct highly targeted phishing attacks against colleagues, and mine personal information for social engineering purposes.

Unsurprisingly, personal authentication habits closely resemble the trends observed in enterprise environments: The most common methods of personal account security are passwords (60%), and SMS (36%). Only 14% of individuals use device-bound passkeys for personal accounts.

> Employees use personal devices for work and work devices for personal activities, turning a personal security misstep into a potential enterprise vulnerability. Personal and professional cybersecurity hygiene should go hand in hand, and be a benefit to each other."
>
> **Ronnie Manning, chief brand advocate, Yubico**

How do you authenticate/login to your personal accounts?



United States Spotlight

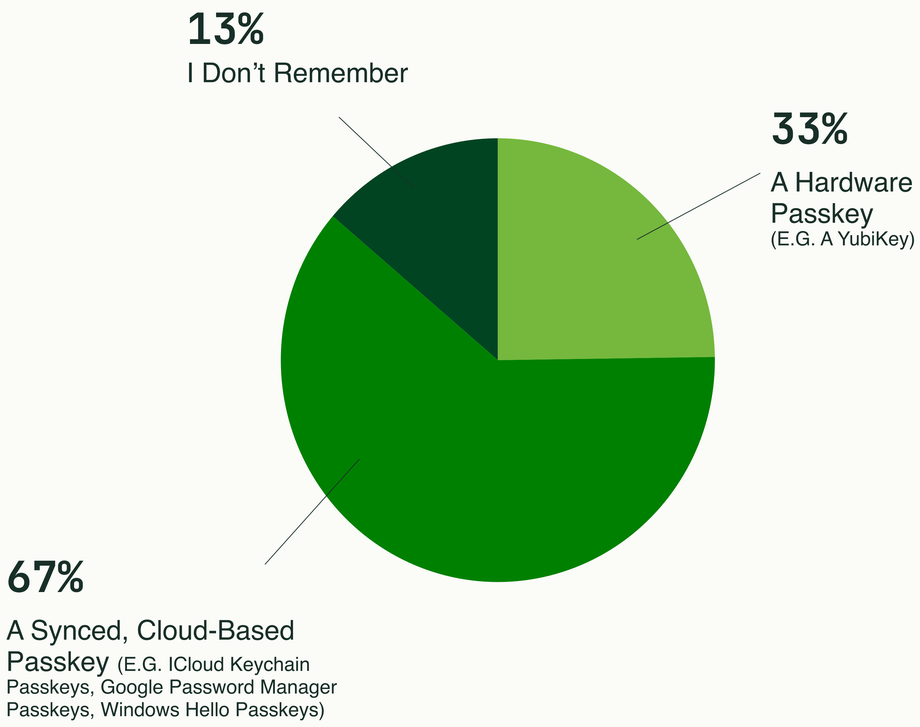
The United States' cybersecurity landscape reveals both progress and significant challenges in enterprise authentication.

Starting with the positives, an encouraging 33% of US respondents who are familiar with passkeys in general have used the more secure type of passkey, the device-bound passkey, which has a significantly higher adoption rate than most of the other regions we surveyed. This signals a greater awareness of more advanced authentication options and is likely driven by the large focus on technology in day-to-day life.

However, any technological advantage is undermined by inconsistent authentication practices within organizations: 44% of US respondents say that their security measures differ based on title and role, creating uneven protection resulting in more potential vulnerabilities.

Perhaps even more notable, 58% of US employees use personal devices for work accounts — a nearly 10% increase over the global average.

What types of passkeys have you used?



Confidence In Advanced Authentication Methods Is Growing:

In the US, 34% of respondents now believe device bound passkeys are the most secure authentication methods, up from 18% in 2024, an 18-point increase.

AI Has Supercharged Cyber Attacks

AI allows an individual to do more in a shorter amount of time. While it has positive features within the workplace, such as productivity and growth, it has also transformed the threat landscape. The barrier to conducting sophisticated attacks is now dramatically lower, and AI-powered tools provide even unskilled attackers with the ability to inflict considerable damage.

AI's ability to bolster cybercrime extends beyond automated tools or bots, as it enables attackers to draft highly convincing phishing emails, customize them to individual targets, and dramatically increase their chances of success. Hackers with no programming experience can build fake websites that are virtually identical to the real thing, create deepfake video and audio files to trick colleagues, and do it all with speed and at scale.

The good news is that many people are indeed aware of the growth of online scams and phishing in the face of AI, with 78% of respondents saying they are aware of new dangers and 70% believing that these types of attacks are more successful. These figures align with observations of global cyber threats and suggest that most recognize the rapidly changing threat landscape, despite a lack of action by their organizations.

Encouragingly, 76% of those surveyed expressed concern about AI impacting the security of their personal or professional accounts. This is an 18% increase over the previous survey period where, in a survey from 2024, Talker and Yubico found that just 58% of respondents were similarly concerned, suggesting a fast-growing awareness of the risks posed by AI.

> AI is actively rewriting the rules of cybercrime, making it easier for bad actors to launch sophisticated and highly targeted attacks. Organizations that utilize basic authentication methods like passwords and SMS are going to find themselves behind the curve. It's clear that the time is now for companies to modernize and adopt security methods that are proven against today's threats."
>
> **Ronnie Manning, chief brand advocate, Yubico**

Blurred Lines Between Human and AI Communication

One of the key threats AI poses in the realm of cybersecurity is its uncanny ability to mimic human communication patterns. This unsettling capability negates one of the most efficient ways of filtering out phishing attacks: Identifying suspicious or unusual dialogue.

We found that of those who have been tricked by phishing messages, 34% of respondents said the reason they fell for the ruse was that it appeared to come from a trusted source. With AI's ability to cater to specific individuals and draw from vast amounts of data, this finding shows how AI is allowing these types of threats to grow and become more successful.

Our data shows that most individuals also struggle to differentiate between human and AI-generated content. When presented with sample messages, just 30% of respondents correctly identified a human-written message, with 70% incorrectly attributing it to AI or were unsure. Conversely, 54% of respondents either misidentified or could not identify an AI-generated message, with just 46% correctly labeling it as AI.

However, these results were not uniform across all age groups. Younger generations demonstrated a greater ability to correctly identify human writing, suggesting that individuals who have grown up around this type of technology are more likely to intuitively know the difference.

Human email

Hi [NAME],

To keep our network secure, we ask that all users reset their login credentials for our project management system every 90 days. Your login is due to expire soon, so please use the link below to reset your credentials — let us know if you have any issues.

https://link/example.com

Thank you,
[NAME]
Company administrator

AI email

Hi [NAME],

Just a quick heads-up: your login for the company's project management system has expired (we reset them every 90 days). To keep things secure, we ask that you set up a new login. You can do that by clicking the link below: https://link/example.com

Reach out if you have any trouble.

Best,
[NAME]
Company administrator

II.

Solutions:
The Path to Building Cyber Resilience

Knowledge is the First Line of Defense

Effective cybersecurity demands a multi-pronged approach. Technology alone is ineffective without the knowledge employees need to protect both themselves and their organization. Our findings suggest significant gaps in broad cybersecurity education that demand attention in order to resist modern threats.

A strong example of how misconceptions can derail security efforts can be seen in the lack of MFA adoption. Respondents who avoid MFA on their personal accounts say they do so due to lack of familiarity (40%), perceived complexity (24%), lack of time (22%), and assumed cost (9%).

Similarly, the recurrent lack of passkey adoption appears to stem from gaps in knowledge as opposed to technical hurdles. Of those surveyed who do not use passkeys, 45% said they had never heard of them. An additional 12% said they are not an option for the sites and services they use, and 11% were concerned they are too complicated. This suggests a need for education and organizational commitment to improve authentication security.

Effective Education Strategies

Bolstering enterprise cybersecurity resilience demands a hands-on approach that includes educational programs, technical training, and regular review of security habits. It's important to dispel misconceptions about the perceived complexity of cybersecurity and present the tools available in straightforward terms. Modern security solutions are built with general users in mind and offer a streamlined approach when compared to outdated passwords.

Educational programs must emphasize the importance of both professional and personal cybersecurity, giving employees a deep understanding of how personal habits can impact workplace security. Regular training sessions are essential in today's rapidly changing threat landscape, and organizations should provide a steady stream of education on emerging risks, including assessments to ensure knowledge retention.

> Employers must dispel the myth that cybersecurity is only for the tech-savvy. With the right knowledge and tools, every single person in the organization can, and should, contribute to a safe online ecosystem."
>
> **Yubico Spokesperson**

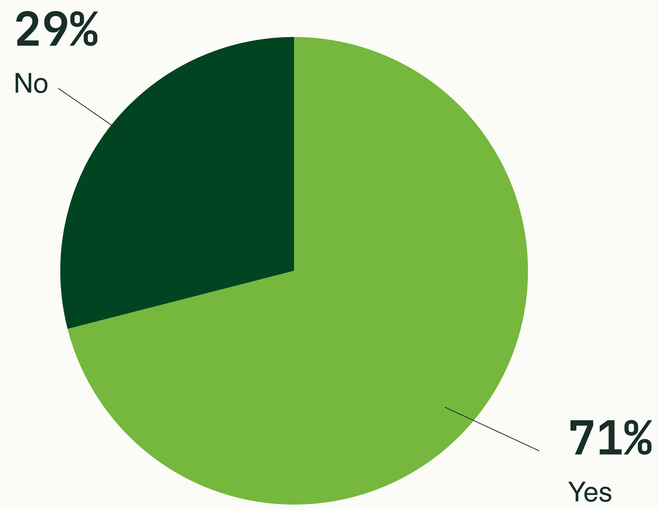
Closing the Gap on MFA Adoption

Our data shows positive momentum for MFA, suggesting people and organizations are open to learning more, ultimately leading to a higher adoption rate. With younger generations like Gen Z (71%) and Millennials (68%) demonstrating higher adoption rates for their personal accounts, it's likely that MFA adoption will continue to grow organically, but organizations should not wait for this inevitability and should instead push for widespread buy-in.

Global variations in adoption rates provide additional insight into effective implementation strategies. Overall, 82% of respondents say they are familiar with MFA passkeys, with the US second in adoption (33%) behind only India (39%) in device-bound passkey usage. Elsewhere, Australia and Singapore lead the world in MFA adoption (both 78%) on personal accounts specifically, highlighting what is achievable with adequate cybersecurity education and support.

It is essential for organizations to work toward eliminating barriers to MFA adoption as a first step. Companies should provide user-friendly tools, easy-to-understand guidance, and continuous support and troubleshooting. The goal should be to make MFA options convenient and streamlined, not just mandate their use.

Do you have multi-factor authentication (MFA) enabled for your personal email?



What Prevents Users From Adopting MFA?

Among those who don't use MFA, the top reasons include lack of familiarity (40%), feeling they don't have the technical know-how (24%), thinking it takes too much time (22%), and believing it's too expensive (9%).

The Case for Hardware Security Keys

In the modern threat environment, complete with AI-boosted phishing efforts and powerful social engineering techniques, hardware security keys with passkeys provide a robust defense. They offer phishing-resistant authentication that requires physical possession of the key as well as interaction from the user.

Demanding proof of both device possession and human presence, hardware security keys are strong protection against even the most sophisticated AI-powered phishing attacks. Whereas passwords can be hacked and used remotely and SMS messages can be intercepted, hardware security keys are not vulnerable to those attack vectors.

Device-bound passkeys like hardware security keys are today's gold standard. While cloud-based synced passkeys do provide an enhanced degree of security over passwords, they are still potentially vulnerable to compromise if an attacker breaches the cloud service or the user's individual account. Device-bound passkeys, which store cryptographic keys locally, do not share these same risks.

Despite being the most phishing-resistant effective tool available today, just 17% of companies use device-bound passkeys for any of their workforce, suggesting significant room for improvement among enterprises. Generational data, once again, provides a glimmer of hope for increasing adoption, with 20% of Millennials and 19% of Gen Z showing the highest usage rates in corporate settings.

Just as with adoption of any new technology, implementing hardware security keys requires planning and user support, but the benefits dramatically outweigh both the initial investment and any training that may be required. The successful deployment of hardware security keys typically results in significant ROI, a precipitous drop-off of account incidents, reduced technical support, and improves user confidence and peace of mind as a whole.

Generational Trends

Generational trends offer optimism for increased adoption, with Millennials (20%) and Gen Z (19%) leading the way in MFA use within corporate environments.

Conclusion

Today’s cybersecurity landscape is faster-moving and more fraught with threats than ever before. The expectation is that legacy approaches should be enough, but the reality is that AI-enhanced attacks and basic MFA practices can leave many organizations dangerously exposed. Reliance on weak authentication methods, inconsistent employee training, and fragmented security policies has created a gap between what companies believe protects them and what actually works.

Proven solutions already exist. Device-bound passkeys, like hardware security keys, are widely available, effective, and ready to be deployed at scale. The barriers to adoption are less about technology and more about organizational mindset, which means change is both possible and within reach.

Generational trends give us a reason to be optimistic about the future, with younger employees more quickly adopting advanced security options and demonstrating a higher degree of skepticism around AI-generated content. With these digital natives positioning themselves for leadership roles, we anticipate they will drive widespread organizational adoption of advanced security protocols.

The way forward for organizations is clear: Embrace integrated approaches with proven technologies that offer true protection against cyber attacks. By taking decisive action today, companies can close the gap between expectation and reality and create a future where security is a shared strength rather than a persistent vulnerability.

About Yubico:

Yubico (Nasdaq Stockholm: YUBICO) is a modern cybersecurity company on a mission to make the internet safer for everyone. As the inventor of the YubiKey, we set the gold standard for modern phishing-resistant, hardware-backed authentication, stopping account takeovers and making secure login simple.

Since 2007, we've helped shape global authentication standards, co-created FIDO2, WebAuthn, and FIDO U2F, and introduced the original passkey. Today, our passkey technology secures people and organizations in over 160 countries—transforming how digital identity is protected from onboarding to account recovery.

Trusted by the world's most security-conscious brands, governments, and institutions, YubiKeys work out of the box with hundreds of apps and services, delivering fast, passwordless access without friction or compromise.

We believe strong security should never be out of reach. Through our philanthropic initiative, Secure it Forward, we donate YubiKeys to nonprofits supporting at-risk communities.

Dual-headquartered in Stockholm, Sweden and Santa Clara, California, Yubico is proud to be recognized as one of TIME's 100 Most Influential Companies and Fast Company's Most Innovative Companies. Learn more at www.yubico.com.

Methodology

Talker Research surveyed 2,000 employed adults from the United States, United Kingdom, Australia, India, Japan, Singapore, France, Germany, and Sweden. The survey was commissioned by Yubico and administered online between August 15 and August 27, 2025.