yubico

EXCLUSIVE RESEARCH | 2024

State of Global Authentication Survey:

A holistic approach to combating cyber threats at work and home

Executive summary

Cybersecurity breaches and phishing schemes are not just a concern for IT departments or tech-savvy individuals. They also pose significant risks to the general public, particularly in the age of Artificial Intelligence (AI). As the sophistication of cyber attacks and online scams continue to evolve, it's more crucial than ever for individuals to remain vigilant both in their personal and work lives.

20,000+
responses

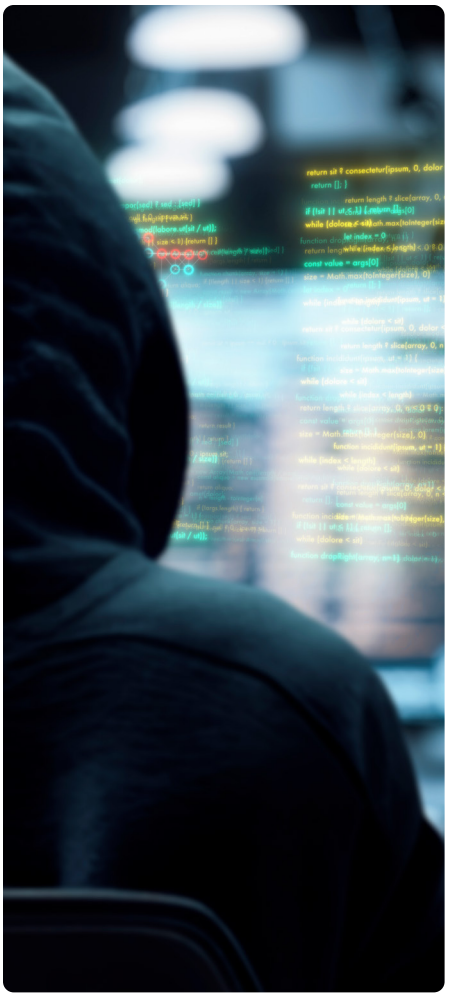
organizations with
1 - 2000+
employees

10
countries

Despite the rise in cyber threats, many people do not have a holistic view of security. While organizations often try their best to implement stringent security protocols at work, our findings show employees are falling behind in maintaining their own cybersecurity practices at home. This gap leaves not only individuals' personal data at risk but also exposes employers to potential vulnerabilities.

Yubico commissioned a global survey, with respondents from Australia, France, Germany, India, Japan, Poland, Singapore, Sweden, United Kingdom and the United States to investigate the global impact of cyber insecurity, both personally and in the corporate realm. Our research into the current state of personal and workplace cybersecurity reveals alarming trends such as the widespread underuse of multi-factor authentication (MFA) and the largely reactive nature of many people's responses to cyber threats. By conducting a comprehensive survey across multiple countries, we explored the risks posed by inadequate security practices and the impact this has on both personal and organizational safety.

Our findings highlight the need for a holistic cybersecurity strategy that encompasses both home and work environments. This includes adopting stronger authentication methods to become phishing-resistant, fostering a culture of security awareness through consistent employee training, and more. Ultimately, building a unified front against cyber threats requires a concerted effort to bridge the gap between perceived and actual security. By integrating advanced security measures into all aspects of our digital lives, we can better protect ourselves, our data, and our organizations.



Setting the scene—AI is evolving how hackers attack:

For years, hackers have leveraged emerging technologies to advance the effectiveness and speed of their phishing attacks. However, the advent of AI presents an unprecedented challenge to enforcing cybersecurity. With the ability to analyze vast amounts of data, learn from patterns, and generate sophisticated phishing schemes, AI has the potential to disrupt the cybersecurity landscape much more dramatically.

In May of 2024, the FBI issued a statement warning the public about the increased risks associated with AI-based cybersecurity threats, including voice and video cloning techniques to impersonate trusted individuals such as family members or co-workers.

What is phishing?

Phishing, a common tactic used by hackers to obtain access to sensitive information, contributes to over **80%** of all security breaches. It involves tricking individuals into revealing personal information by impersonating legitimate entities through email, social media, text messages, or fake websites.

At the root of many phishing attacks are passwords, as they, unfortunately, are the frontline for malicious actors to breach an account. While passwords have long been the go-to method for verifying identity online, they're inherently insecure. Users are typically required to create complex strings of characters that they must remember and input correctly each time they access a system or application. However, this method has proven to be flawed in many ways.

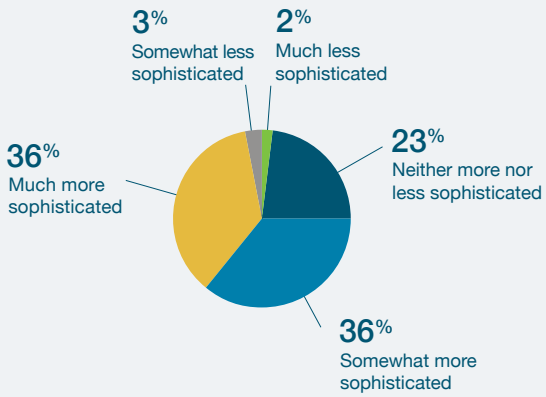
This is because people tend to reuse passwords across multiple accounts and/or use easily guessable passwords, which gives hackers the ability to breach multiple accounts with a single login. Additionally, people can be easily tricked into sharing their passwords due to the sophistication of today's phishing attacks—for example, hackers are able to manipulate a fake website to appear legitimate.

58% of respondents *****

are **concerned** about AI impacting the security of their personal and/or business accounts

AI and cybersecurity threats: survey findings

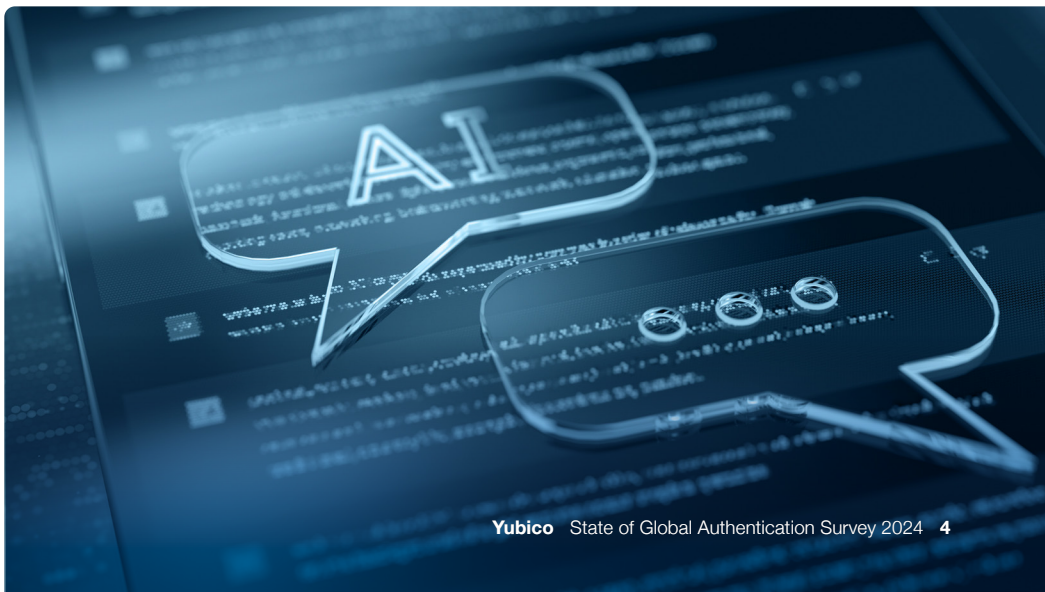
Do you believe that online scams and phishing attempts have become more or less sophisticated due to the use of artificial intelligence (AI)?



Not surprisingly, our survey revealed that respondent fears are running high when it comes to the cybersecurity dangers posed by AI:

- **72%** of respondents believe online scams and phishing attacks have become more sophisticated due to the use of AI.
- **66%** of respondents believe these attacks have become more successful because of AI.
- **58%** of respondents are concerned about AI impacting the security of their personal and/or business accounts.

The evolving threat of AI underscores the urgent need for a more integrated approach to cybersecurity; one that also considers the increasing role of new technology in online fraud. That is why it is no longer sufficient to rely on outdated security practices—the tools and techniques we use to protect our data must evolve in tandem with the threats we face.



Nearly half (49%) of respondents

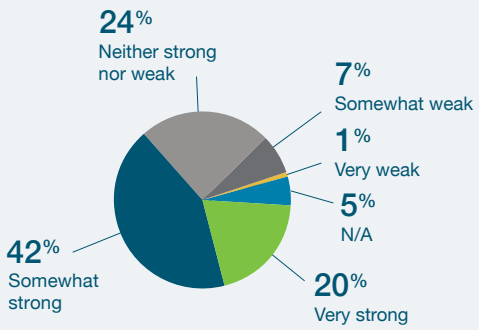
are more concerned about the security of their **personal information** than the security of their company's information.

Phishing-resistant multi-factor authentication

MFA is a critical tool in the fight against phishing attacks. However, **not all MFA methods are created equal**. Phishing-resistant MFA, such as hardware security keys, offer a **higher level of protection** by requiring a physical device to authenticate, making it much harder for attackers to gain access to your accounts.

Personal cybersecurity: confidence vs. reality

In your opinion, how strong or weak are the cybersecurity measures you have in place to protect your personal information?

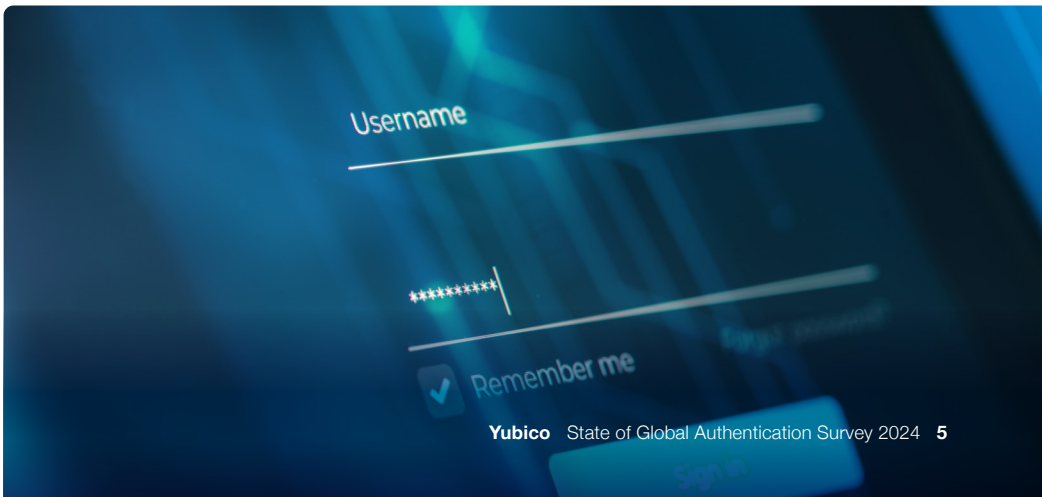


A significant number of survey respondents reported feeling secure in their personal cybersecurity practices, even prioritizing it over security at work.

- **63%** of respondents say they have strong or very strong cybersecurity measures in place to protect their personal information.
- Nearly half (**49%**) of respondents are more concerned about the security of their personal information than the security of their company's information.

However, while many individuals feel confident about their personal cybersecurity measures, this confidence may be misplaced. When we delve deeper into their actual practices and experiences, it is clear that many individuals are not as secure as they believe:

- **70%** of respondents have been exposed to cyberattacks in their personal lives in the past 12 months.
- Many respondents are reactive rather than proactive when responding to cyber threats in their personal and professional lives (**45%** and **44%** respectively).
- **39%** believe that simply using a username and password is the most secure way to protect accounts and information, and furthermore, **58%** of respondents use only a username and password to log in to their personal accounts.



70% of respondents

have been exposed to a cyber attack in their **personal life** in the last 12 months

60% of respondents

have been exposed to a cyber attack **at work** during the last 12 months

The ripple effect: how personal cybersecurity impacts workplaces

What types of workplace cyber attacks have you been exposed to in the last 12 months?*

Top 6 most common responses

* Multiple answers allowed

The gaps in personal cybersecurity practices do not just pose risks to individuals; they also expose workplaces to vulnerabilities. As more employees work remotely or use personal devices for work-related tasks, the line between personal and professional cybersecurity has become blurred. This integration can inadvertently open doors for cybercriminals to access corporate networks through compromised personal accounts.

Our survey found **50%** of respondents were exposed to cyberattacks at work in the past 12 months. This statistic highlights the interconnected nature of cybersecurity in today's world.

> "When individuals fail to secure their personal accounts, they also put their workplaces at risk. This is why it's crucial for enterprises to adopt a holistic approach to cybersecurity that considers the security of both work and personal environments."
>
> **Derek Hanson** | VP Standards and Alliances | Yubico

Solutions for a unified cybersecurity front

Given the interconnected nature of modern cybersecurity threats, it's clear that both individuals and organizations need to take a more integrated approach to security. This means not only implementing strong measures at work but also encouraging and enabling employees to adopt better practices in their personal lives. The top safety measures we recommend include:

SOLUTION 1: Bridge the gap between work and home

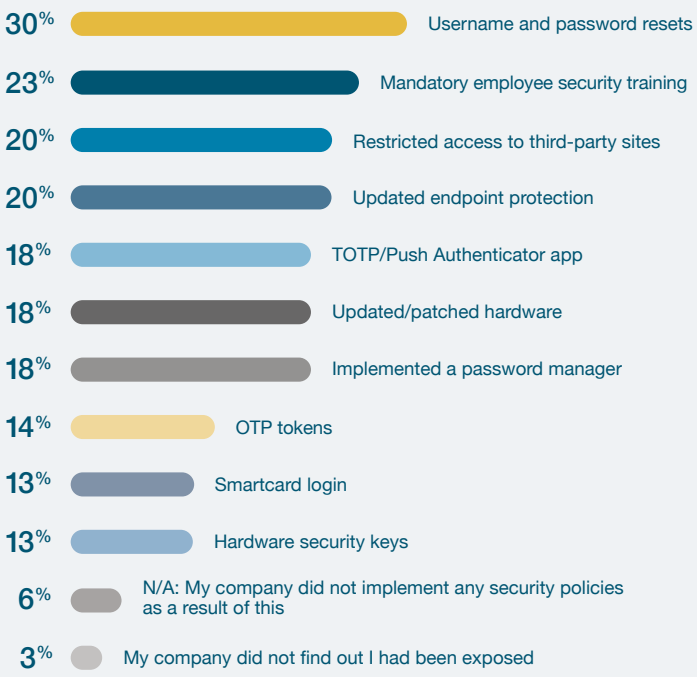
To create a truly secure environment, both employers and employees must understand that cybersecurity is not relegated to the workplace. A comprehensive approach to cybersecurity must involve taking consistent and proactive measures to protect all aspects of your digital life.

That is why enterprises should provide resources that extend beyond the workplace, helping employees secure their personal devices and accounts. As an example, encouraging the use of phishing-resistant MFA and other advanced security measures for both work and personal accounts can significantly reduce vulnerabilities.

SOLUTION 2: Provide employee training and educational awareness

You said you have been exposed to a cyber attack in the last 12 months at work. What new security technologies or policies, if any, did your company implement, as a result?*

Top 12 most common responses



* Multiple answers allowed

40% of respondents

reported not receiving any cybersecurity training **at work**

47% of respondents

said their personal digital security habits have changed based on what they've learned or have done **at work** to protect their accounts

One effective way for enterprises to improve cybersecurity practices is through education and comprehensive training. However, our survey revealed that not all employees receive adequate training, and those who do may not always carry these practices into their personal lives. Here are the statistics:

- **40%** of respondents reported not receiving any cybersecurity training at work.
- **47%** of respondents said their personal digital security habits have changed based on what they've learned or have done at work to protect their accounts.

This data indicates that while training can be effective, it is not reaching everyone and there is room for improvement in how it is delivered and reinforced. Moreover, cybersecurity training must be consistent across all levels of the organization, from entry-level employees to senior executives. More junior employees, in particular, should not be overlooked.

Enterprises should also regularly update employees on the latest cybersecurity threats, especially those related to AI-driven attacks. The importance of MFA should be clearly communicated to ensure employees understand how to implement it for both work and personal accounts.

What's more, nearly a quarter (**23%**) of employees who had been exposed to a cyberattack at work said that their employer responded by implementing mandatory security training. While this is a reasonable response to mitigating a cyber threat, employees should be regularly reminded of "best practices" at multiple points during the year as a preventative measure.

SOLUTION 3: Authentication methods—securing access at work and home

58% of respondents

use their **username and password**

34% of respondents

rely on **SMS** based authentification

22% of respondents

use a **mobile** authentification app

54% of work accounts

use their **username and password**

21% of work accounts

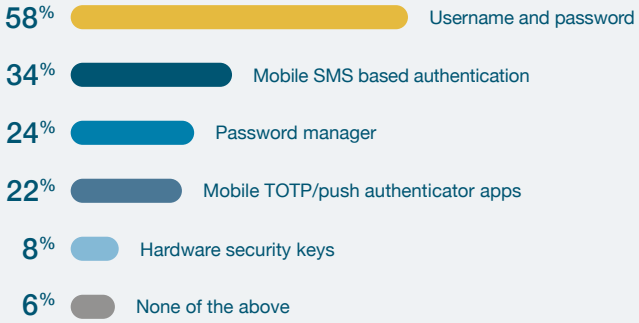
rely on **SMS** based authentification

21% of work accounts

use a **mobile** authentification app

How do you authenticate/login to your personal accounts?*

Top 6 most common responses



* Multiple answers allowed

Multi-factor authentication is one of the most critical aspects of cybersecurity, but our survey found many people are still relying on outdated methods to secure their accounts, both at work and at home.

- For personal accounts, **58%** of respondents use their username and password, **34%** rely on SMS based authentication, **22%** use a mobile authentication app
- For work accounts, **54%** use username and password, **21%** rely on mobile SMS-based authentication, **21%** use a mobile authentication app.

These findings suggest that while a majority of respondents are relying on their mobile phone for SMS text messages and authentication apps to authenticate the fact of the matter is that some employees do not want to use mobile authentication. The reasons for this are numerous. They may not want to use personal devices for work or allow admin access to their devices, or there may be union restrictions or compliance requirements. Some employees may not be able to even use a smartphone. If the fallback option is usernames and passwords, this makes the organization even more vulnerable to phishing and account takeovers.

To combat these threats, passwordless multi-factor authentication (MFA) offers a secure and user-friendly solution. By eliminating the need for passwords, this method uses alternative factors like biometrics or hardware security keys to verify identity. This approach significantly reduces the risk of unauthorized access since there are no passwords for hackers to steal or guess.

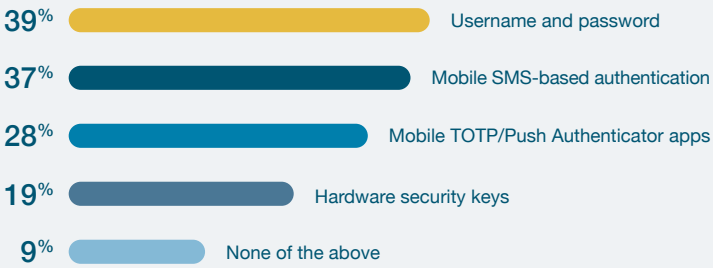
The future of authentication lies in passkeys, and even more specifically, hardware security keys that contain device-bound passkeys. Hardware security keys are a tangible passkey solution, providing the highest level of security from phishing attacks by making them less vulnerable to theft or compromise compared to passwords. Additionally, password-less authentication simplifies the user experience by removing the need to remember complex passwords, leading to higher user satisfaction and productivity, especially in enterprise settings.

> In addition to being highly secure, passkeys greatly simplify the user experience. By removing the need for users to remember complex passwords, it reduces the friction associated with logging in and eliminates the frustration of forgotten passwords.
>
> This can lead to increased user satisfaction and productivity, especially in enterprise environments where employees often juggle multiple accounts and passwords.
>
> When we look at today's options for passkeys, those that are device-bound on security keys provide the highest level of phishing-resistance and meet the strictest security standards."
>
> **Derek Hanson** | VP Standards and Alliances | Yubico

The case for passkeys

What do you believe are the most secure methods of authentication?*

Top 5 most common responses

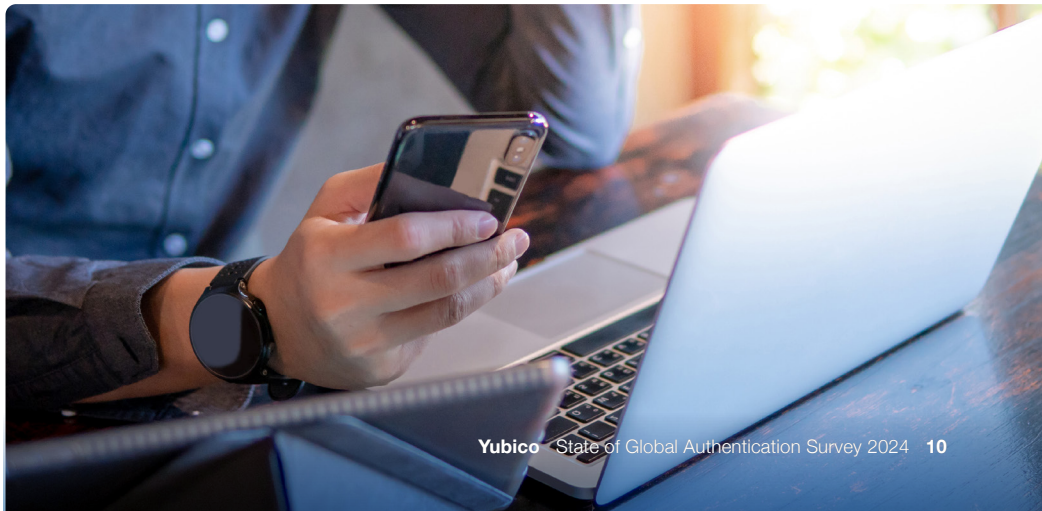


* Multiple answers allowed

The increasing popularity and adoption of passkeys have exploded due to their widespread support by the world's largest tech companies—who also happen to be the most used identity providers collectively—as millions of users begin to make the shift. Yet, there is still a lot of education to be done amongst consumers and enterprises alike, as **39%** of respondents believe username and password are the most secure option. For this reason, employers should help their employees learn more about passkeys—particularly about device-bound passkeys—and educate them on why passkeys are an important part of any healthy cybersecurity regiment.

Passkeys are an emerging authentication method that creates cryptographic security "keys" stored in the cloud or locally on a user's device. They offer a superior alternative to passwords since users are not required to recall or manually enter long sequences of characters which can be forgotten, stolen or intercepted.

Passkeys on a hardware security key provide an even higher level of security as they are device-bound (meaning they are stored within a physical hardware device) and cannot be copied nor tied to a specific vendor. Other forms of passkeys are syncable, meaning they are stored in the cloud, which are tied to a specific platform and can be copied across devices. It's important to note the distinction as individuals and organizations continue adopting passkeys so that they can determine based on their threat model, what the most secure option will be for their use-case.



Conclusion

The findings from this survey highlight the importance of taking a more integrated and proactive approach to cybersecurity. As AI continues to evolve and cyber threats become more sophisticated, both individuals and organizations must work together to build a unified front against these risks.

Our research also uncovered the increasing sophistication of cyber threats, especially those driven by AI, which requires a more advanced and holistic approach to cyber-security. It is apparent that there is a significant gap between perceived and actual security, both in personal and professional contexts. Many individuals believe they are more secure than they actually are, which creates vulnerabilities that cybercriminals can exploit.

A unified cybersecurity strategy that bridges the gap between personal and professional security is essential. This involves educating employees on best practices, encouraging the use of more secure authentication methods like hardware security keys and passkeys, and making sure that training and security protocols are consistently applied across all levels and employees of an organization in order to create phishing-resistant users.

As we continue to navigate the ever-changing and increasingly dangerous landscape of cybersecurity, embracing emerging like hardware security keys and passkeys will undoubtedly play a pivotal role in safeguarding our digital identities and securing the systems and services we rely on every day.

yubico

About Yubico

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO), the inventor of the YubiKey, offers the gold standard for phishing-resistant multi-factor authentication (MFA), stopping account takeovers in their tracks and making secure login easy and available for everyone. Since the company was founded in 2007, it has been a leader in setting global standards for secure access to computers, mobile devices, servers, browsers, and internet accounts. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries.

Yubico's solutions enable passwordless logins using the most secure form of passkey technology. YubiKeys work out-of-the-box across hundreds of consumer and enterprise applications and services, delivering strong security with a fast and easy experience.

As part of its mission to make the internet more secure for everyone, Yubico donates YubiKeys to organizations helping at-risk individuals through the philanthropic initiative, Secure it Forward. The company is headquartered in Stockholm and Santa Clara, CA. For more information on Yubico, visit us at www.yubico.com.

Methodology

This survey was conducted by Talker Research between July 22 and Aug 12, 2024, involving 2,000 employed adults from each of the following countries: the United States, United Kingdom, Australia, India, Japan, Poland, Singapore, France, Germany, and Sweden. The survey aimed to gather insights into personal and professional cybersecurity practices and perceptions, particularly in the context of emerging threats.