yubico

EXCLUSIVE RESEARCH

State of Global Enterprise Authentication Survey

How modern enterprises are embracing phishing-resistant MFA

Executive Summary

Authentication plays a critical role in today's cybersecurity landscape, determining whether attacks gain entry and wreak havoc or get stopped in their tracks. It's increasingly complicated to get authentication right as companies embrace hybrid work models and leverage cloud services, and there can be serious consequences for getting it wrong given the frequency, growth and damage of cyber attacks. Using out-of-date or ineffective authentication risks both security and productivity, so Yubico decided to further investigate how companies are handling their authentication by asking them directly.

16,000+
responses

organizations with
1 - 2000+
employees

8
countries

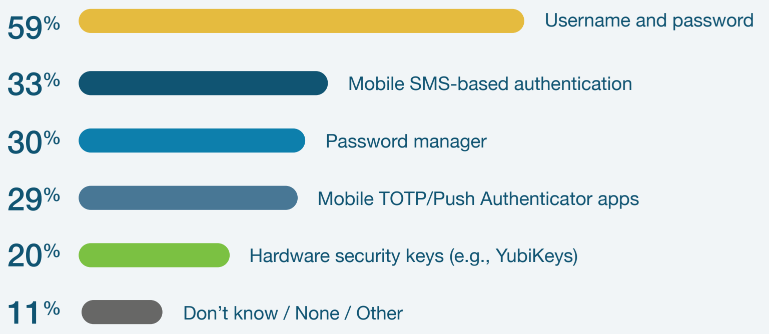
Our inaugural State of Global Enterprise Authentication Survey, conducted between 30th August and 14th September 2022, was designed to get a snapshot of authentication at companies around the world. We received over 16,000 responses from entry-level employees up to business owners at organizations ranging in size from one to 2,000+ employees, in eight countries: the UK, the USA, Australia, New Zealand, Singapore, France, Germany, and Sweden.

The results are collected and contextualized in the following report. They offer an in-depth and objective look at the practices and attitudes driving authentication at real companies. The numbers show that organizations are aware of, exposed to, and harmed by cyber attacks. Yet few have taken significant steps to replace legacy authentication practices—like single-factor or mobile authentication—with best practices like phishing-resistant multi-factor authentication (MFA).

Modern MFA, when done correctly, offers a relatively easy, affordable, and effective way for any organization to upgrade their security—but most companies **are not** using it to their advantage. This report, drawing on extensive survey data, reveals where authentication practices still need to improve and helps organizations understand how and why.

Enterprise authentication practices remain unchanged

What are the primary ways you authenticate your business accounts?*



* Multiple answers allowed

Despite sweeping advances in how enterprises use IT, how they handle authentication hasn’t changed as quickly. Single-factor authentication based on providing a username and password remains the primary means of authentication (by a wide margin) even though there’s ample evidence that bad actors can buy, steal, or break their way through those credentials with ease. The data is damning: **the least secure form of authentication is also the most common.**

Mobile SMS-based authentication, password managers, and authenticator apps, all of which enable MFA, are each used by around 30% of respondents. Requiring a second authentication step makes it harder to gain unauthorized access—but these methods have flaws. Texts can be hijacked in transit, apps can be exploited, and any form of MFA reliant on phones is vulnerable to lost, broken, or stolen devices. Each is better than single-factor authentication but far from perfect.

Security keys offer the kind of phishing-resistant MFA required by governments around the world, including federal agencies in the US. **Security keys are widely seen as the gold standard for MFA,** but they were mentioned by fewer than 20% of respondents. Furthermore, more than 10% either weren’t aware of how their company authenticated or used no authentication at all. This question reveals that most companies are vulnerable (highly so) as a result of weak, single-factor authentication. And even among those with MFA already in place, the risk of phishing attacks and authentication struggles remains high. Enterprise MFA adoption still has a long way to go.

59% of employees

still rely on **username and password** as a primary method to authenticate into their accounts

Phishing

Tricking users into providing login credentials or other sensitive data

Single-factor authentication

Authentication based on one-factor, typically a personal password

Multi-factor authentication

Authentication requiring one or more additional factors such as a push notification, one-time code or cryptographic key

Phishing-resistant MFA

Multi-factor authentication that’s immune to attackers intercepting, or even tricking users into revealing, access information

22% of employees *****

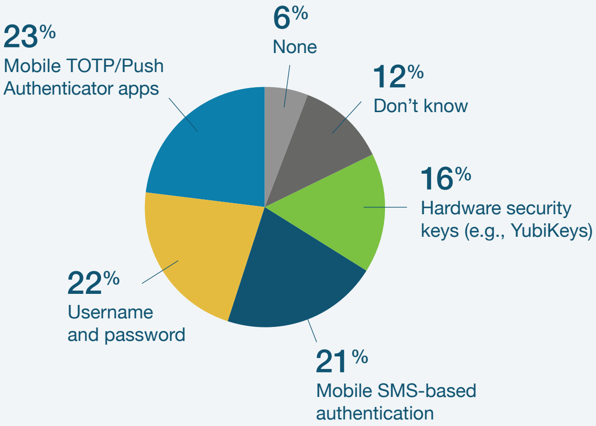
believe username and password is the **most secure**

Why are security keys ideal for authentication?

Requiring a specific, physical key to log into online accounts completely negates the risk of remote attacks. Security keys contain a unique cryptographic code which cannot be extracted and FIDO2 protocols mean that keys will only respond to trusted sources, making them impersonation-resistant. Security keys come in a variety of form factors (USB-A, USB-C, Lightning, NFC) to easily interface with more devices and, as the form of MFA most trusted by professionals and security experts, are ideal for strong authentication.

The Perception is not the reality

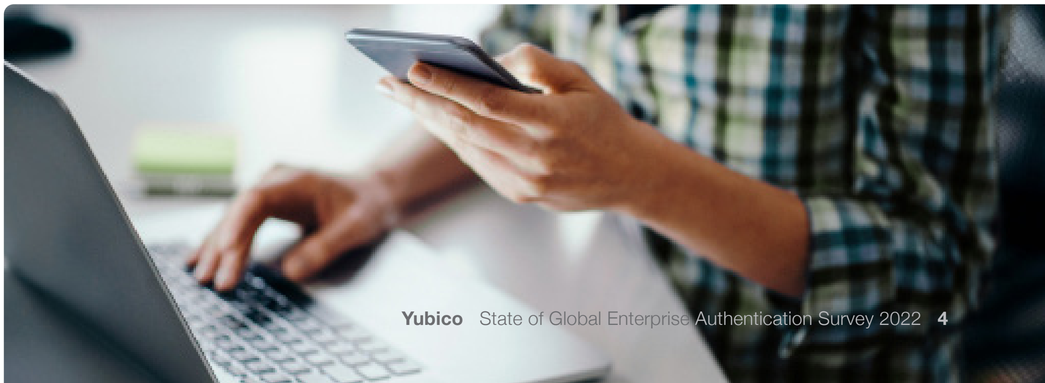
What do you think is the most secure method for authentication?



It's a positive sign that close to a quarter of respondents listed authenticator apps (like Google Authenticator or Okta) as the most secure method of authentication. They provide a significant security upgrade over single-factor authentication and some forms of multi-factor as well. These apps can be problematic because they depend on having access to one's phone, and they're vulnerable to sophisticated phishing attacks. Still, the fact that they took the top spot suggests people are becoming more aware of what makes authentication secure vs. insecure.

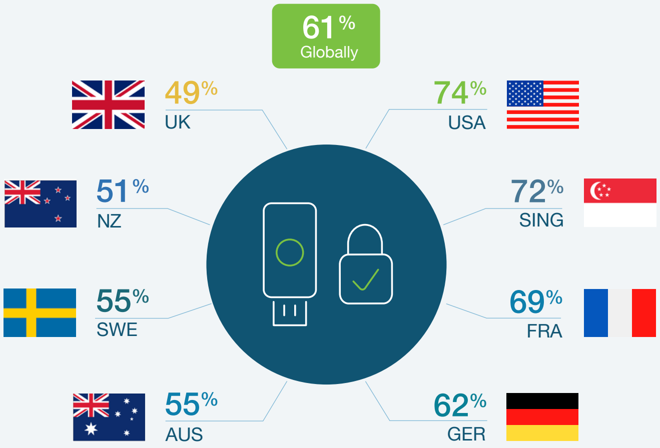
Undercutting that assertion, however, is the response that came in a close second: username and password. **More than a fifth of respondents believed that basic login credentials were not just secure but the most secure,** even though there's been years of widespread warnings and corporate training focused on password insecurity in particular. In the third spot was mobile SMS-based authentication, which is better than nothing, but it's widely seen as the most insecure form of MFA because of the high phishing risk. Compared to authenticator apps, almost twice as many people identified authentication factors with conspicuous security flaws as the most secure options available, suggesting a massive perception gap around authentication.

Reinforcing that conclusion is the fact that only 1 in 6 employees singled out security keys as the most secure option. The percentage rose to 42% at the VP level, which could indicate that more junior employees need better education on MFA (along with more secure options).



People have contradictory feelings about authentication

My organization needs to upgrade to modern phishing-resistant MFA (like hardware security keys)



More than 60% of respondents agreed that their organization needs to upgrade to phishing-resistant MFA (79% at the VP level), and close to a quarter indicated they “strongly” agree. Perhaps more telling, barely 10% of respondents disagreed, and strong disagreement tracked below 5%. The survey shows strong support for adding phishing-resistant MFA and little to no meaningful opposition. It seems strong MFA is a policy people are already on board with, especially in the leadership ranks.

Complicating that finding, however, are the results from another survey question: For the authentication options that your organization offers, do you feel like they offer enough security? Almost 80% of respondents agreed with that statement, and only 15% disagreed. Skepticism about security was highest among French respondents and lowest with US respondents—but respondents everywhere felt security was at least enough.

Based on some of the perception gaps exposed in the previous question, it’s fair to wonder how accurately people can assess security. Setting that aside, the data suggests that **while people think security is adequate, they also recognize there’s room for improvement and that phishing-resistant MFA is a missing piece wherever it’s absent.**

61% of employees and 79% of VP level staff

think their organization needs to upgrade to **modern phishing-resistant MFA** (like hardware security keys)

Power users choose phishing-resistant MFA

The survey data contained an interesting revelation: **among respondents who log into 9+ accounts or applications on a daily basis, the vast majority (76%) want their organization to adopt phishing-resistant MFA**. That number fell below 40% for people who average no daily logins. It makes sense that these power users put a high-priority on security and stronger authentication. It also makes sense they prefer phishing-resistant MFA in particular, which offers much faster login than authenticator apps requiring new one-time passcodes for every account sign on.

Cyber attacks are a fact of life

78% of respondents

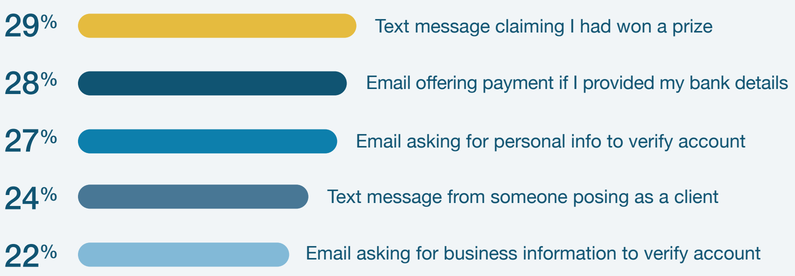
have been exposed to a cyber attack in their personal life in the last 12 months

60% of respondents

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

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

Top 5 most common responses



* Multiple answers allowed

The numbers also highlight the prevalence of phishing tactics. In both settings, attacks appeared in the form of text message, emails, or push notifications asking for private information, and in some cases those prompts came from seemingly "trusted" organizations. Respondents confirm that phishing attacks remain a popular and potent form of attack that targets people where and when they least expect.

Authentication can be a point of strength or weakness against these attacks. With phishing-resistant MFA, it does not matter if an initial phishing attack succeeds and hackers access a user's login credentials. So long as the attackers cannot compromise the second MFA layer as well, they are locked out of the account and the attack fails. Knowing that most people encounter frequent phishing attacks—and that most companies still use single-factor authentication—stronger MFA becomes mandatory.

Spear phishing

Phishing attacks targeted at very specific people, such as system admins

Whaling

Phishing attacks targeted at high-level employees such as executives

Vishing

Phishing attacks over phone and voice message where the identity of the other person is hard to confirm

Smishing

Phishing attacks that take place over text or chat where trust is implied and information flows freely

Attacks risk severe consequences

The survey shows that any exposure to cyber attacks comes with troubling risks and the high likelihood of damage, potentially devastating. **Fewer than 30% of respondents saw no consequences as a result of attacks** (though this data also includes junior employees who may not have been privy to an attack's consequences). 35% of respondents experienced reputational damage and, similarly, 35% suffered damage to profits. Equally alarming, 17% lost employees because of cyber attacks, and 20% had their operations suspended. Everything is at stake in a cyber attack.

The consequences eclipse the corrections

You said you have been exposed to a cyber-attack in the last 12 months at work.*

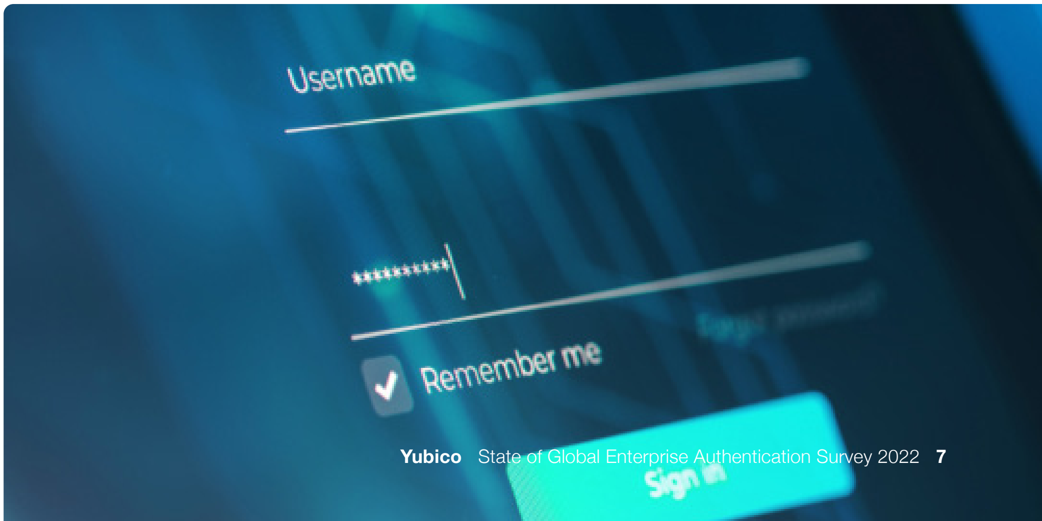
What new security technologies or policies, if any, did your organization implement as a result?

29%	Username and password resets
28%	Updated endpoint protection
24%	Mandatory employee security training
22%	TOTP/Push Authenticator app
21%	Restricted access to third-party sites
20%	Updated/patched hardware
20%	Password manager
17%	Hardware security keys (e.g., YubiKeys)
17%	Smartcard login
15%	OTP tokens

* Multiple answers allowed

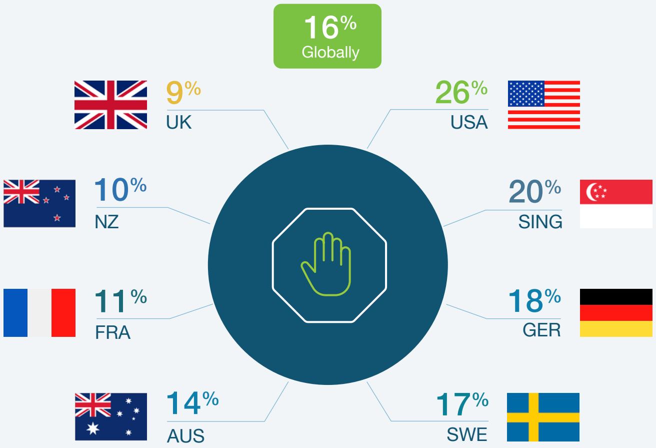
Given the consequences, one would expect companies to put robust upgrades in place, but that doesn't always seem to be the case. The most common response, resetting usernames and passwords, does not prevent hackers from stealing credentials again and repeating the same attack which perpetuates the problem. Security training, another common response, makes people more aware but does nothing to actually stop credential exploitation from happening or succeeding. Authenticator apps, in the fourth spot, were the first mention of MFA, and security keys came in last.

The fact that phishing-resistant MFA was used so rarely in response to attacks despite being the most secure form of authentication is troubling. Even more concerning is that some companies aren't taking further action to upgrade cybersecurity and improve authentication following attacks. **The survey data reveals a remarkable disparity between the risk of cyber attacks and the response.** Improved authentication directly addresses that disparity and quickly closes the security gaps that enabled the original attack.



Complacency holds back progress

My organization hasn't adopted MFA across all apps and services because it isn't concerned that an attack will happen to them.



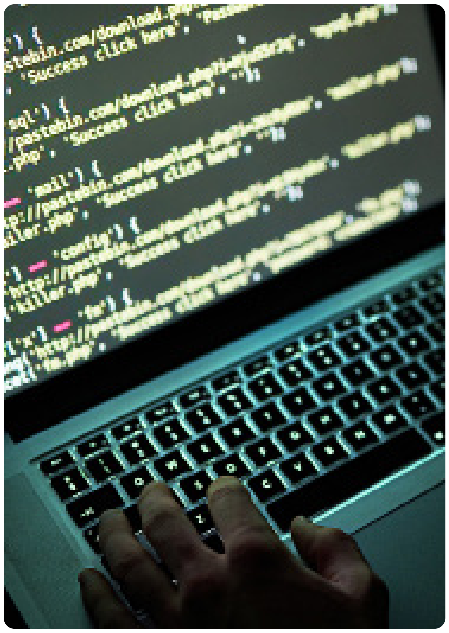
Despite its reputation as a global leader for cybersecurity, more than one quarter of American companies limit their use of MFA because they don't believe they are at risk of cyber attack. This means these companies—and their customers' data—are vulnerable to phishing attacks.

True protection against cybercrime requires using MFA across all apps and services, yet this was true for only 12% of respondents' organizations. Rates were the lowest in Germany (6%) and at companies with 1-9 employees. They were the highest in the UK (16%) and at 500+ employee companies. Universal MFA is seen as an authentication best practice and a vital part of cybersecurity. Nonetheless, for most companies, the perceived barriers appear to outweigh the benefits.

The survey data has already revealed that companies often misunderstand their protection relative to the attacks they face. Something similar is at work here, where MFA is seen as harder and less necessary than it really is. This attitude sheds light on why phishing-resistant MFA is still not the norm and why attackers continue to exploit authentication so often. It also points to an untapped cybersecurity solution there's no reason to avoid.

Slow adoption brings risks

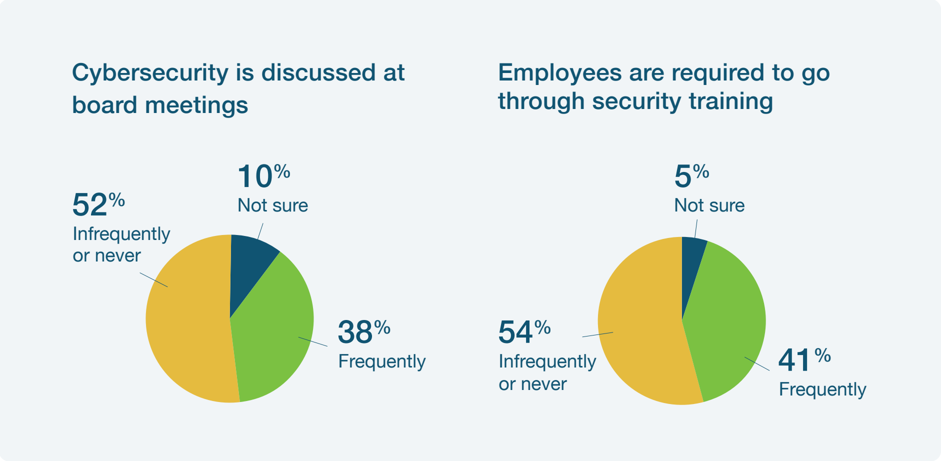
MFA has few barriers to entry, yet **only 12% of companies surveyed have implemented MFA for all the apps and services they use.** We asked respondents what holds them back from implementing strong authentication, even when they admit to being concerned about attacks. Being slow to adopt technology ranked first (19%), but close behind was the perception that MFA was expensive (19%), unnecessary (16%), time-consuming (16%), complicated to deploy (15%) or difficult to use (14%).



Cyber attacks cause insomnia

Asked to list the top five cybersecurity concerns that kept them up at night, respondents said: getting hacked on a private account, mobile device compromise, data breach, customer data compromise, and getting hacked on organization accounts. **Fewer than 30% said no cybersecurity concerns kept them up at night.** Professionals at all levels (especially senior leadership) are worried about cybersecurity and see the consequences for both themselves and their company. The institutional response, however, hasn't kept up with individual anxieties.

Security isn't top of mind


Cybersecurity is discussed at board meetings

Employees are required to go through security training

Cyber attacks and how to prevent them should be on the minds of every organization, wherever they are in the world. The survey data, though, shows that for the majority of companies the topic is infrequently or never discussed, and reveals vast disparities between approaches globally. The US leads the pack: cybersecurity is frequently discussed at board level meetings at 60% of companies, compared to the global average of 38%, with New Zealand the global laggard at 24%. Similarly, 62% of employees at US companies are required to go through cybersecurity training, compared to a global average of 42%, with New Zealand again trailing at 32%.

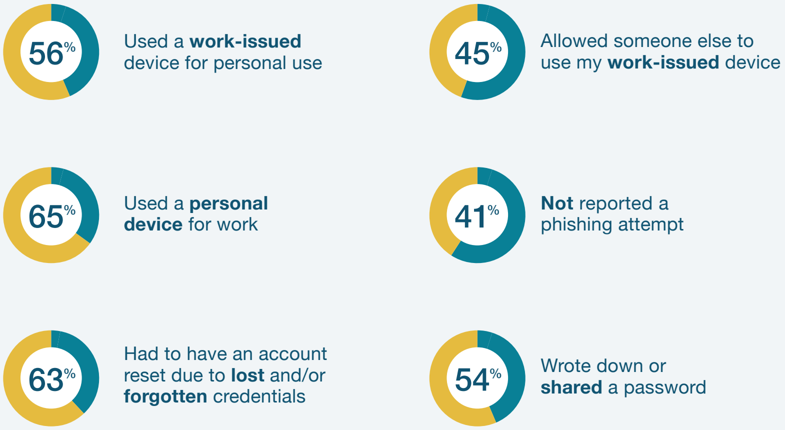
Informed and vigilant employees are essential to any successful cybersecurity strategy, yet in most organizations they aren't being given the training or equipment they need to be effective cyber defenders. Phishing-resistant MFA ensures authentication remains secure until (and after) education efforts catch up.

US employees risk data breaches

The US may lead the world when it comes to educating employees about cybersecurity, but there's still a long way to go. American employees hold an unenviable record: they take the least care of their passwords. An incredible 62% of Americans have either written down or shared a password over the past 12 months. This compares unfavorably to the global average of 54%. At 44%, New Zealand is the nation whose employees take most care over their passwords, despite being offered least cybersecurity training.

Cyber hygiene has big room for improvement

Have you done the following at least once during the last 12 months?



The survey asked a series of questions to explore how often employees engage in risky behaviors that undermine cybersecurity and put authentication at risk. It's inevitable that people, especially professionals eager to be productive and efficient, will push the limits of cybersecurity. The question is how often and in what ways?

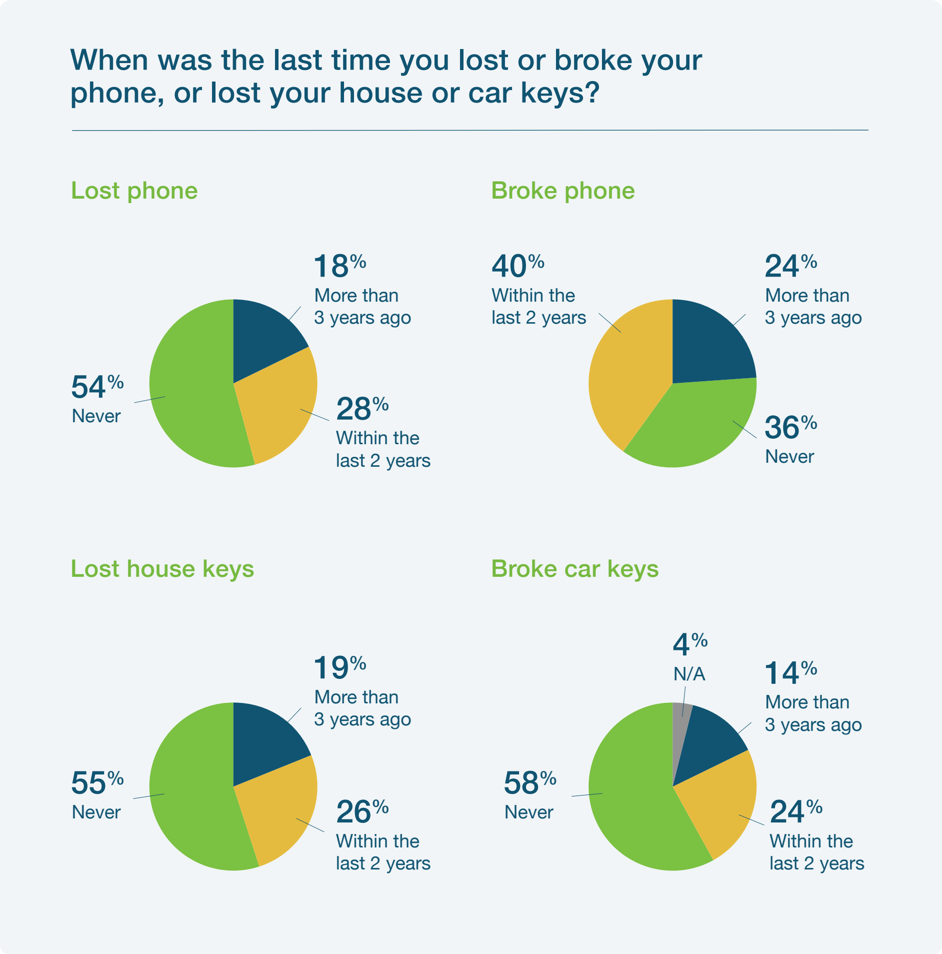
Reassuring is the fact that large percentages of respondents either never or rarely engaged in unsafe practices. That said, it only takes one mistake to unleash an attack. Furthermore, being willing to bend or break the rules, even if just occasionally, suggests that people don't know enough about or care enough about cybersecurity. **Indeed, one of the most astounding revelations from the survey is that 54% of employees admit to writing down or sharing a password in the last 12 months, revealing widespread but probably overlooked issues with account security.**

Taken in aggregate, the answers to this question highlight the complex and unpredictable ways that holes develop in cybersecurity. Occasional liberties may not be an issue on an individual level. But expanded across all employees it means huge numbers of security flaws could be occurring and overlapping all at once. Requiring phishing-resistant MFA across all accounts prevents these vulnerabilities from allowing attacks to explode into serious incidents.

When authentication becomes an emergency

The survey shows most people log into between one and five accounts or applications daily, and a quarter log into six or more. Being unable to authenticate because of a lost or stolen device is more than inconvenient—it's an insurmountable obstacle to accomplishing anything. Single-factor authentication poses the largest liability—but the *wrong* form of MFA comes with liabilities as well.

We care most about our keys



When was the last time you lost or broke your phone, or lost your house or car keys?

When someone leaves the house or office they typically carry two essentials with them: their phone and their keys. The data shows almost a quarter of people broke their phone within just the last year, and barely 36% had never broken their phone. Slightly more than 50% of respondents had never lost their phone, but it's hardly rare. The largest percentage of people had never lost their car or house keys, either recently or ever.

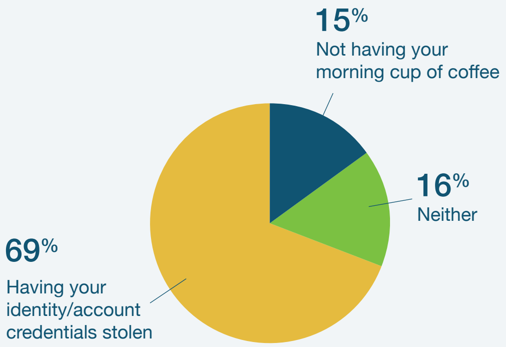
Since multi-factor authentication often depends on someone having their phone or a security key to pass the second factor, the loss rates matter. A broken phone could make access inconvenient (even impossible), and a lost phone could fall into the wrong hands. **Notably, directors reported losing their phones at the highest rates, putting all the access that depends on that phone at risk.**

As companies begin to explore adding MFA across all apps and services, they must compare the strengths and weaknesses of various "second" steps. Phones, which we interact with constantly, are always vulnerable to the unexpected. Keys, on the other hand, live mostly inside pockets and bags, which explains why they get lost less frequently. MFA based on security keys rather than phones fits better into how people actually live.

> The majority of respondents agreed that having credentials stolen was more concerning than missing out on their morning cup of coffee.

People care about their credentials

Are you more concerned about having your identity/account credentials stolen or not having your morning cup of coffee?



Thankfully, far more people care about their identity/account credentials than their morning cup of coffee, which encapsulates an important truth: people care about protecting their accounts. They see the threats and understand the risks, which is why they overwhelmingly rank account security above even coffee. **As the survey data shows time and again, people want strong, multi-factor authentication—but only if it's simple, seamless, and secure.**

As cyber risk gets worse in every way—increasing attacks, deepening damage, expanding compliance requirements—companies need to get serious about strong MFA. It's the first, most important, and most impactful area to focus on. And, as the survey data reveals, it's an area that isn't up to par at most organizations. Target phishing-resistant MFA to make the greatest strides in cybersecurity. And choose YubiKeys for a shortcut to a strong, compliant security posture.

YubiKeys

YubiKeys, which are hardware security keys, offer phishing-resistant MFA that elevates authentication in every way. Security keys make authentication immune to phishing attempts and accounts inaccessible to everyone except the one person with the correct key. Losing the key is less of a risk, and replacing the key is easier than replacing a phone. More than just a security key, Yubico offers an enterprise MFA solution that's appropriate for small to large companies across industries, and especially in those industries facing extensive security regulations.

yubico

About Yubico

As the inventor of the YubiKey, Yubico makes secure login easy and available for everyone. The company has been a leader in setting global standards for secure access to computers, mobile devices, and more. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards.

YubiKeys are the gold standard for phishing-resistant multi-factor authentication (MFA), enabling a single device to work across hundreds of consumer and enterprise applications and services.

Yubico is privately held, with a presence around the globe. For more information, please visit: www.yubico.com.

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
5201 Great America Pkwy, #122
Santa Clara, CA 95054, USA
844-205-6787 (toll free)
650-285-0088