yubico

YUBICO RESEARCH REPORT

Cybersecurity in the work from anywhere era

Findings on employee attitudes and adaptability to at-home corporate security

Contents

Introduction

When COVID-19 struck, businesses scrambled to connect remote employees in a bid to propel productivity. Many did so successfully and rapidly—but at what cost to cybersecurity?

Much of the world's workforce is still getting to grips with performing their roles remotely at least part time, a trend that is set to continue even after we emerge from the pandemic.

Virtual working patterns bring new opportunities for businesses and employees but also introduce additional risk. This includes new avenues for bad actors to breach corporate defences. With millions of workers focused on the pressures of completing tasks in varying, and sometimes unusual circumstances, cybersecurity best practices are often put on the backburner.

Organisations that don't get a handle on these hazards risk lasting financial and reputational damage from attacks that can leave their assets in tatters.

To better understand attitudes towards remote work, personal devices and the potential cybersecurity gaps that exist, Yubico surveyed more than 3,000 employees to pinpoint their attitudes and behaviours as it relates to at-home corporate security. Respondents varied from business owners to entry-level employees at companies with 250 or more employees, across sectors, in France, Germany and the UK. All of them have worked from home at some stage of the pandemic using work-issued devices.

The results offer fascinating insights into the use of work-issued devices for personal matters, sharing and remembering business passwords, the adoption of two-factor authentication (2FA), and other security measures. This report assesses how enterprises are responding. The main questions are: how is your business faring? And can you afford to be left behind?

3,006
employees

companies with
250+
employees

3
countries

12
verticals

Key findings

Only 55%

are more cautious about cybersecurity while working from home

51%

often **try to solve their own IT problems** rather than contacting IT

54%

admit they **use the same passwords** across multiple work accounts

Employees are engaging in poor cybersecurity practices since working remotely

Bad habits are widespread and, not surprisingly, poor password hygiene ranks high with 54% of all employees admitting they use the same passwords across multiple work accounts. But that's not where bad password practices end—22% of respondents report they still remember passwords by writing them down, including 41% of business owners and 32% of C-level executives.

Furthermore, 42% of respondents admit to using work-issued devices for personal reasons daily while working from home. Of these individuals, 29% are using work devices for banking and shopping, and 7% are watching illegal streaming services. What's worse is that business owners and C-level executives are among the biggest offenders—44% of business owners and 39% of C-level executives admit to performing personal tasks on work-issued devices every day since working from home.

Despite these risky behaviours, only 55% are more cautious about cybersecurity while working from home. Not to mention 73% of all employees declare themselves confident about spotting phishing attacks, which is cause for further concern given the rising success rates of modern phishing attacks. Even to the best-trained eye, these attacks can be difficult to spot, so with employees exhibiting increased levels of false confidence around phishing detection, attackers can find opportunities to strike while their guard is down.

73%

of all employees **feel confident** about spotting phishing attacks

Enterprises fall short on cybersecurity best practices as hybrid working persists

43% of all employees suggest that cybersecurity isn't the responsibility of the workforce, with 60% saying that IT teams should handle it all. However, data suggests that IT departments are not meeting employee expectations; only 37% of respondents say they feel more supported by IT than they did when working onsite with their firm's cybersecurity team close by.

A year after the pandemic began and work-from-home policies were implemented, 37% of all employees across sectors still report they are yet to receive cybersecurity training to work from home, leaving businesses hugely exposed to risk.

Meanwhile, a supportive top-down security culture is lacking in many organisations, causing employees to feel increased levels of anxiety or stress when dealing with IT or security problems. 51% often try to solve their own IT problems rather than contacting IT, and 40% who clicked on a suspicious link wouldn't immediately tell IT—14% would turn to Google instead.

37%

report they are **yet to receive cybersecurity training** to work from home

Only 27%

of firms are rolling out **FIDO-compliant hardware security keys**

Businesses are trying to address these problems but have not identified the most secure methods

Only 22% of respondents report that their company has introduced 2FA technology since the pandemic began, despite it being the best line of defence to protect against stolen, lost, and phished credentials that result in a majority of all account takeovers. The most popular security policies to be newly implemented are VPN access to corporate networks (46%) and frequent password updates (33%). Even among those whose organisations have implemented 2FA, a majority are overlooking the strongest forms of the technology. Only 27% of firms are rolling out FIDO-compliant hardware security keys, which offer the most advanced form of phishing protection, while others are instead relying on more vulnerable and outdated solutions, such as mobile authentication apps (54%) and SMS one-time passcodes (47%).

45% of all respondents now use mobile devices for work more than they did prior to the pandemic, proving the further need for more secure methods of authentication that are not tied to the mobile device itself. Mobile devices are multi-purpose computing devices, which naturally introduce a larger attack surface. If a user's mobile device is compromised (e.g. through SIM swapping), this automatically compromises any 2FA that is also tied to the same device.

Shaky security strategies

Shaky security strategies

Many employees at all levels of seniority feel confident about cybersecurity since COVID-19 caused an unprecedented rush to home working.

Only 37% of all respondents who worked in an office full time prior to the pandemic, but have since worked at home, now say they feel more vulnerable to a rising tide of cyber threats. The figure reaches 51% of people who were already doing their job at home pre-COVID.

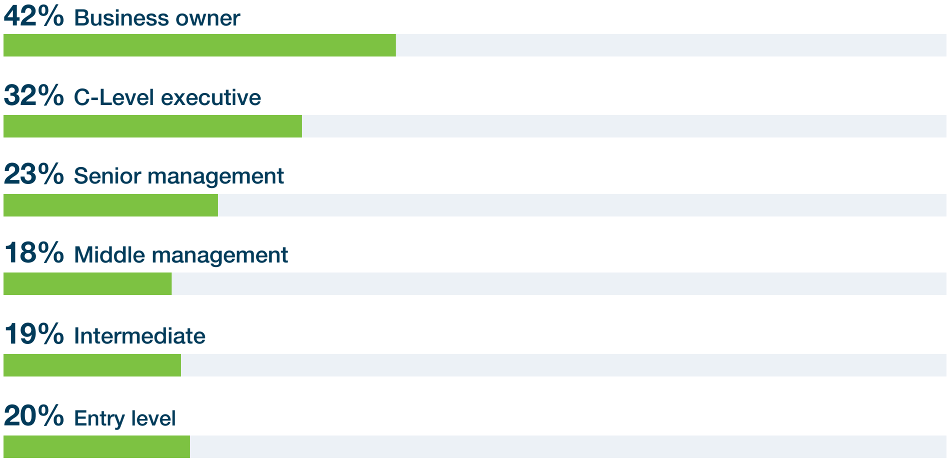
Complacency isn't the only issue that should worry cybersecurity teams—"DIY diagnosis" is another. 51% of all respondents try to solve their own IT issues before contacting their firm's tech experts. The figure rises to 61% of people who worked at home pre-pandemic.

Any potential or actual breach must be addressed immediately by all relevant parties at an organisation—including senior management, IT, HR, and legal. The longer security experts and senior management aren't in the loop, the harder a breach is to rectify—with potentially worse consequences for company finances and brand reputation.

Our survey also delivered the shocking statistic that 73% of respondents are confident they can spot a phishing attempt. In reality, phishing is one of the most common and successful forms of account takeover. It forms a majority of all breaches according to Verizon's 2021 Data Breach Investigations Report. This may indicate a false sense of confidence among employees who believe "It won't happen to me." In turn, this provides an opportunity for attackers to strike while defences are down.

Of the 73% of individuals who feel confident in spotting a phishing attack, 21% said they feel very confident. Of that amount, there is an increased confidence among high-profile users—the audience most likely to receive highly targeted phishing ploys. Here is the breakdown by seniority:

Targets of phishing ploys: high profile users



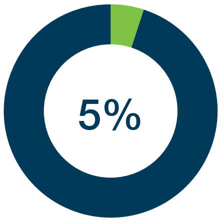
61%

of people who worked at home pre-pandemic **try to solve their own IT issues** before contacting their firm's tech experts

32%

of all **C-level executives feel confident** about spotting phishing attacks

Confidence in spotting phishing attempts also varies across sectors. While 31% all employees working in IT & telecoms, and 22% in financial services, are 'very confident' this drops to 18% in manufacturing and 12% in retail, catering & leisure. 1 in 20 respondents (5%) in healthcare do not even know what phishing is.



1 in 20 respondents **in healthcare** do not know what **phishing** is

Let's not forget it only takes one mistake born of over-confidence to cause existential threat to an enterprise.

While phishing may be among the worst consequences of misplaced cybersecurity confidence, our study unearthed numerous risky behaviours.

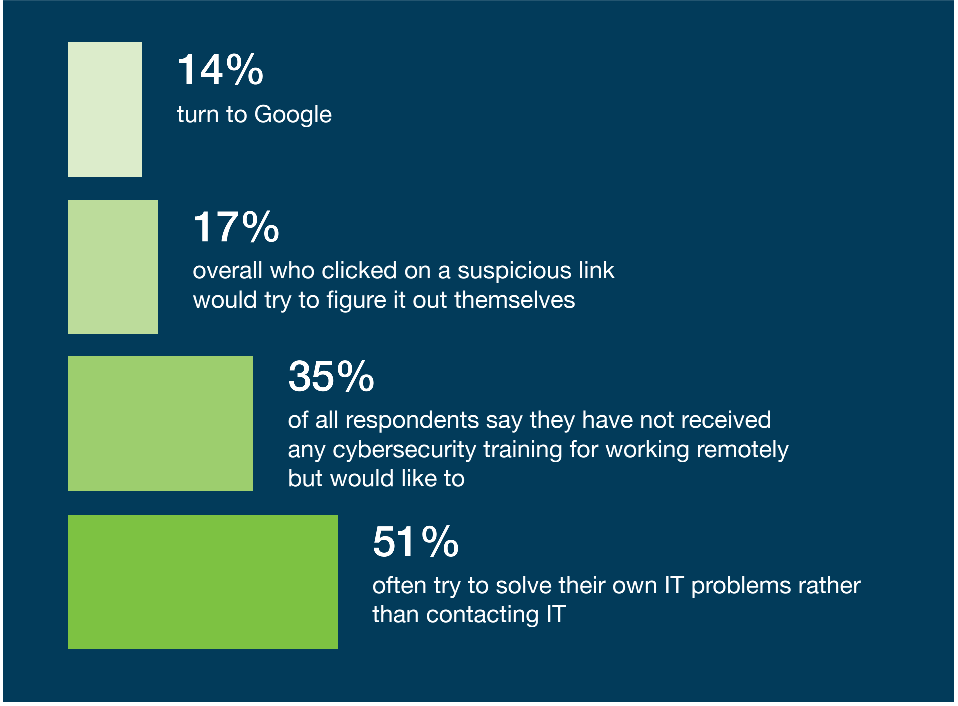
So who are companies' biggest cybersecurity culprits and what are their anxiety-provoking attitudes?

Concerning cybersecurity behaviours exist top-down

Many employees at all levels, from enterprise owners to entry-level staff, share misconceptions about cybersecurity and act poorly—with lack of faith in IT teams and processes one possible reason.

Bad habits are rife among those forced to work from home for the first time by the pandemic, and because remote work will likely continue, employees' unhelpful behaviour won't disappear.

Lack of faith in IT teams



14%
turn to Google

17%
overall who clicked on a suspicious link would try to figure it out themselves

35%
of all respondents say they have not received any cybersecurity training for working remotely but would like to

51%
often try to solve their own IT problems rather than contacting IT

Risky Behaviours

42%
of respondents admit to using work-issued devices for personal reasons daily while working from home

55%
are more cautious about cybersecurity while working from home

67%
of all respondents admit they'd sooner lose work credentials than personal data in a breach

29%
use work devices for both banking and shopping

7%
watch illegal broadcasts

14%
online gaming

19%
of respondents preferring to permanently work from home admit their partner uses their work-issued device

26%
of respondents who allow others to use their devices do so without offering security tips

73%
feel very or somewhat confident they can spot a phishing attack

76%
of those currently working from home feel very or somewhat confident they can spot a phishing attack

One of our most worrisome findings is the lack of a top-down approach to cybersecurity. Some 44% of business owners and 39% of C-level executives admit to performing personal tasks on work-issued devices every day since working from home. Additionally, 52% of senior managers do the same. They are not setting a good example, leading from the front on cybersecurity, and are consequently exposing their firms to unnecessary risk of cyber attacks. Junior staff are actually stricter about how they use their devices with 39% of both intermediate and entry-level employees using work devices for personal matters daily.

44%

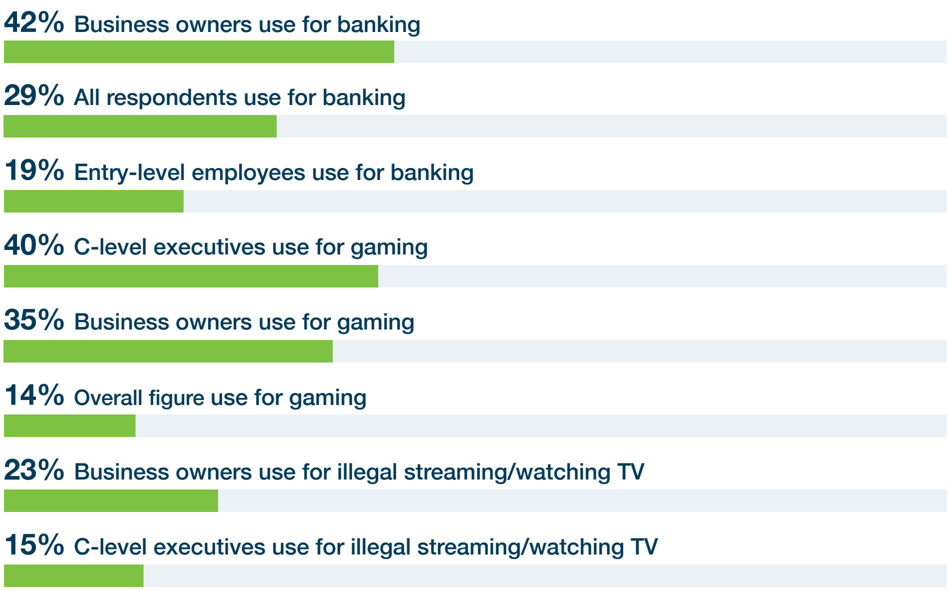
of business owners

39%

of C-level executives

admit to performing **personal tasks on work-issued devices** every day since working from home

Approach to cybersercuity: Business owners & C-level



Meanwhile, C-level executives and business owners are the most likely to admit allowing another person to use their work-issued devices. 45% of C-level executives and 42% of business owners let their partner do so; 34% of business owners and 27% of C-level employees allow their children to use these devices.

Seniority should not be taken as a signal of practicing good cybersecurity. In fact, these individuals may require increased measures of specialised cybersecurity training, and only 26% of business owners and 20% of C-level executives say they have yet to receive training in this vital area, exposing a knowledge gap at the highest level.

But cybersecurity oversight isn't confined to senior staff. Here are some of the key attitudes and assumptions of intermediate and junior employees:

Key attitudes and assumptions of mid-level and entry-level managers

Believe cybersecurity is the **sole responsibility of IT**

61% Mid-level managers

61% Entry-level managers

Would **try to fix an IT issue themselves** before seeking help

50% Mid-level managers

48% Entry-level managers

Feel more vulnerable to cyber attacks while working from home

39% Mid-level managers

31% Entry-level managers

37%

of both middle managers and intermediate employees **use work-issued devices for personal admin tasks** while working from home

30%

of entry-level respondents have **ignored required software updates** on their work devices since working from home

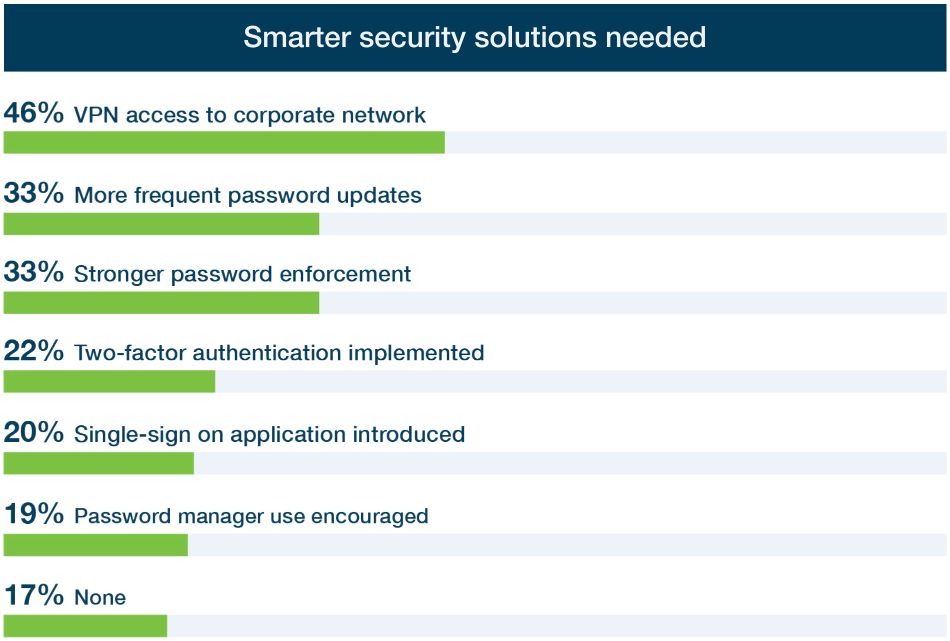
2FA and MFA: smarter security solutions

2FA and MFA: smarter security solutions

Let's focus on who is and isn't making headway in the mission to improve cybersecurity—and discover how two-factor and multi-factor authentication (2FA and MFA) can vastly improve it.

According to all of the respondents we polled, 83% said their organisations have introduced new cybersecurity policies since mass remote working began, with just 17% saying their company hasn't.

If we take a deeper look, however, the picture is less rosy with many employers needing to make investments in more secure policies.


Smarter security solutions needed

As 2FA offers the best first line of defence against cyber threats it is surprising that fewer than a quarter of enterprises have turned to this technology with more employees working remotely.

The problem with passwords

Many corporations have still turned to passwords as a preferred method of shoring up work-from-home cybersecurity. However, even with the best practices and hygiene, passwords fall short in terms of providing adequate security. Strong and unique passwords can be easily phished, so increasing efforts in this area is not a sure-fire way to improve organisation-wide security.

Nevertheless, many organisations continue to ramp up strong password policies, which are ultimately rendered pointless if employees reuse their credentials across services, which 19% of all our respondents admit to doing for all of their work accounts. A further 35% say they duplicate passwords across some work log-ins.

19%

of all respondents admit to **reusing passwords** for all work accounts

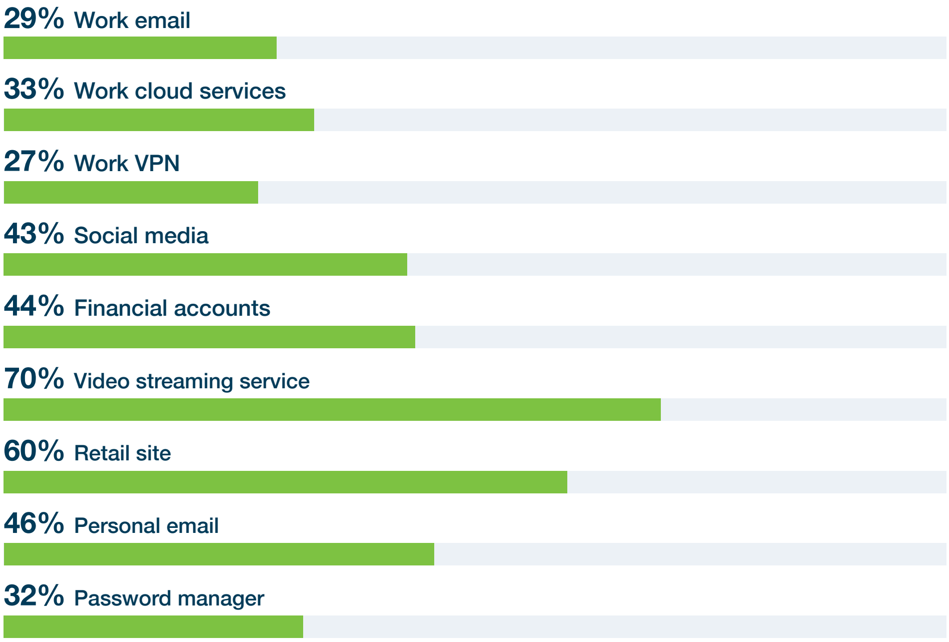
35%

duplicate passwords across some work log-ins

Jotting down passwords is even less secure, but still happens on a consistent basis. 22% write passwords down, including 41% of business owners and 32% of C-level executives—compared to 21% of entry-level employees. Using a password manager with strong 2FA is one option to improve password security but at present just 17% do so, the same for work and personal accounts.

Meanwhile, as the following table shows, a worrying proportion of everyone we surveyed would happily share passwords with their colleagues, family or friends:

Percentage of respondents that would share password, by account

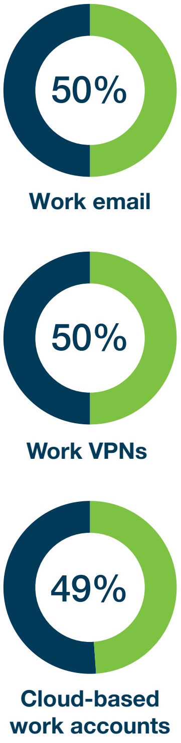


Even compromised passwords aren't considered a problem by many employees. Half say they would reuse a stolen password for their work email; a similar proportion claim the same for work VPNs, and 49% for cloud-based work accounts.

Apart from the real risks of continuing to view passwords as a catch-all security measure, employees whose company has implemented the below cybersecurity policies since working from home find them irritating. 58% consider updating passwords more frequently to be an additional burden on their daily workload, while the same proportion (58%) dislike the idea of using a password manager. A further 52% feel encumbered by being asked to select stronger passwords.

Stolen passwords

Percentage of respondents who say they would **reuse a stolen password**

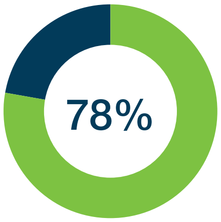


2FA's growing role in repelling cyber threats

When looking to replace cumbersome—and often ineffective—cybersecurity measures, 2FA and MFA should be top of mind for businesses.

Adding another layer of security beyond passwords helps to create another obstacle for bad actors in the case that an employee's credentials are phished, stolen, or reused. It is an effective, proactive measure rather than a way to simply react to attempted attacks.

What's more, using sophisticated MFA hardware—such as FIDO-compatible security keys that offer a fully secure single-gesture log-in flow—can successfully eliminate account takeovers from modern phishing and man-in-the-middle attacks.



A huge 78% of enterprises **are yet to realise the value of implementing 2FA**

Types of 2FA being introduced

54%	Mobile authenticator apps
47%	SMS OTP
32%	OTP hardware tokens
27%	Hardware security key

But the devil is in the detail. A huge 78% of enterprises are yet to realise the value of implementing 2FA. And even among those that do, only 27% use the most secure method, hardware security keys. They are the strongest alternative to password-driven security, giving convenient and more effective protection against breaches than other outdated forms, such as one-time passcodes sent via SMS or battery-operated hardware key fobs.

When it comes to utilising 2FA in the workplace, 38% of employees use it across all of their work accounts, and a further 32% do so for some accounts. But for companies to be as secure as possible that figure should be far higher.

It's critical, then, for organisations to take a holistic view of employee attitudes towards 2FA when designing people-centered solutions.

3

Cybersecurity across sectors

Financial services

Strong authentication and overall best practice around cybersecurity is crucial for the financial services industry where firms need to protect critical business and customer data. But research shows that while training levels are relatively good for employees at financial firms, and 90% of companies have introduced new policies, many lack some of the most important protection for a remote environment like 2FA. Plus, many are still overlooking the advantages of hardware security keys in favour of less secure tools.

Beliefs and behaviours

	Financial Services	Across Sectors
Cybersecurity measures Have not taken any additional cybersecurity measures in the pandemic	10%	17%
Sharing devices Allow others to use and do not pay attention to how people use them	22%	19%
Stressed by cyber threats Employees who feel more stressed by cyber threats while working at home rather than in the office	40%	35%
Suspicious links Would not admit to clicking on a suspicious link	10%	7%
Cybersecurity training Much more likely to have received cybersecurity training to work from home	44%	34%

	Pre-Covid	Post-Covid
Since working from home Employees who use work-issued devices daily for personal matters	29%	44%

42% banking

8% watch illegal streams/TV

Who owns cybersecurity?

IT Teams

61% of workers think that IT teams should fully own cybersecurity

Employees

62% think employees need to take more ownership

2FA Implementation: Financial Services

Financial Services	All sectors
27% have implemented 2FA use since employees worked from home	**22%** have implemented 2FA use since employees worked from home
26% have introduced use of hardware security keys	**27%** have introduced use of hardware security keys
49% have introduced use of mobile authentication	
44% have introduced use of SMS OTP	
40% have introduced use of hardware tokens	

Financial Services Employees

23%
of all employees never use 2FA across their work accounts

26%
never use 2FA for personal accounts—some of which they access via work devices

53%
of all employees find 2FA cumbersome, which is less than overall figures for single sign-on and password measures

Healthcare

Protecting patient data, increasing medical staff productivity and meeting regulatory compliance are challenges the healthcare industry is met with every day. The pandemic has highlighted the urgency for better security more than ever but research shows that there is still a huge task ahead to increase acceptance and adoption of cybersecurity measures. In an era of highly sensitive patient information this should sound alarm bells. Employees are taking a lax attitude towards using work devices, their firms aren't implementing proper 2FA technology and many employees believe they can self-diagnose security issues.

18%

of all employees would **ask Google** how to remedy clicking on a suspicious link

Beliefs and behaviours

	Healthcare	Across Sectors
Cybersecurity measures Healthcare firms who have not taken any additional cybersecurity measures in the pandemic	16%	17%
Sharing devices Allow others to use and do not do not think about the security aspects of doing so	29%	26%
Supported by IT Feel less supported by IT while working compared to the cross-industry average	42%	36%
Solve tech problems Attempt to solve their own tech problems rather than telling IT	61%	51%

	Healthcare Teams	Employees
Ownership of IT More people believe IT teams should fully own cybersecurity than think employees need to take more ownership	68%	63%

	Pre-Covid	Post-Covid
Since working from home Employees who use work-issued devices daily for personal matters	37%	42%

39% conduct personal admin tasks on them

10% illegally stream / watch TV on them

2FA Implementation: Healthcare

Healthcare	All sectors
21% have implemented 2FA use since employees worked from home	**22%** have implemented 2FA use since employees worked from home
32% have introduced use of hardware security keys	**27%** have introduced use of hardware security keys
54% have introduced use of mobile authentication	
58% have introduced use of SMS OTP	
36% have introduced use of hardware tokens	

Healthcare Employees

29%
of all employees never use 2FA across their work accounts

28%
never use 2FA for personal accounts—some of which they access via work devices

60%
of all employees find 2FA cumbersome—the highest for any new security measures introduced in this sector

IT & Telecoms

The pandemic has driven us to rely more heavily on connectivity than ever before, and the telecom and IT industries lie at the heart of ensuring we stay connected. But due to the overwhelming amount of sensitive information available, bad actors are taking advantage. Research shows that while not as high as in some sectors, training in IT & telecoms has been offered to more employees than the all-industry average. However, nearly 6 in 10 (58%) try to solve their own IT issues—almost a fifth (17%) would Google what to do upon clicking on a suspicious link—a concern to cybersecurity teams and business leaders. This sector is also yet to widely adopt the most secure forms of 2FA hardware, suggesting there is vast scope for further implementation.

Beliefs and behaviours

	IT & Telecoms	Across Sectors
Cybersecurity measures Firms who have not taken any additional cybersecurity measures in the pandemic	9%	17%
Cybersecurity training Received cybersecurity training to work from home workers	41%	34%
Sharing devices Allow others to use work-issued devices and do not pay attention to how people use them	21%	19%
Stressed by cyber threats Feel more stressed by cyber threats while working at home rather than in the office	43%	35%

	IT Teams	Employees
Ownership of IT Slightly fewer agree that IT teams should fully own cybersecurity than think employees need to take more ownership	61%	64%

	Pre-Covid	Post-Covid
Since working from home Employees who use work-issued devices daily for personal matters	34%	42%

34% use work devices to shop

25% use devices for gaming

*****

19%

of all respondents admit to **reusing passwords** for all work accounts

35%

duplicate passwords across some work log-ins

58%

of employees try to **solve their own IT issues**

17%

almost a fifth of employees **would Google what to do** upon clicking on a suspicious link

2FA Implementation: IT & Telecoms

IT & Telecoms	All sectors
31% have implemented 2FA use since employees worked from home	**22%** have implemented 2FA use since employees worked from home
30% have introduced use of hardware security keys	**27%** have introduced use of hardware security keys
58% have introduced use of mobile authentication	
48% have introduced use of SMS OTP	
43% have introduced use of hardware tokens	

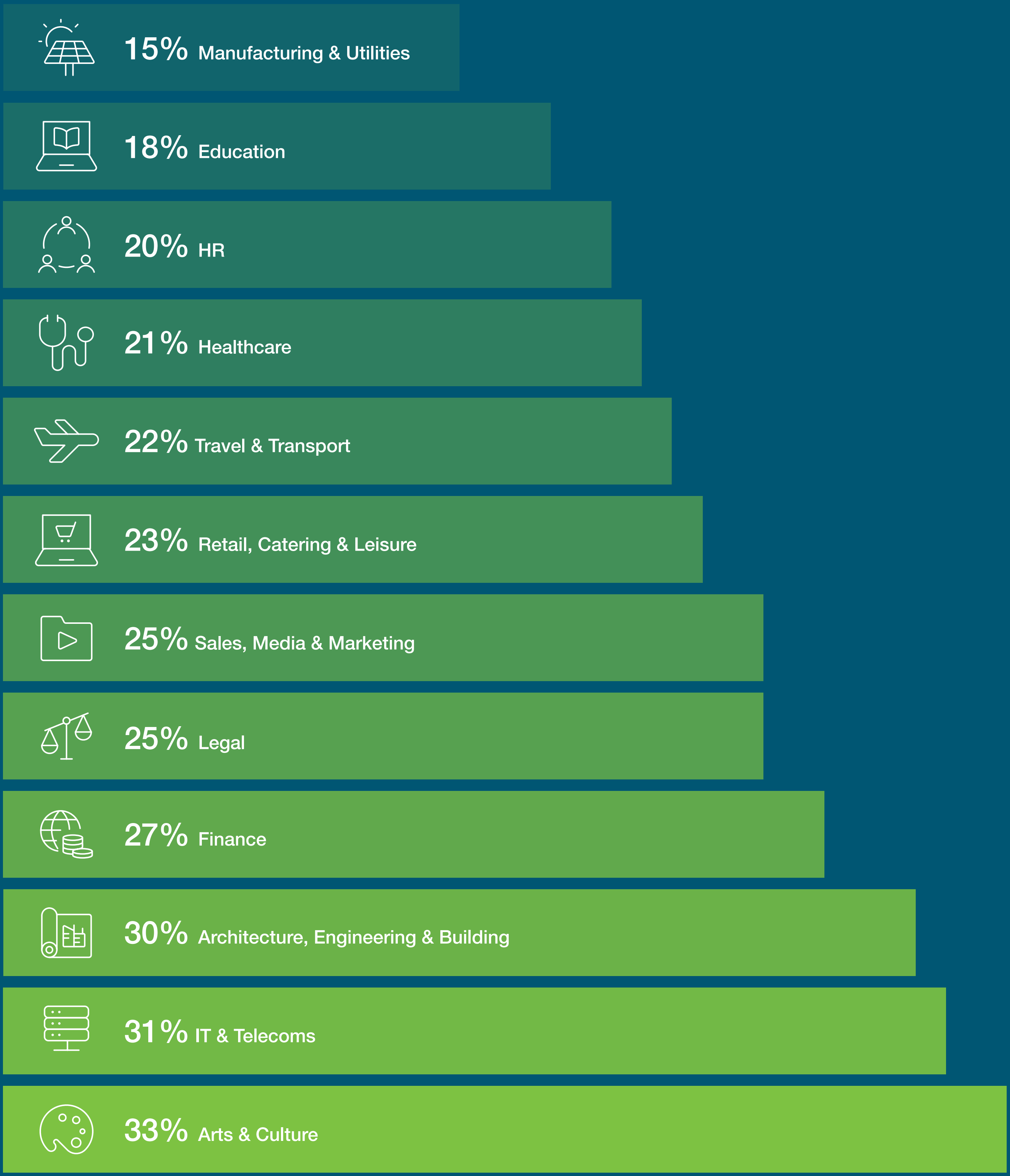
IT & Telecoms Employees

22%
of all employees never use 2FA across their work accounts

19%
never use 2FA for personal accounts—some of which they access via work devices

57%
of all employees find 2FA cumbersome, less than overall figures for single sign-on and password measures in this sector.

Ranking of sectors introducing 2FA since the pandemic began



4

Market forces: cybersecurity by country

France

Employee habits—all respondents in France

Everyday personal use of work-issued devices:

41%
Pre-Covid

53%
Post-Covid

Main personal use activities on work devices:

37%
Admin

35%
Article reading

27%
Banking

10%
Gaming

10%
Illegal streaming

Everyday work use of personal devices:

30%
Pre-Covid

42%
Post-Covid

Allow third parties to use device:

78%
Business owner

70%
C-level

Remembering work passwords:

23%
Write down

14%
Password manager

11%
Save to document on the device

11%
Same password for multiple accounts

Use of work credentials:

28%
Share work email password

23%
Would use same work log-in again after breach

75%
Would rather have work credentials than personal data stolen

Cybersecurity and IT:

40%
Feeling more vulnerable to cyber threats since working from home

36%
Feeling unsupported by IT

30%
Completed cybersecurity training for remote work

KEY FINDINGS

A lax attitude to cybersecurity is not exclusive to French employees but some of their actions and beliefs are of concern.

Alongside the revelations above, 26% of those who hope to continue working remote post-pandemic ignore software and operating system updates for their work-issued devices. These are vital to maintaining a barrier against cyber threats.

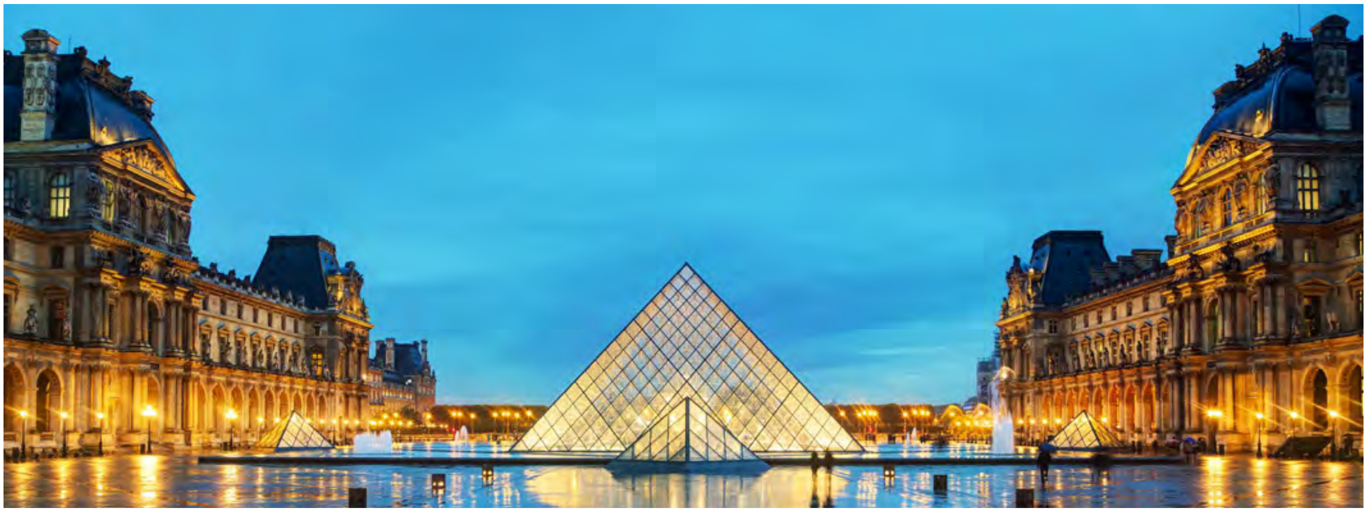
While 59% of all respondents based in France believe IT should be solely responsible for cybersecurity, 63% believe home-working employees should take more ownership.

Just 30% of all respondents say they have received security training, and 36% feel they are less supported by IT compared to working in the office.

This is likely prompting the 48% of all employees who attempt to fix IT issues on their own rather than notifying IT, and this percentage rises to 69% for both business owners and the C-suite. As we have seen, this can be linked to over-confidence about spotting phishing attacks—with 67% of all employees feeling they can identify one.

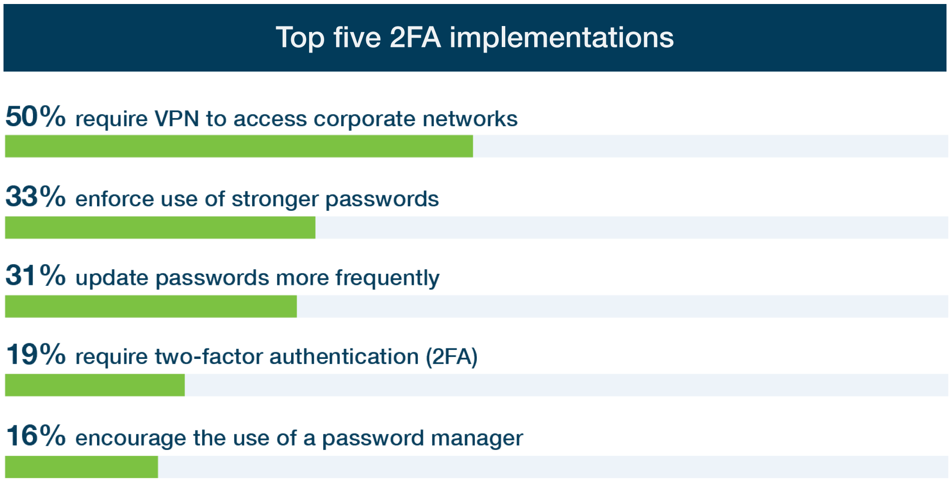
67%

confident about spotting a phishing attempt



2FA IMPLEMENTATION

What are firms in France doing to improve cybersecurity practice among employees? The top five implementations are:


Top five 2FA implementations

Delving into the detail, mobile authentication (40%), SMS one-time passcodes (OTP) (53%) and hardware security keys such as YubiKey (28%) are the top implementations since working from home became more widespread.

However, 54% of French respondents whose company has implemented 2FA since working from home said that it has been cumbersome or disruptive to their workflow.

There's clearly a long way to go before French organisations are confidently equipped to secure a long-term remote workforce: 38% of employees never use 2FA for work accounts—and only 34% do so for personal log-ins.

Cybersecurity teams must find ways to implement seamless security solutions for employees, since over half of respondents (54%) find 2FA disrupts their workflow.

Germany

Employee habits—all respondents in Germany

Everyday personal use of work-issued devices:

21% Pre-Covid

30% Post-Covid

Main personal use activities on work devices:

48% Article reading

40% Social media

34% Admin

31% Banking

31% Shopping

19% Gaming

Everyday work use of personal devices:

19% Pre-Covid

28% Post-Covid

Allow third parties to use device:

90% Business owner

65% C-level

Remembering work passwords:

23% Write down

21% Password manager

12% Save to document on the device

8% Same password for multiple accounts

Use of work credentials:

31% Share work email password

63% Would rather have work credentials than personal data stolen

21% Would use same work log-in again after breach

Cybersecurity and IT:

36% Feeling more vulnerable to cyber threats since working from home

32% Feeling unsupported by IT

Immediate reaction to clicking suspicious link during work:

59% Tell IT ASAP

18% "Ask Google"

KEY FINDINGS

In Germany, some employees have taken a stricter approach to cybersecurity during the pandemic. While everyday personal use of work-issued devices has risen overall, the proportion of people doing this who already worked from home pre-pandemic actually fell from 42% to 34%—suggesting they are more conscious of the increased risk.

As with the overall responses, business owners are no saints when it comes to security: a quarter of them who are based in Germany admit using work devices for illegal streaming.

Only 35% say they have received cybersecurity training from their employer. This includes half of all C-level executives, but only a quarter of entry-level employees.

Patching is patchy, too; important updates on work devices are strongly neglected, only 11% on average keep their work devices updated, along with a further 27% of home workers.

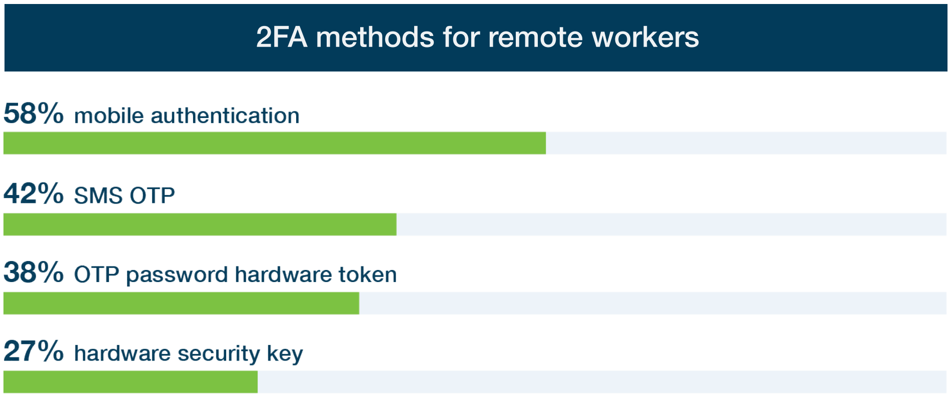
Additionally, respondents based in Germany are overly confident in spotting a phishing attempt with 71% of all employees stating they are very or somewhat confident.

71%

confident about spotting a phishing attempt

2FA IMPLEMENTATION

What are firms in Germany doing to improve cybersecurity practice among employees? 53% have added SSO, 37% have added VPN access and 47% have added 2FA.


2FA methods for remote workers

Winning over a majority of employees in Germany to get onboard with security functions will take more effort and resources: 57% find password managers disruptive, 47% think the same about 2FA, and although VPN is the most accepted form of security, 37% still label it disruptive.

United Kingdom

Employee habits—all respondents in the UK

Everyday personal use of work-issued devices:

25%
Pre-Covid

44%
Post-Covid

Main personal use activities on work devices:

36%
Article reading

36%
Admin

36%
Shopping

30%
Banking

28%
Social media

15%
Gaming

Everyday work use of personal devices:

25%
Pre-Covid

38%
Post-Covid

Allow third parties to use device:

73%
Business owner

71%
C-level

Remembering work passwords:

20%
Write down

15%
Password manager

16%
Save to document on the device

9%
Same password for multiple accounts

Use of work credentials:

31%
Share work email password

62%
Would rather have work credentials than personal data stolen

22%
Would use same work log-in again after breach

Cybersecurity and IT:

42%
Feeling more vulnerable to cyber threats since working from home:

39%
Feeling unsupported by IT

38%
Completed cybersecurity training for remote work

Immediate reaction to clicking suspicious link during work:

59%
Tell IT ASAP

16%
Figure it out myself

12%
“Ask Google”

KEY FINDINGS

UK business owners are stricter about their own personal use of work on their devices than their counterparts in Germany and France.

In contrast, UK-based employees have become more relaxed: 20% more of them admit to using work-issued devices for personal affairs since working from home.

Meanwhile, UK respondents feel less supported by IT than those in Europe—but they’re also the most confident in their own ability to spot phishing attacks, with 80% of all employees indicating they could identify an attempted breach.

This combination is concerning, an apparent ‘DIY culture’ born from perceived inaccessibility of expert help.

Just as in the other markets surveyed, a large majority would rather lose work than personal credentials. It’s worth remembering—and reminding employees—that protecting all credentials is vital to excellent overall cybersecurity.

80%

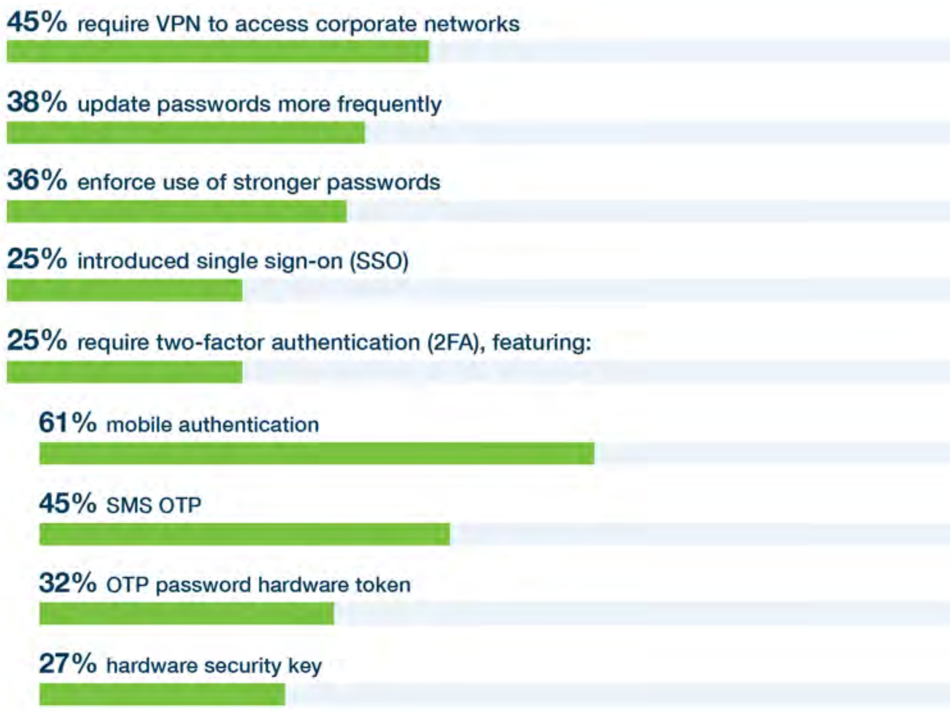
confident about spotting a phishing attempt

2FA IMPLEMENTATION

UK business cybersecurity experts are on the case but as in other markets 2FA still lags behind adoption of other solutions.

Yet 15% of businesses are yet to add any further measures, and 58% of all employees in the UK consider 2FA cumbersome, with SSO disliked by 62%—although this falls to 52% for VPN access. Password managers are deemed cumbersome by 65%, using stronger passwords by 57%, and 65% do not like frequently updating passwords.

Additional cybersecurity policies implemented since working from home



Conclusion

So the COVID-related saying goes, “no one is safe until everyone is safe.” In other words, until vaccines have given enough people protection against the disease, it will remain a serious threat everywhere.

The same ethos can be applied to cybersecurity. If even one employee persists with risky behaviour, your entire organisation is left open to bad actors and a potentially operation-crippling breach.

Hopefully the wealth of data in this report has given you food for thought about cybersecurity practices and technology at your enterprise.

Better cybersecurity starts with an awareness of what your employees think about it and how they are behaving. It’s then a matter of rolling out tools that build trust in their use, no matter where your teams are, the devices they use or the tasks they perform.

Regardless of seniority it’s clear employees across firms, sectors and countries we surveyed are at best confused about best practice, and at worst ignore security altogether.

This ranges from a penchant for DIY diagnosis and repair of IT issues to misplaced confidence that they can spot a phishing attempt.

While these approaches could be catastrophic for your business, it isn’t all your employees’ fault. Many of them are yet to be trained in cybersecurity best practice, and there is a gulf in trust between remote workers and IT teams by whom they feel unsupported.

The remedy to this is better defences and better processes that will shore up your organisation’s security. During the pandemic, firms have implemented many changes and additional cybersecurity measures, including two-factor authentication. There is still much room for growth in the most effective form of 2FA, hardware security keys.

As the working environment changes for good, smart enterprises are already recognising that cutting-edge cybersecurity tools can propel positive outcomes; from employee compliance, to easy and secure access to all of the assets people need to be productive.

Methodology

Yubico's survey was conducted by independent research company Censuswide, polling 3,006 employees at large organisations (250+ employees)—who have worked from home at some stage of the pandemic and also use work-issued devices—in the UK, France and Germany between February 19, 2021 and March 3, 2021.

The survey included:

156 business owners
122 C-level executives
355 senior managers
933 middle managers
1,021 intermediate-level employees
223 entry-level employees
196 'other' roles

And covered the following sectors:

Architecture, Engineering & Building
Arts & Culture
Education
Finance
Healthcare
HR
IT & Telecoms
Legal
Manufacturing & Utilities
Retail, Catering & Leisure
Sales, Media & Marketing
Travel & Transport
Other

Censuswide abides by, and employs members of, the Market Research Society, which is based on the ESOMAR principles.

yubico

About Yubico

Yubico sets new global standards for simple and secure access to computers, mobile devices, servers, and internet accounts. The company's core invention, the YubiKey, delivers strong hardware protection, with a simple touch, across any number of IT systems and online services. The YubiHSM, Yubico's ultra-portable hardware security module, protects sensitive data stored in servers.

The company's technology is deployed and loved by 9 of the top 10 technology companies, 4 of the top 10 U.S. banks, 2 of the top 3 global retailers, and by millions of users in more than 160 countries. Yubico is also a leading contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor open authentication standards. Founded in 2007, Yubico is privately held, with offices in Sweden, UK, Germany, USA, Australia, and Singapore. For more information: www.yubico.com.