Lookout™

The State of Remote Work Security

Hybrid Work And BYOD: Enterprise Security Risks On The Rise

With workers now able to work from anywhere and on any device, new security solutions are needed to enable employees while protecting the organization.

Introduction

Companies have always enabled some of their employees to work from anywhere.

And thanks to cloud and mobile technologies, the number of remote workers have steadily increased. But in recent years, largely due to the COVID-19 pandemic, this trend accelerated significantly. Prior to the pandemic, the percentage of employees working remotely in the United States and Europe hovered around 5%. In 2020 and 2021, it shot up to 40%. In 2022, the number of remote workers represented 30% of the overall workforce.[1,2,3]

The remote work trend and the acceleration of digital transformation has meant that the cloud has become a crucial backbone for most organizations. In 2020, 61% of businesses in the U.S. had migrated their workloads to the cloud – triggered by the need to quickly support remote work. As of 2022, 60% of all corporate data was stored in the cloud.[4]

While providing employees with remote access to corporate data in the cloud provides flexibility and potential boosts to productivity, cloud computing coupled with bring your own device (BYOD) policies can also increase an organization's exposure to risk and has huge implications for IT security.

With electronic files and communications no longer limited to the confines of office walls, IT departments have limited ways to view, understand and protect their sensitive data. To tackle the security challenges related to this new normal, organizations need a completely new approach to security. Security will need to keep pace with the way remote users access data and collaborate with one another.

Executive Summary

The boundaries between work and home have blurred. People are using personal devices, also known as bring your own device (BYOD), to get work done. And increasingly, BYOD includes mobile devices such as tablets and smartphones, where it becomes easy to mix personal and work tasks.

When people use devices that are not managed by the organization, IT does not have any control over whether operating systems and applications are up to date, which increases the risk of exposure to software vulnerabilities. The same goes for apps that employees use that have not been approved for enterprise use, a problem known as “shadow IT.”

In hybrid work, attacks such as mobile phishing and social engineering are much more effective when targeting devices that are used for personal activities. And because cybersecurity training still focuses on employees that work inside offices with corporate-issued laptops, users are often not equipped to identify these attacks.

Away from watchful eyes in the office and accustomed to the flexibility of hybrid work, employees are less likely to follow data security best practices. This report shows remote workers engage in unsafe data practices out of convenience, which means their organization is exposed to increased risks from unintentional negligence.

The workers of today no longer reside within a traditional security perimeter. So what can an organization do to protect its data? First, set a baseline of security expectations for any device used for work, regardless of whether it’s personal or corporate owned. Second, use a cybersecurity platform that has visibility into all activities, whether it occurs on BYOD mobile devices or in cloud apps.

Key Findings

43% use their own device

Remote employees that use their own device in place of company-issued equipment.

Jump to Page 8

Nearly 1 out of 3

Remote employees that work 20+ hours per week using personal mobile devices.

Jump to Page 22

Nearly 9 out of 10

Remote employees that work in a place other than their home, with an average number of 5 different locations.

Jump to Page 15

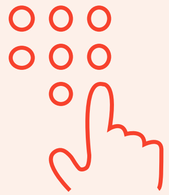
32% use unapproved apps or software

Remote employees that use apps or software that are not approved by their IT department.

Jump to Page 16

45% use a sharing password

The percentage of remote employees that use the same password for both work and personal accounts.



Jump to Page 22

46% save work files onto their personal device

Remote employees have saved a work file onto their personal device instead of their employer's network drive.

Jump to Page 22

92% of remote workers

Perform work tasks on their personal mobile devices.

Jump to Page 11

31% less likely to follow safe security practices

The number of remote employees who are less likely to follow safe security practices when working remotely.

Jump to Page 21

Chapter 1

Home and Work Have Blurred

06

Home and work have blurred

Work routines have definitely changed, but how? And what are the implications for IT security?

With the rise of remote work, the boundaries between work and home have become less distinct as people attend to work and personal tasks simultaneously throughout the day — and often on the same device. Moreover, work has crept into personal time, with remote workers actually putting in more hours on evenings and weekends than in-office workers. [5]

The blurring of boundaries between work and home has introduced additional risks to the enterprise, including risks associated with mobile and personal devices.

A recent study found that people typically have their smartphones with them at all times, which means that the barrier to using these devices is much lower than compared to a laptop or desktop computer – a habit that has a rippling effect on cybersecurity. [6]

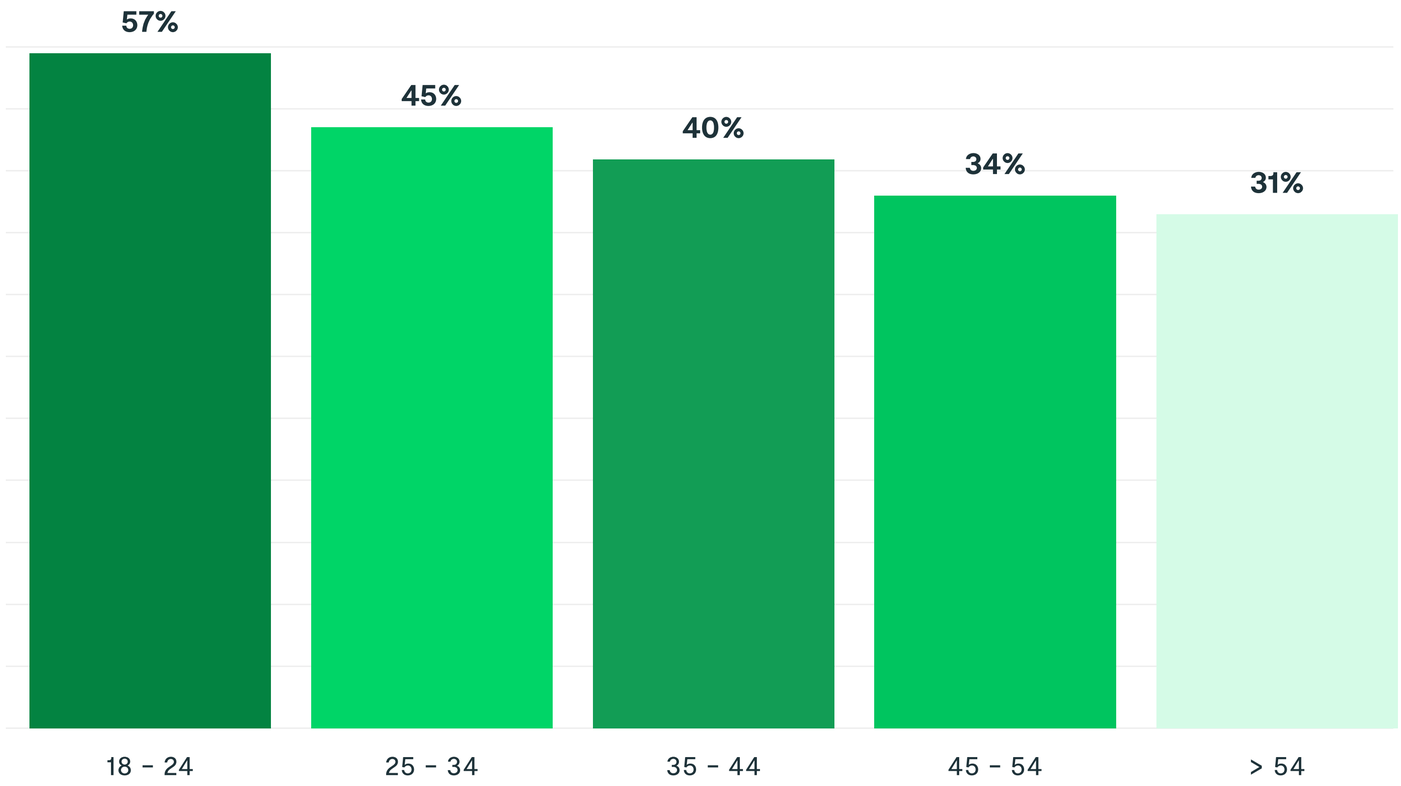
A number of factors related to remote work increase the risk posed to an organization's sensitive information. The data findings below reveal these risky behaviors and practices.

The Rise of Bring Your Own Device (BYOD)

One of the major trends related to remote work is the use of personal devices, or “Bring Your Own Device” (BYOD), for work instead of corporate-owned devices.

While BYOD programs provide flexibility and potential boosts to productivity, they also introduce a number of security risks. Because these devices are most likely not managed by IT, organizations have little visibility or control over the risks they pose. This includes operating system and app vulnerabilities, the types of apps that access corporate data, as well as threats such as phishing that the user is exposed to. Organizations need to keep in mind that with cloud apps, any device can have easy access to sensitive data, not just corporate-issued laptops.

Younger workers are more likely to BYOD



% of remote workers per age group who bring their own device for work

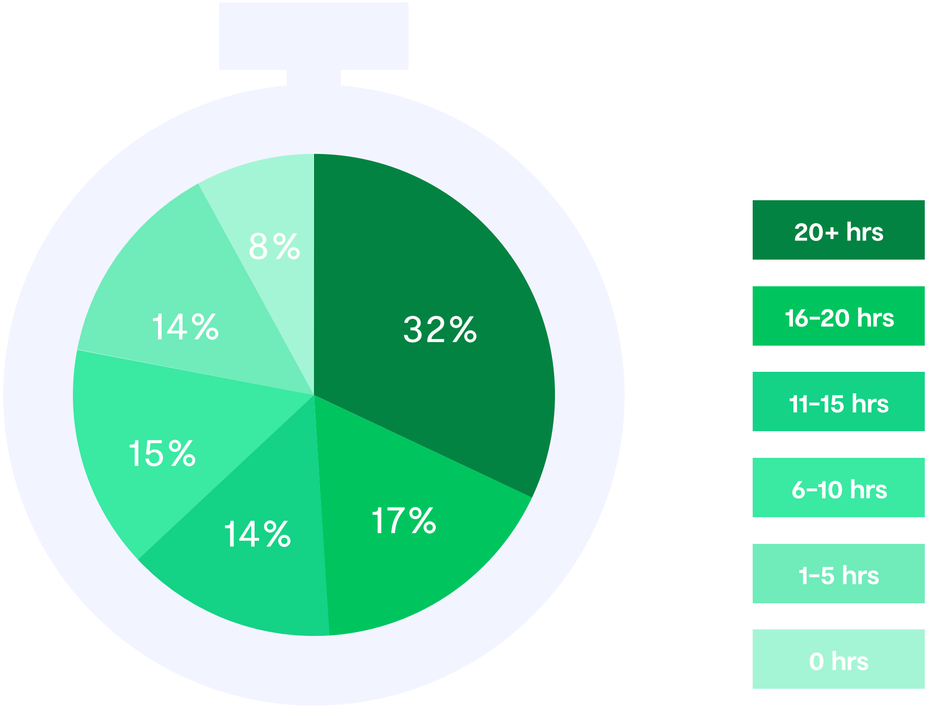
Employees working more from their tablets and smartphones

The vast majority of remote workers perform work tasks — and spend a great deal of time on those tasks — on their personal mobile devices. This practice poses security risks on two fronts:

One, mobile devices often operate outside corporate networks, which means that any perimeter-based security tools cannot protect them.

Two, these devices often have dozens of apps installed, and not all of them are approved by IT. Therefore, any data accessed by the device is exposed to countless new risks, including risky data access and phishing attacks.

Nearly 1/3 of remote employees spend 20+ hours per week working on their personal mobile devices



% of employees doing work tasks on personal tablets or smartphones per week

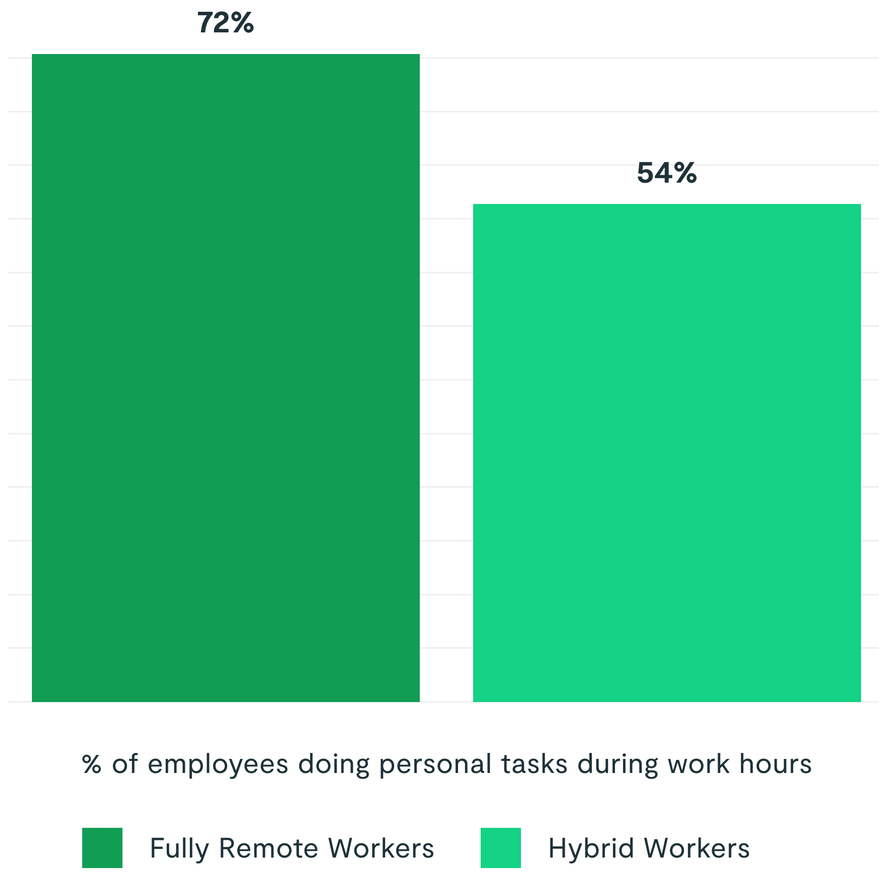
Personal and work tasks are blurring together

Prior to the proliferation of remote and hybrid work, there was a clearer line between work and personal life — whether it's the computer a user only has access to in the office or the time they stop working to commute home.

This is no longer the case.
The survey results show that personal and work tasks are blurring together, and the boundaries between the two have become more porous. A significant number of people mix work and personal tasks, with 72% of fully remote workers and 54% of hybrid workers doing personal tasks during work hours.

These shifts have implications for IT security risk exposure, for both fully remote and hybrid workers in any organization.

Fully remote workers are more likely to do personal tasks during work hours

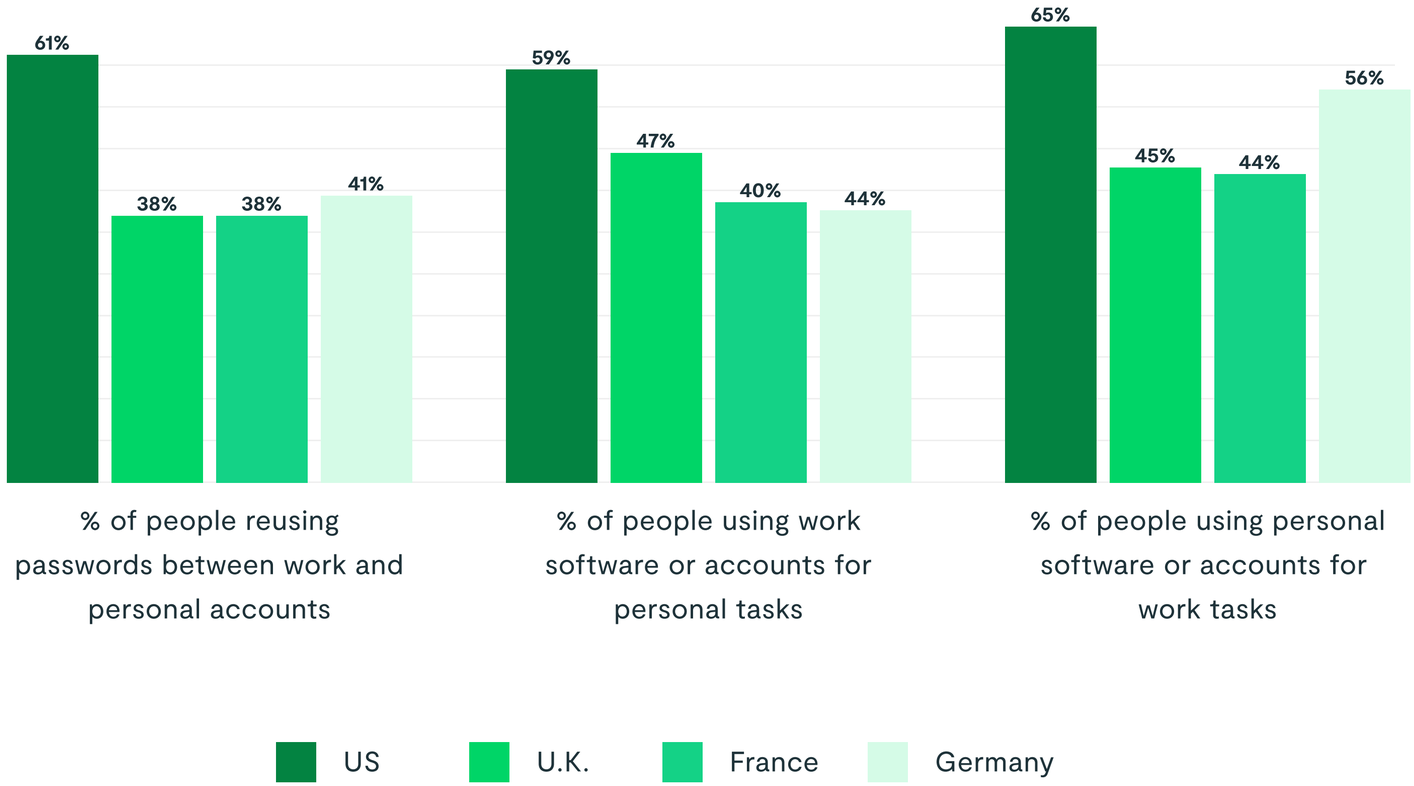


Work and personal security start to mix

Remote workers were asked several questions to assess the boundaries of their work and personal security practices.

On all three measures, a sizable portion of remote workers mixed personal and work security practices. These practices pose significant IT security risks.

About half of remote workers mix work and personal security



Chapter 2

Organizations Are More Vulnerable

12

Organizations are more vulnerable

While the boundaries between home and work have blurred, vulnerabilities exist on the organizational side as well.

In the past, enterprise cybersecurity infrastructure was built with the goal of having an impenetrable fortress.

However, with a large portion of employees working remotely beyond a physical corporate office space, this approach has become outdated. The proliferation of mobile devices has only made this more of a challenge. New security threats arise from distributed work environments as the attack surface has now left the building.

The rapid adoption of web solutions is problematic because they tend to come with relatively basic security settings. A previous Lookout study found that attackers leverage these platforms against users, evidenced by the fact that users are far more likely to be phished if they're using a cloud-based productivity app.

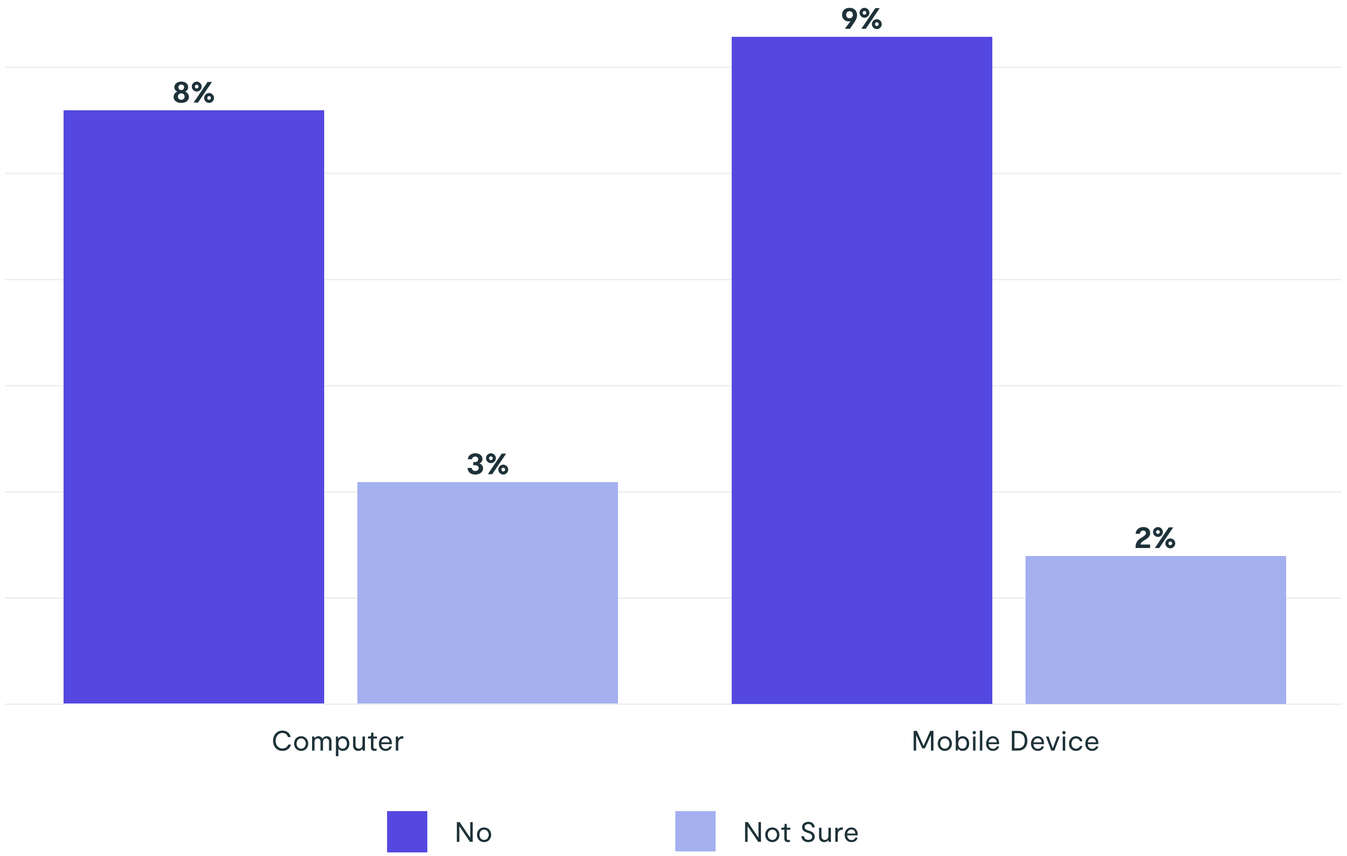
Moreover, personal devices and apps are far more likely to be out-of-date than work devices since they cannot be forced to update, which means they are not protected against the latest vulnerability exploits and malware. With training specifically for mobile security lagging and phishing attack incidents are on the rise, mobile phishing has now become the most lucrative attack vector for cybercriminals.

Personal devices are out of date

One of the most difficult challenges with remote workers using personal devices for work is ensuring that their devices are up to date. Nowadays, almost every mobile OS update is centered around security.

In the BYOD model, it is the responsibility of the employee to update their device, not the employer. Without software updates, defenses are down.

Is your personal device up-to-date with the latest OS?



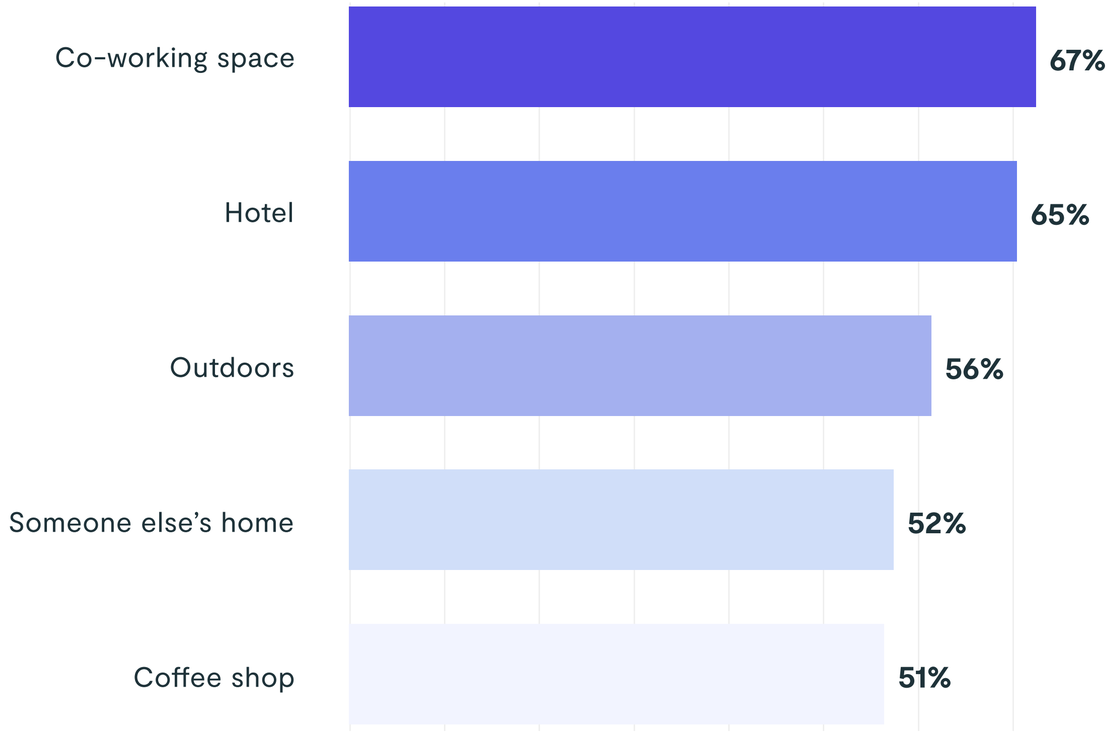
“Work from anywhere” brings new security risks

While most remote employees work from home, our study found that most people work from several different locations in addition to home.

Working from multiple remote “offices” brings new security threats. Company data can be exposed to risks present in the multiple networks that are not monitored by the company’s IT department. In addition, having devices in multiple physical locations also increases the risk of accidental access, loss, and theft. The most popular places to work besides home are public spaces such as co-working spaces, hotels, and outdoors.

The most popular places to work besides home are public spaces such as co-working spaces, hotels and outdoors.

Percentage of remote workers that work in different locations (besides home)



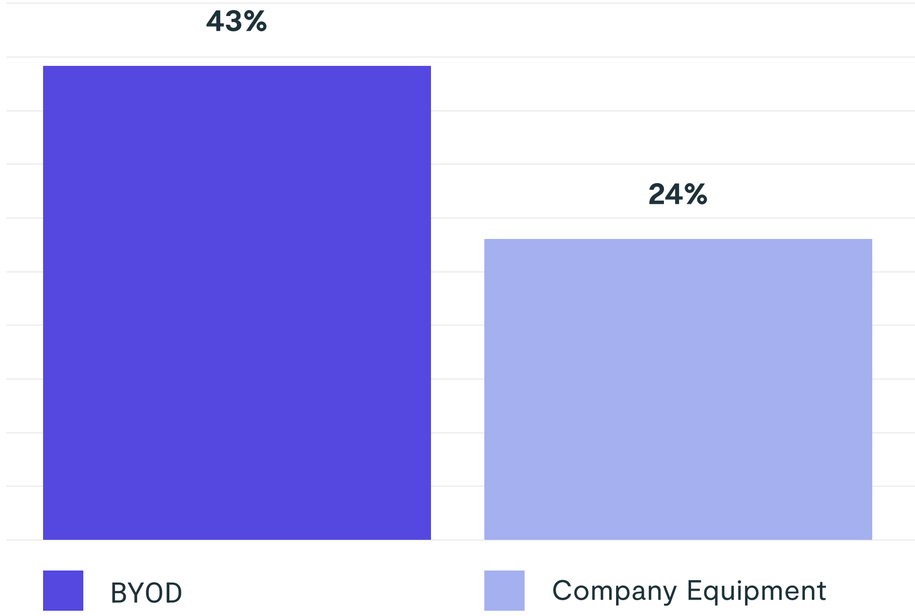
Shadow IT: Unapproved app exposes data

Shadow IT is the use of applications or devices that have not been vetted by the employer's IT department. This challenge has grown exponentially due to the rise of cloud-based applications, which are accessible from any device. Shadow IT introduces security risks because the IT department cannot ensure that the app used is secure and follows best practices to minimize the chances of data leakage.

Our study shows that employees using BYOD tend to have twice as many unapproved apps than those using company-issued equipment.

About one out of three remote workers said that they used apps or software that are not approved by their IT department out of convenience.

Shadow IT is a much bigger risk on BYOD than on company-issued equipment

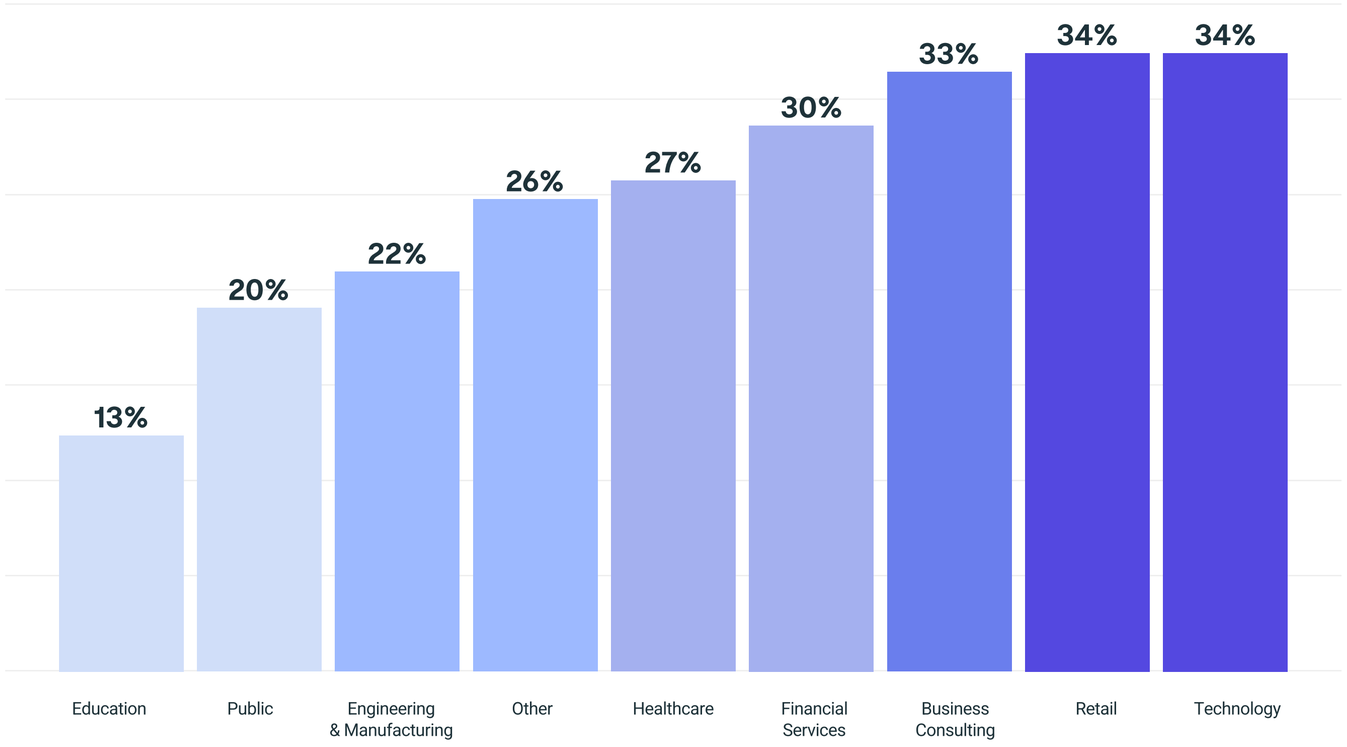


Training has not kept up

A company's cybersecurity posture is only as strong as its weakest link, and that weakest link is often the employees themselves. Thus, employees need to be trained on secure data practices in order to reduce human error and keep company data secure from phishing, malware, and hackers.

The industries with the highest rates in lack of remote security training for remote security were all private industries — technology, retail, business, and financial services. The industries with that best perform in training for remote security were education and public administration.

Technology and retail sectors rank the highest in lack of remote security training amongst employees



% of employees that don't have the necessary tools/training to protect corporate data remotely per sector

Remote workers are more heavily targeted

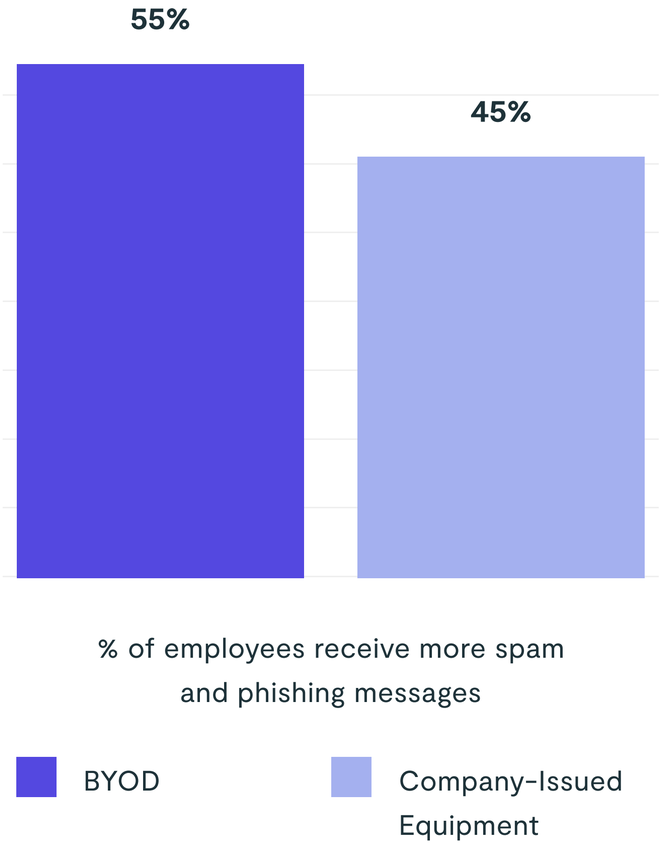
Remote workers present an attractive population of targets for attackers, as they may be using insecure networks and unmanaged devices. At the same time, organizations have moved their data to the cloud, which means any risks to the end user could easily translate to the organization.

The data shows that remote workers are targeted more frequently by phishing attacks in an attempt to steal their corporate login credentials, and that employees who used BYOD were more likely to encounter phishing attempts than employees who used company devices. Why is this?

First, users on personal devices often have countless apps that threat actors use as avenues for their phishing attacks. Any app with messaging functionality (which includes SMS, WhatsApp, third-party messaging platforms, gaming, and even dating apps) can be used for phishing attacks.

Second, employees act with far less caution if they are on a personal device versus a work-issued device, which means that they are more likely to engage with a suspicious link.

About 5/10 remote workers receive more spam or phishing messages than they used to



Chapter 3

Remote Workers Are More Careless

19

Remote workers are more careless

Data breaches aren’t always caused by an outside intruder.

One of the greatest threats to an organization’s data security is its own employees and the potential for human mistakes or carelessness. In fact, one study found that 95% of cybersecurity breaches are caused by human error. [7]

Remote workers are less careful because they work in a more fluid environment where work and life have merged. One of the biggest threats to corporate information is the use of weak or recycled passwords, which negates the effectiveness of security software and other data protection solutions that may be in place. Hackers can use software to crack weak passwords. Once they have a set of credentials that works, they can use them on other cloud apps to access and steal an organization’s or an individual’s sensitive data.

In addition to increased risk of credential compromise, data protection capabilities outside the office are not necessarily the same as those inside the traditional perimeter. File storage and file sharing in the office is often on a corporate network and protected by encryption, whereas the same protection is not there in a remote setting.

Employees also make unintentional mistakes while working remotely. One of the more common causes of unintentional data leakage is when an employee is logged into both their personal and work account in the same app and mistakenly downloads sensitive data to their personal account. Under any compliance standard that requires data to stay within certain boundaries, this would count as a violation.

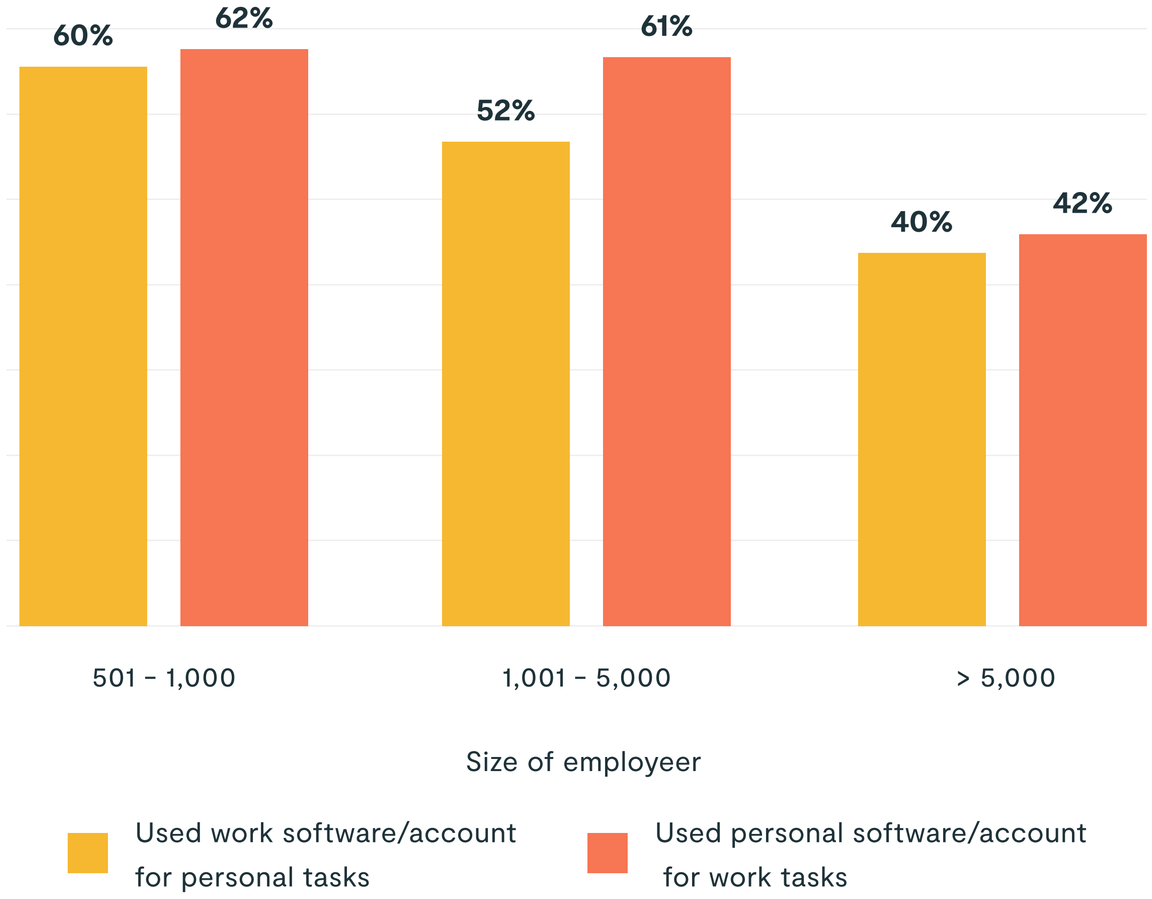
The antidote to insider threats is a strong security policy, training, and robust tools to detect and respond to incidents. Employees should be empowered to take responsibility for security issues and have the software tools to support them.

Employees are less likely to follow safe data practices when working from home

Safe data practices include keeping work and personal data separate. However, about half of remote employees mix work and personal software and accounts, and the direction went both ways – 53% of respondents had used personal software or accounts for work tasks, and 47% of respondents had used work software or accounts for personal tasks. These unsafe data practices introduce the risk of exposing corporate data outside of the work environment.

In addition, remote workers at medium-sized organizations were more likely to mix work and personal software or accounts than those in very large-sized organizations — about 60% of the former compared to 40% of the latter.

Percentage of remote workers mixing work and personal software/accounts



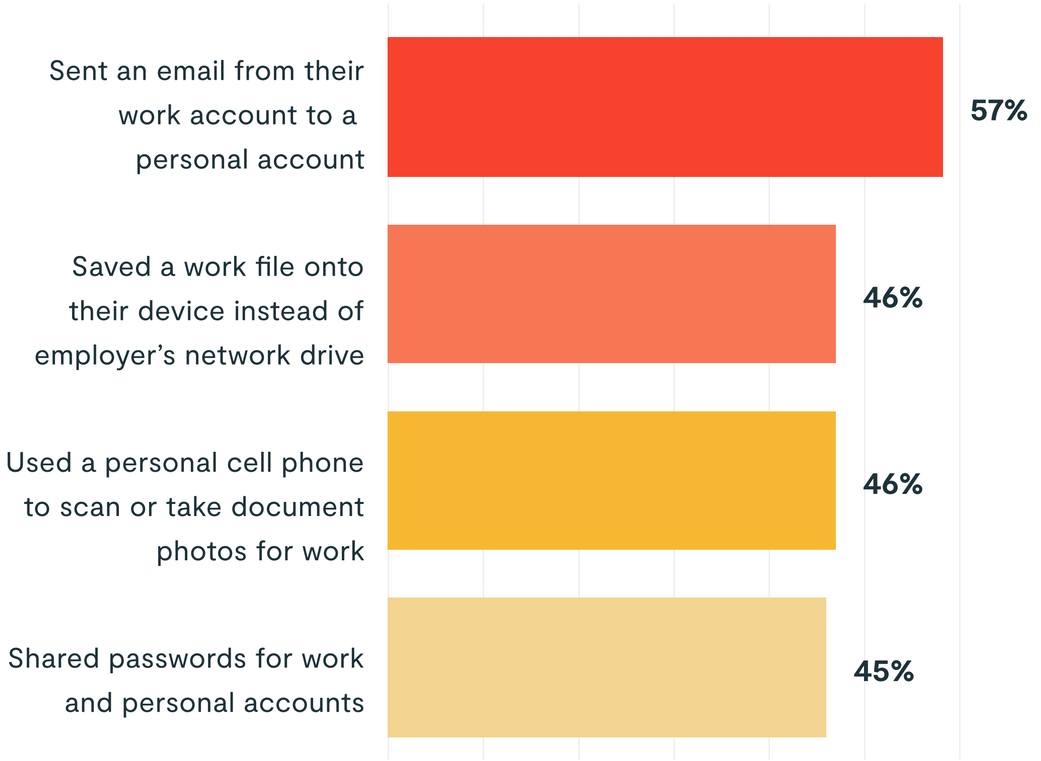
Employees are breaking safe data practices out of convenience

Some of the most common unsafe data practices are sending emails from a work account to a personal account, saving a work file outside the employer's network, and using the same password for both work and personal accounts. Nearly six in 10 respondents admitted to having sent an email from their work account to their personal account out of convenience, leading to a possible data loss incident or breach.

Almost half of respondents have saved a work file onto a personal device instead of their employer's network drive — whether it's directly saving a file or using a personal cell phone to scan or take photos of work documents.

Moreover, 45% of respondents use the same password for work and personal accounts. Reusing passwords exposes all of one's accounts to cybercriminals if any single account gets hacked. This practice increases the risk of identity theft, stolen money, and the loss of sensitive information from work.

Percentage of remote workers breaking safe data practices out of convenience



How to stay safe while working remotely

The majority of employees working remotely are using personal devices and networks that IT does not control. What can organizations do to stay safe?

Start by implementing consistent policies across the board. These policies should carry forward to principles of zero trust, which can be applied to any user and any data that they try to access, including those using BYOD mobile devices. Continuous validation of users and data is critical — especially as attackers get more discreet about compromising employee credentials. Deviation from baseline behavior should be an immediate reason to have a user reauthenticate, and one of the most obvious deviations is when they access data they shouldn't be accessing.

In addition to policies, organizations should be able to protect any device or user from phishing attacks — including mobile devices. Attackers have set their sights on compromising employee credentials through mobile devices because users can be vulnerable to social engineering across a myriad of apps. In the context of hybrid work, when employees constantly move between work and personal tasks on their mobile devices, then protecting against mobile phishing is a critical first line of defense.

Advanced context-aware data protection is essential to every organization. Based on who is trying to access data, where they're accessing it from, or what device they're accessing it on, an organization's security solution should be able to allow, limit, or deny access to that data. Doing so minimizes the risk of compliance violations, data leakage, and unauthorized access to sensitive data.

At Lookout, we make it as simple as possible for IT and security leaders to secure their data, regardless of whether their employees use corporate or personal devices to access it. With an endpoint-to-cloud platform, we have the ability to detect and mitigate threats such as phishing and data exfiltration. We also continuously monitor the risk levels of users and endpoints so that sensitive data is protected.

Lookout, Inc. is the endpoint to cloud security company purpose-built for the intersection of enterprise and personal data. We safeguard data across devices, apps, networks and clouds through our unified, cloud-native security platform — a solution that's as fluid and flexible as the modern digital world. By giving organizations and individuals greater control over their data, we enable them to unleash its value and thrive. Lookout is trusted by enterprises of all sizes, government agencies and millions of consumers to protect sensitive data, enabling them to live, work and connect — freely and safely.

LOOKOUT.COM

Learn More About Lookout.

What to learn more about how Lookout can protect your remote employees and keep your corporate data safe?

REQUEST A DEMO ->

More Insights, Every Week.

Latest news, threat info, and security updates from the leaders in cloud security.

- Cyber Threats
- Tips for Enterprises
- Industry News

READ MORE->

Appendix

[1] 2023 Zippia: 25 Trending Remote Work Statistics

[2] 2020 EU Horizon Magazine: Teleworking is Here to Stay

[3] 2023 Euronews: Want to Work From Home?

[4] 2023 Zippia: Amazing Cloud Adoption Statistics

[5] 2022 Inc.com: Microsoft Finds That Remote Staff Work More

[6] 2020 Forbes: Is A Blurred Work Life Balance the New Normal?

[7] 2022 IBM Cyber Security Intelligence Index Report

[8] 500 or more employees

About the Report

In January 2023, Lookout surveyed 3,000 remote and hybrid workers from large enterprises [8] in the United States, United Kingdom, France, and Germany. Nationally-representative samples for each country were used, with 750 respondents per country.

Most remote workers were hybrid workers, comprising 72% of all remote workers surveyed. The remaining 28% of respondents were fully remote.

Lookout

About Lookout

Lookout, Inc. is the endpoint to cloud security company purpose-built for the intersection of enterprise and personal data. We safeguard data across devices, apps, networks and clouds through our unified, cloud-native security platform — a solution that's as fluid and flexible as the modern digital world. By giving organizations and individuals greater control over their data, we enable them to unleash its value and thrive. Lookout is trusted by enterprises of all sizes, government agencies and millions of consumers to protect sensitive data, enabling them to live, work and connect — freely and safely. To learn more about the Lookout Cloud Security Platform, visit www.lookout.com and follow Lookout on our Blog, LinkedIn, and Twitter.

For more information visit
lookout.com

Request a demo at
lookout.com/request-a-demo