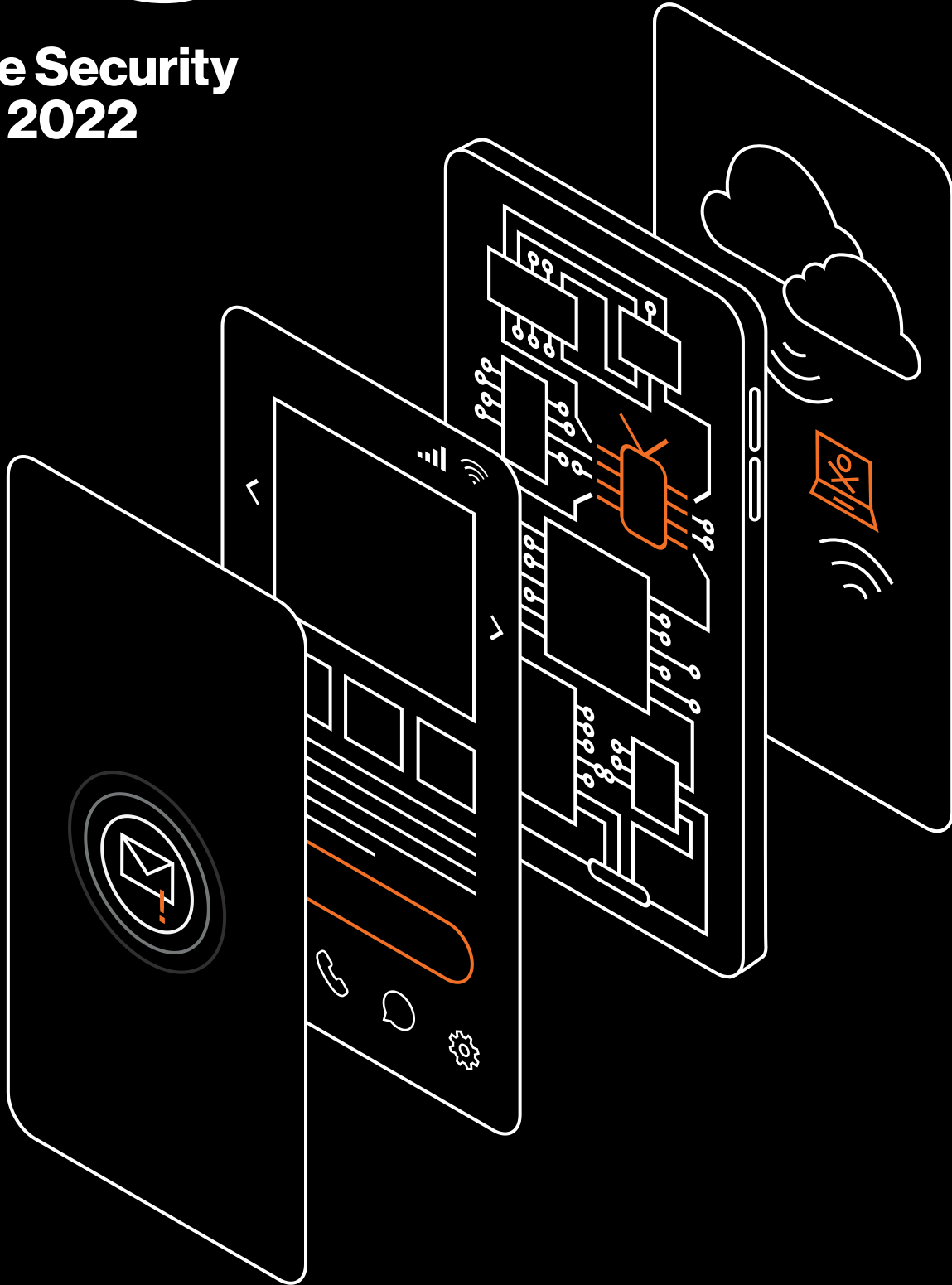


MSI

Mobile Security Index 2022



Who should read this report?

We produced this fifth annual Verizon Mobile Security Index to help security professionals, like chief information security officers (CISOs), assess their organization's mobile security environment and calibrate their defenses. While the report is packed with detail, there's also lots of information that would be interesting—and extremely relevant—to anybody involved in the specification, procurement or management of IT devices and services.

About this report

In April 2022, we commissioned an independent market research company to survey more than 600 people responsible for security strategy, policy and management. We also surveyed security practitioners and interviewed nine C-level experts in the field. And again this year we worked with several leaders in mobile device security: Absolute, Check Point, IBM, Ivanti, Jamf, Lookout, Netskope, Proofpoint and Thales. These contributors provided additional information, including incident and usage data.

We'd like to thank all our contributors for helping us to present a more complete picture of the threats that affect mobile devices and what is being done to mitigate them. This report wouldn't be possible without them.

For more information on our methodology, see page 61.

Table of contents



Foreword

Attacks are up—losses too.	4
Changing working practices is a challenge.	5
Companies are more reliant on mobile devices.	6
Security spend is rising in response.	7





1

Introduction	8
Mobile is now critical.	9
Everywhere, all the time	9
Success brings unwanted attention.	13
The severity of attacks has grown.	13
Security spend	14

2

Bring your own dangers	16
Bring your own office	17
Bring your own device (BYOD)	19
Bring your own applications	19
 How to secure BYOD devices	19
Training and acceptable use policies	21
 How to work from home, securely	23

3

Threats and defenses	24
3.1 Users and behaviors	25
Passwords	26
Phishing	28
Inappropriate content	33
The great exfiltrations	34
 How to secure against phishing	35
 How to create an effective incident reporting process	36
3.2 Apps	37
App permissions	38
Malware	39
Ransomware	40
Mobile ransomware	43
 How to secure apps	44
3.3 Devices and things	45
Lost or stolen devices	46
Device management	46
Check Point: The case for UEM	47
The dangers of things	48
 How to secure IoT devices	49
3.4 Networks and clouds	50
Public Wi-Fi	51
Home Wi-Fi	52

4

Zero Trust	55
Zero Trust network access	56
A continuous Zero Trust mindset	57
Conclusion	58

5

Appendices	59
Terminology used in this report	60
Survey methodology	61
Contributors	62

Foreword

In 2021, America experienced an unprecedented increase in cyberattacks and malicious cyber activity. Normally, the legal team would never let us say something as bold as that; they'd want evidence for such a dramatic statement. But those words are verbatim from the opening of the FBI's 2021 Internet Crime Report.¹ And our research found that compromises that were known to involve a mobile device followed this trend—in fact, the growth in the number of companies affected was higher.

% Companies that suffered a mobile compromise

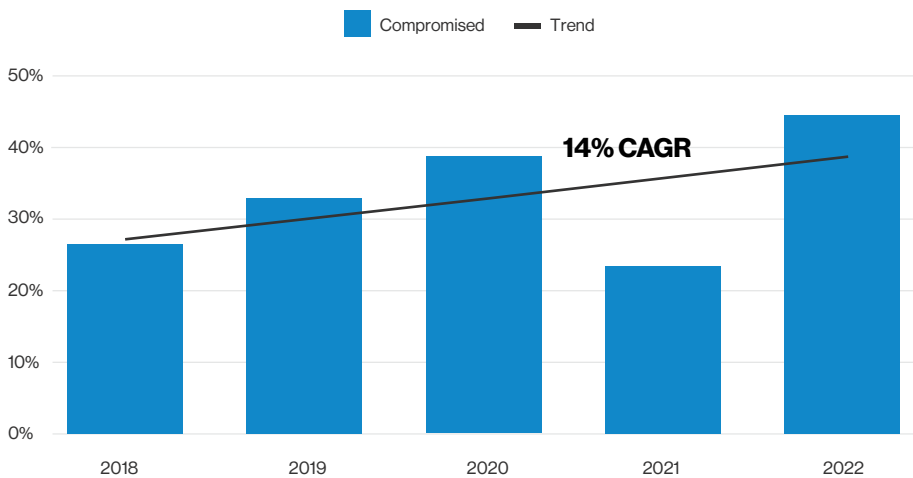


Figure 1. Percentage of respondents that admitted their company suffered a compromise that involved a mobile device and led to the loss of data or downtime.
[n=601, 671, 876, 856, 632]

In 2021, the FBI's Internet Crime Complaint Center (IC3) team received a record 847,376 complaints—a 7% increase from 2020. The estimated potential losses were over \$6.9 billion.¹ Unsurprisingly, ransomware, business email compromise (BEC) and the criminal use of cryptocurrency were among the most commonly reported types of incident.

Attacks are up—losses too.

45%

Close to half of the companies that we surveyed said they had suffered a compromise involving a mobile device in the past 12 months. Companies with a global presence were even more likely to have been affected. More than three in five (61%) had been hit, compared to 43% of organizations with only a local presence.

¹ FBI, 2021 Internet Crime Report, 2021

Changing working practices are a challenge.

According to a survey by Proofpoint, 64% of people have changed where they work. Changes driven by the pandemic have stuck. Sixty-eight percent of those surveyed have started working from home either full time or some of the time.² IT organizations did a stellar job enabling millions of people to work from home on short notice. New security approaches and tools mean that employees working from home can be just as secure as those working from the office. And managing a mix of remote, home, hybrid and office-based employees doesn't need to be any more difficult either.

But companies are still struggling. Almost four-fifths of respondents agreed that recent changes to working practices had adversely affected their organization's cybersecurity.

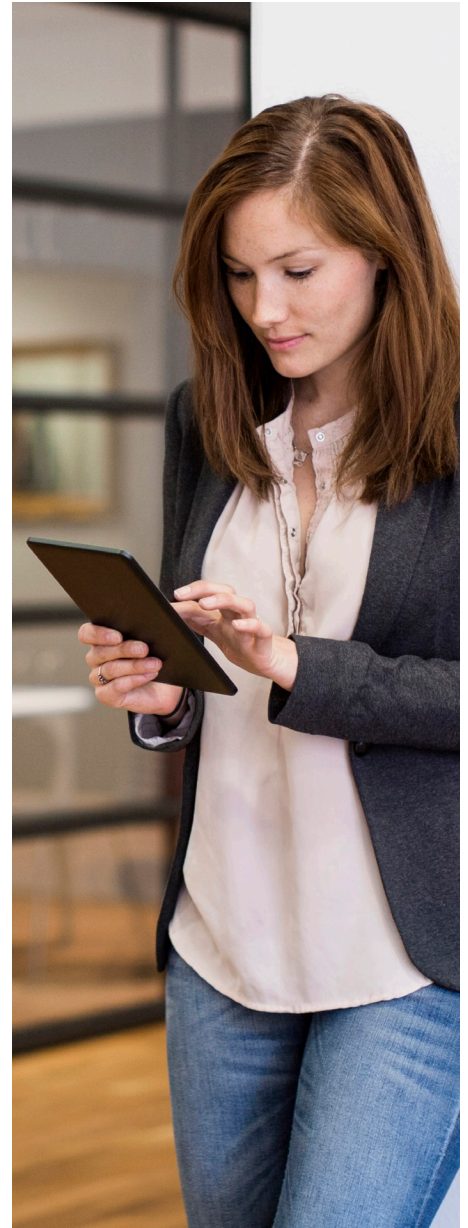
79%

Almost four-fifths of respondents agreed that recent changes to working practices had adversely affected their organization's cybersecurity.

Almost two in three CISOs across all regions agree that remote working makes their organization more vulnerable to cyberattack.

22%

Over a fifth (22%) of IT leaders in an Absolute study said that their primary reason for wanting employees to work from the office is to maintain a better corporate security posture.³



² Proofpoint, 2022 State of the Phish, 2022

³ Absolute, The Future of Work, 2022

Companies are more reliant on mobile devices.

Companies are increasingly reliant on mobile devices. This is partly driven by the shift toward more hybrid working, but there are several other factors too. For many, mobile devices are no longer a secondary device.

58%

We have more users using mobile devices than 12 months ago.

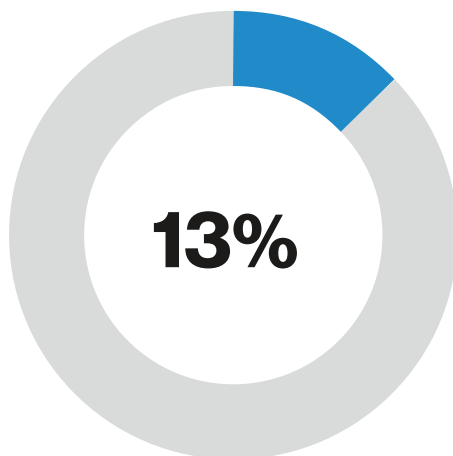
59%

Mobile users are doing more with the devices than 12 months ago.

53%

Mobile devices have access to more sensitive data than a year ago.

Many employees now have access to much of the same data—customer lists, banking details, employees' personal data, billing information, etc.—and systems—messaging, enterprise resource planning (ERP), etc.—via their mobile devices as they would sitting at a desktop in the office. This means that the compromise of a mobile device can now pose a significant risk to customer data, intellectual property and core systems.



Only one in eight respondents said they had few (less than 10% of their workforce) people working from home or following a hybrid working model.

Security spend is rising in response.

Over three-quarters (77%) of respondents said that their security spend had increased in the preceding year. More than a fifth said that it had increased significantly.

Change in security spend

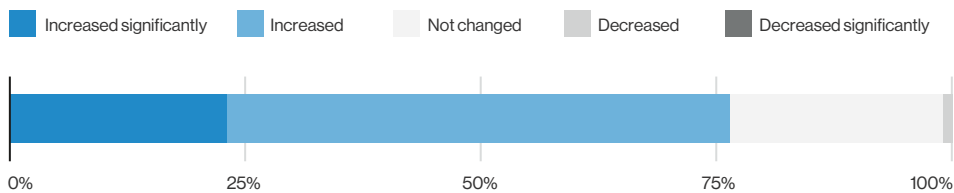


Figure 2. Year-over-year change in security spend. [n=632]

Factors driving increase in security spend

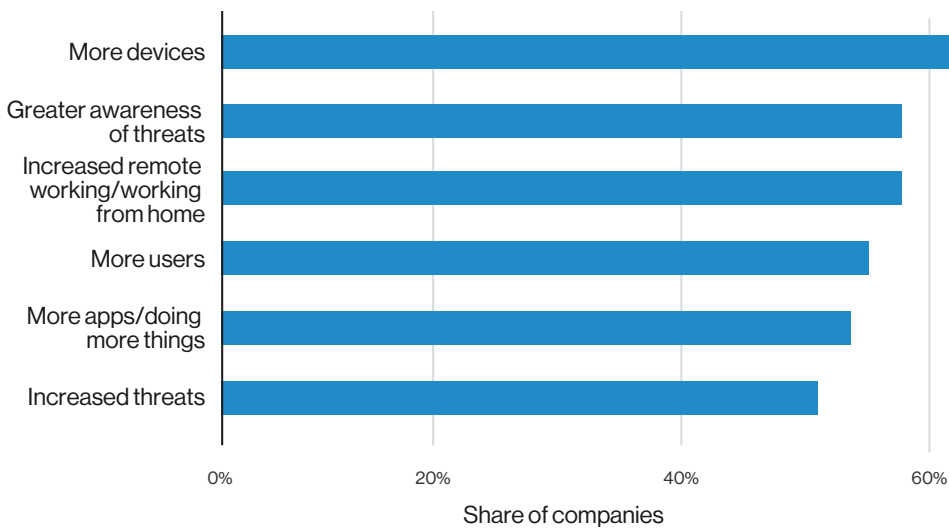
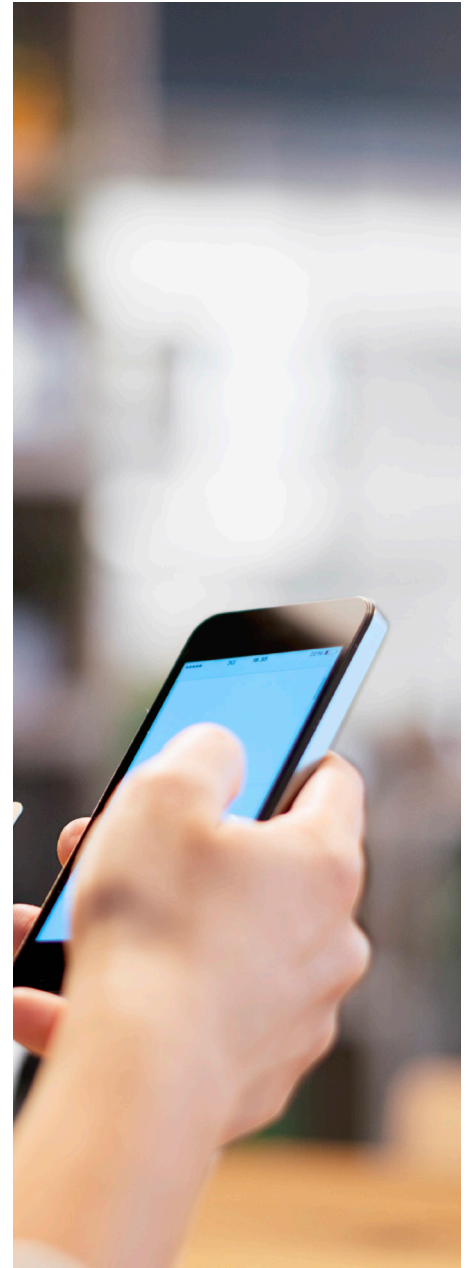


Figure 3. Factors that respondents said drove the increase in security spend that they had seen in the preceding 12 months. [n=626]



Introduction

1

Whereas traditionally technology got a foothold in the enterprise and then trickled down to consumers, it was consumers that drove the growth of what we then called smartphones. Fifteen years ago, around when the first edition of the Verizon Data Breach Investigations Report (DBIR) was being written, most home computers were large boxes with separate monitors and keyboards. These devices were pretty rudimentary compared with what we're used to today, but at the time they were game changing. Now you could have a device in your pocket that enables you to access the web, send and receive emails, and more.

Mobile is now critical.

It's worth remembering that one of the early successes in the mobile device field was BlackBerry, and specifically BlackBerry Enterprise Server. The first thing that springs to mind when most people think of BlackBerry is the physical keyboard. But looking back, what's really interesting about BlackBerry is that security was central to how it was designed.

However, BlackBerry's dominance, driven by enterprise users, was quickly overwhelmed by consumer-friendly devices from the likes of Apple. And that's when people started having better technology at home than at work. Executives around the world started putting pressure on IT teams to give them devices for work that were as user friendly as their personal devices. And it wasn't just hardware, it was apps too.

Today, few people even use the phrase "mobile phone"—unless you're well over 40, anyway—and laptops have become the norm. And it's not just the hardware that's changed, what we do with it has exploded.

Mobile devices are now critical to how we work. With increased capabilities and expansive connectivity, we now have access to far more information and tools than we ever did in the days of desktops and personal digital assistants (PDAs). Partly driven by the growth in cloud-based applications, a smaller screen no longer means less powerful.

Importance of mobile devices

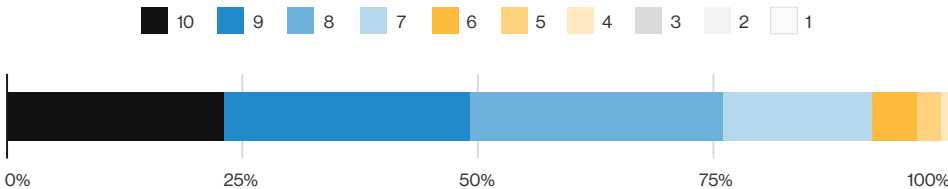


Figure 4. Responses to the question "How critical are mobile devices to the smooth running of your organization?" [n=632]

When asked how critical, on a ten-point scale, mobile devices were to the smooth running of their organization, 91% of respondents in our survey answered seven or above—and 78% answered eight or higher. The picture was very similar regardless of company operations (local, regional or global) and company size (small, medium or enterprise size). The difference was no more than two percentage points up or down.

85%

The vast majority of respondents said that flexibility in where they work and what devices they can use will be important to attracting the best new talent.

Where employees call "the office"

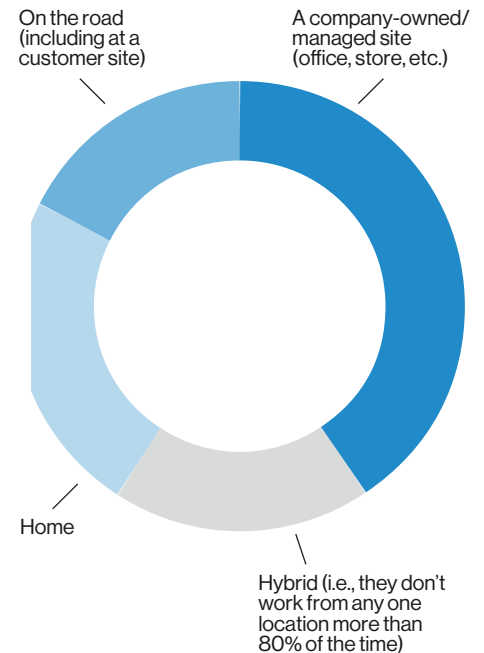


Figure 5. What proportion of your organization's staff work from each of these locations most (80% or more) of the time? [n=632]

Everywhere, all the time

Fifteen years ago when we wrote about mobility, we often talked about the new ability to work from anywhere at any time. Marketers came up with all kinds of clever phrases, like “Make work an activity, not a location.”

Obviously, the COVID-19 pandemic had a dramatic impact on working practices. But it didn’t create the trend toward more flexible working, it just accelerated it. On average, about two-fifths (40%) of employees work from the office most of the time (80% or more). About the same percentage (41%) work from home or “on the road” most of the time.

There is a downside. For many people, “any time, anywhere” has evolved into “everywhere, all the time.” Sometimes, it’s employers putting expectations on employees to be contactable outside, often way outside, working hours. In some cases, it’s employees themselves slipping into the habit of checking messages, and more, at all hours of the day. It’s easy to find ways to justify it to yourself: “This project is important,” “I’d rather know now than worry about it all night,” and countless more.

Prior to 2016, employers in France were able to dismiss employees for failing to respond to out-of-hours messages – and some did. Then the French government passed a law giving workers the right to disconnect.⁵ Since then, Ireland, Italy and Spain have enacted similar legislation. The province of Ontario is considering enacting a similar law.

Reasons for not being able to disconnect

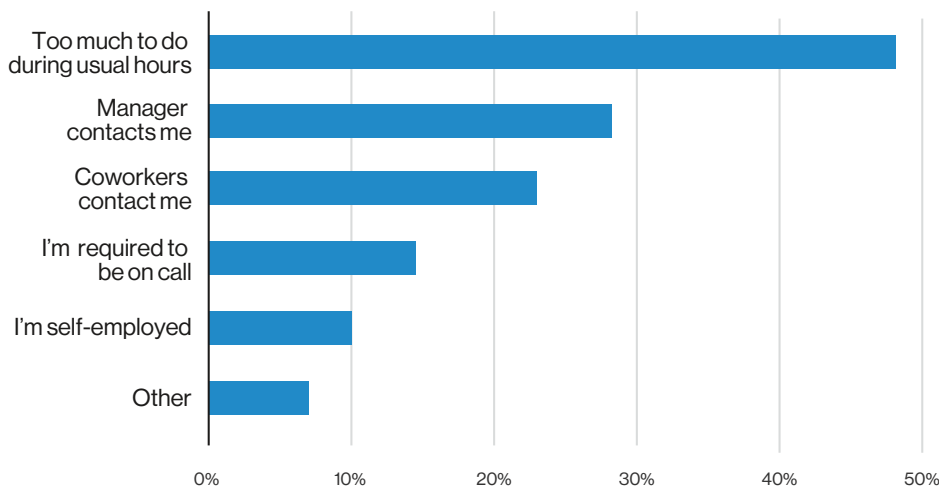


Figure 6. Reasons why employees feel unable to “disconnect” from work.⁴

4 LifeWorks, The Mental Health Index by LifeWorks, 2022

5 Légifrance, Partie législative (Articles L1 à L8331-1), 2017

6 Legislative Assembly of Ontario, Bill 27, Working for Workers Act, 2021, 2021

Assembly of Ontario: Schedule 2 Employment Standards Act 2000

The Schedule amends the Employment Standards Act, 2000. The new Part V11.01 of the Act imposes a requirement on employers that employ 25 or more employees to have a written policy with respect to disconnecting from work. The term “disconnecting from work” is defined to mean not engaging in work-related communications, including emails, telephone calls or the sending or reviewing of other messages, so as to be free from the performance of work.

Figure 7. Extract from Working for Workers Act, 2021 in the Legislative Assembly of Ontario.⁵

Working excessive hours can affect mental health. LifeWorks found that the 21% of workers who disagreed with the statement “I am typically able to disconnect from work after usual work hours” had a Mental Health Index score 4.8 points lower than those that were able to switch off.⁷

Mental Health Index over time

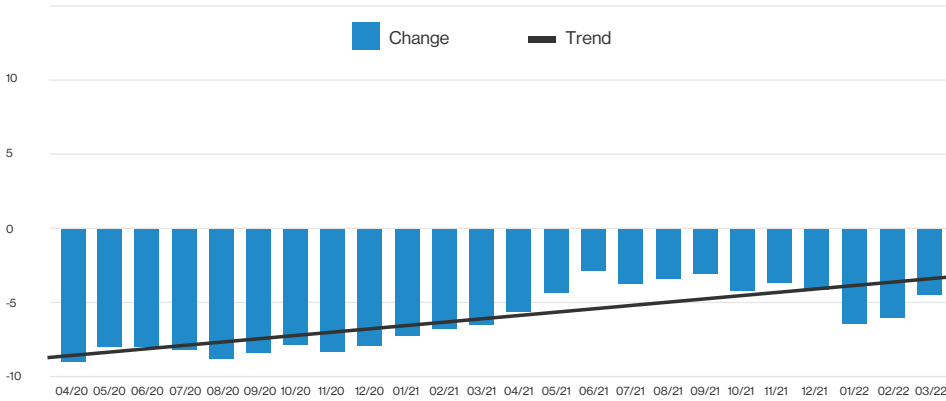


Figure 8. Global Mental Health Index score by month.⁸



^{7, 8} LifeWorks, The Mental Health Index by LifeWorks, 2022

This is more than an interesting aside; there is a direct connection with cybersecurity. In previous editions, we've discussed why mobile phones can make it harder to spot an attack like a phishing email. Tired or distracted employees are also more likely to tap on something that they shouldn't.

Imagine two scenarios:

It's mid-morning and you're sitting at your desk in the office. An email drops into your inbox. You double-click it and start reading.

You've just taken a training course about phishing, so you're a bit suspicious. But the email includes some personal information, looks professional and has no obvious giveaways like bad grammar.

What do you do?

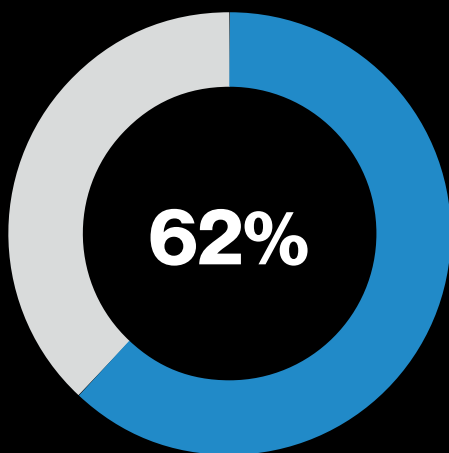
- Hover over the button and check the actual URL in the status bar
- Expand the message header and check the sender's address
- Close the email and decide to review later
- Flag the email as spam/suspicious
- Click the button

It's late. You've been out for the evening and had a couple of beers. You're in a cab on your way home when your phone buzzes in your pocket. You tap on the notification and the email opens up.

You've just taken a training course about phishing, so you're a bit suspicious. But the email includes some personal information, looks professional and has no obvious giveaways like bad grammar.

What do you do?

- Close the email and decide to review later
- Flag the email as spam/suspicious
- Click the button



Nearly two-thirds of cyberattacks attributed to insiders were assessed to be due to negligence rather than malicious intent.⁹

⁹ Ponemon, 2020 Ponemon Cost of Insider Threats Global Report, 2020

Success brings unwanted attention.

Now that mobile is so critical to business operations, it's getting more attention from bad actors too. From coordinated state-sponsored campaigns to unfocused, opportunistic criminal exploits, the volume of attacks is going up. Whether the attacker is a well-trained and well-resourced professional or an amateur taking advantage of the many commercially available exploits, mobile devices are an attractive target.

Growth in incidents and losses

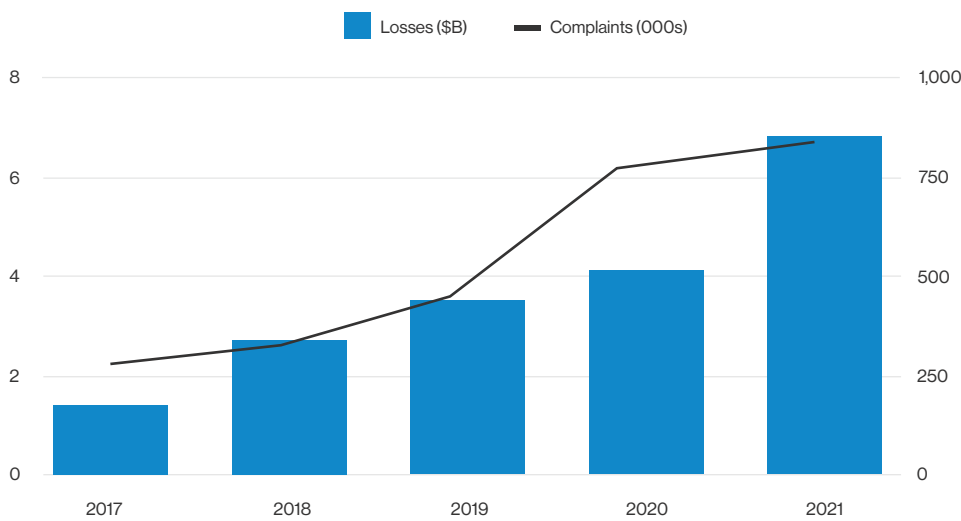


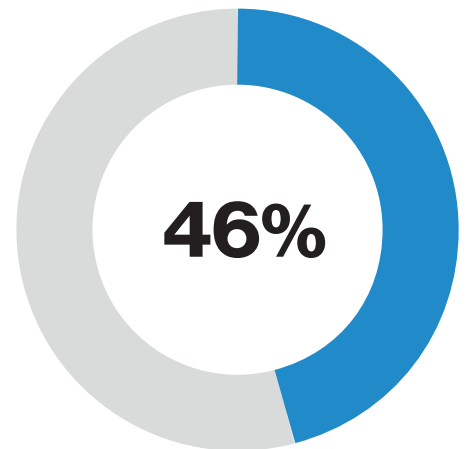
Figure 9. Reported incidents and losses, based on FBI data.¹⁰

Despite this, we still get respondents saying that mobile devices are of less interest to cybercriminals than other IT assets—36% in our latest survey, up from 30% in our 2021 report.

The severity of attacks has grown.

As mentioned earlier, 45% of respondents said that their organization had been subject to a security incident involving a mobile device that led to data loss, downtime or other negative outcome.

Of those respondents, 73% described the impact of the attack as major, and over two-fifths (42%) said that it had lasting repercussions. That's up from our previous report, where less than half of incidents were described as major, and just 28% were said to have had lasting repercussions.



Nearly half of SMBs that had suffered a mobile-related compromise said that the impact was major and that it had lasting repercussions.

¹⁰ FBI, 2021 Internet Crime Report, 2021

However, the 2021 data was a bit of an anomaly—wonder why? This year’s severity figures show a return to the level we’ve seen since we started producing the Mobile Security Index, just a little higher. Of course, with a lot more respondents saying that their company had experienced a mobile-related compromise, this means a lot more companies are facing major, and lasting, consequences.

Prevalence and severity of mobile-related compromises

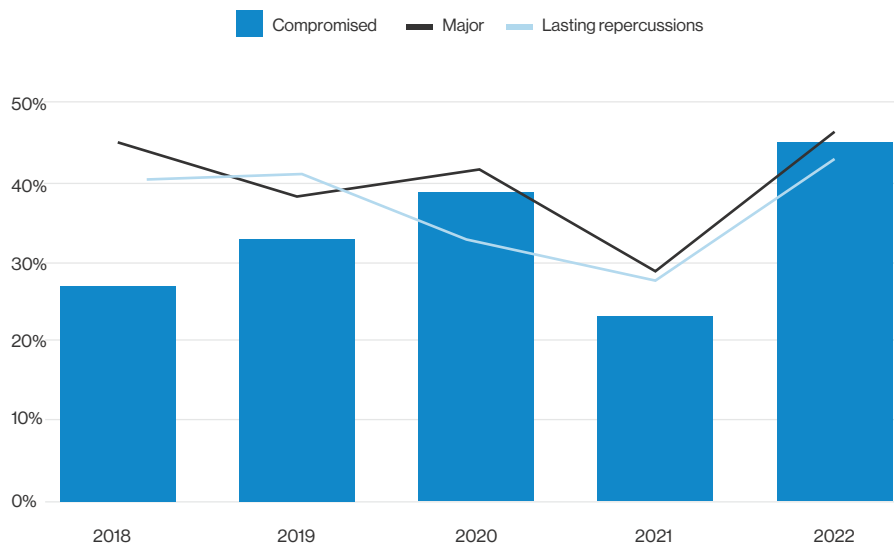
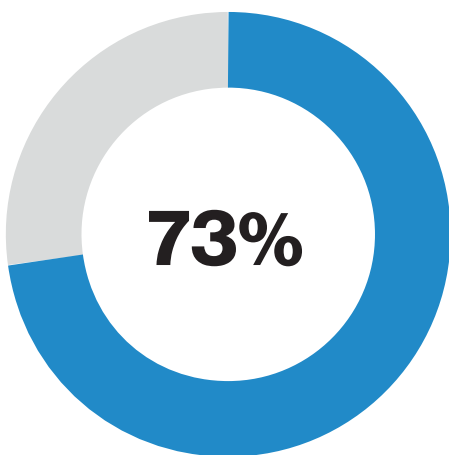


Figure 10. Prevalence and severity of mobile-related compromises. [n=601, 671, 876, 856, 632]



Nearly three-quarters of respondents from small and medium-sized businesses said that they perceived the risk as significant or high—compared to “just” 60% of those from larger organizations.

Security spend

These factors help explain why 77% of respondents said that their cybersecurity budget had increased in the previous 12 months—that’s up from 65% in the previous edition of this report—and close to a third (29%) of those said it had increased significantly.

77%

Over three-quarters of respondents said that their cybersecurity budget had increased in the previous 12 months.

And respondents expect their budgets to grow again. Over three-quarters said that they expected their budget to grow in the following 12 months; 25% said they expected it to increase significantly. Just 1% expected their budget to decrease.

77%

Over three-quarters of respondents said that they expect their cybersecurity budget to increase in the coming 12 months.

67%

Over two-thirds said that spend had increased in the previous 12 months and they expected it to rise again in the next 12 months.

Of course, growing budgets sounds like good news for CISOs, but what really matters is whether that budget is sufficient to meet needs—especially when needs are growing as we’ve discussed.

Four out of five (80%) of our respondents said that they expected their budget to be adequate to do the job.

The most common objective for security spend was increasing the security of existing user activities. That’s not as obvious a statement as it might seem at first glance. With so many new hybrid workers and the continuous stream of new applications and capabilities, you might expect that the focus would be on securing new things, but apparently a lot of companies know that they have much to do to secure existing activities.

In the past, companies focused their spend on Protect activities, as defined by the National Institute of Standards and Technology (NIST) Cybersecurity Framework. But our research found that companies are now spending more evenly across the five NIST categories. This is a very encouraging sign.

Factors driving increase in security spend

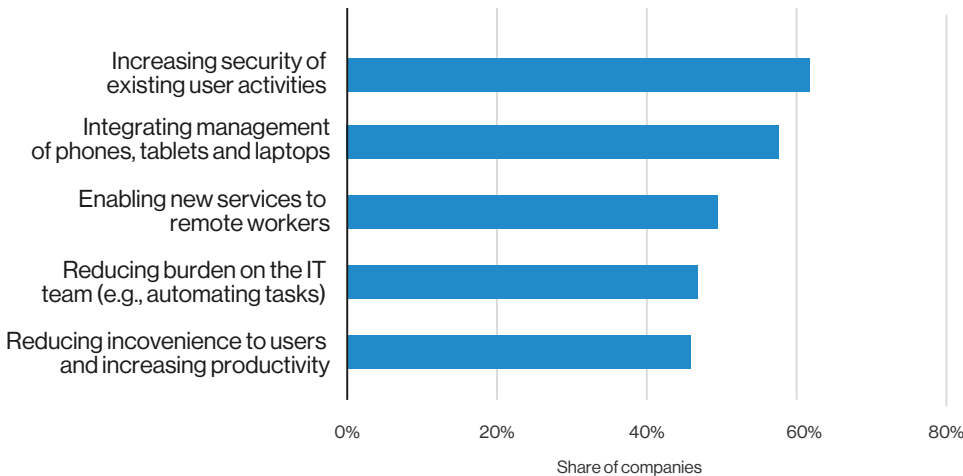


Figure 11. Objectives for cybersecurity spend. [n=632]

Spend by NIST category

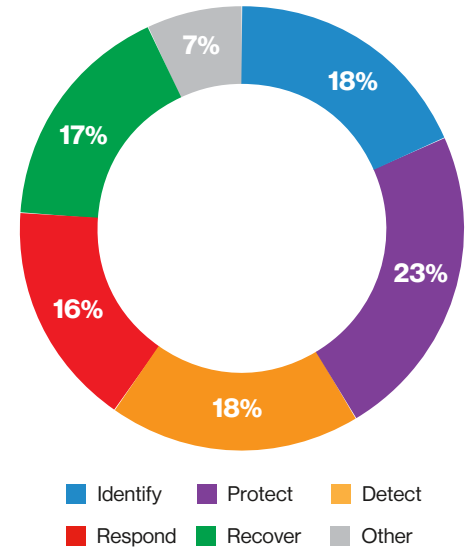


Figure 12. Respondents' estimated breakdown of security spend by NIST category. [n=226]

40%

According to a report by Thales, two-fifths of organizations are not confident that their current security systems could effectively secure remote work.¹¹

67%

Over two-thirds of respondents agreed that companies only take cybersecurity seriously enough after they have been compromised.

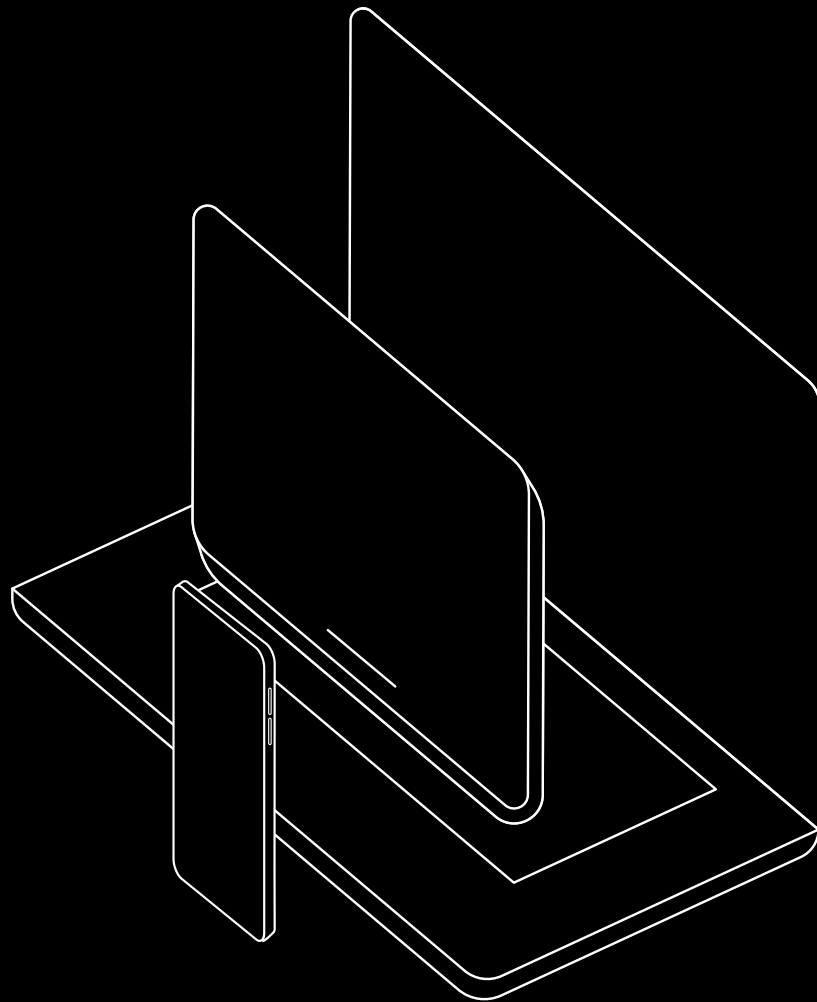
85%

The vast majority of companies said that they have a defined budget for mobile security.

¹¹ Thales, 2022 Thales Data Threat Report, 2022

Bring your own dangers.

2



Working patterns were changing long before we all learned what a coronavirus is. But the COVID-19 crisis catalyzed dramatic changes in expectations, for both employers and employees. These new behaviors have brought new challenges and threats with them.

Bring your own office.

Biggest challenges to managing risk and compliance under “work from anywhere” policy

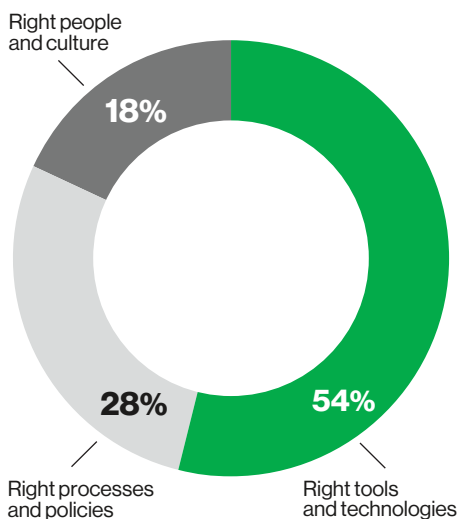


Figure 13. Challenges to managing risk and compliance. Data from Absolute.¹³

79%

According to Thales, nearly four in five organizations are still “somewhat” or “very concerned” about the security risks and threats that a greatly increased remote workforce poses.¹⁴

Challenges to managing risk and compliance

How many times have you seen a “look what I just received” post on LinkedIn? Somebody has just started a new job and received a new laptop, monitor and bunch of logo’d swag – typically including a water bottle and a mousepad. That’s what onboarding has looked like for a lot of people over the last couple of years.

As working from home has become more commonplace, people have invested in building a more comfortable place to work. There’s been a boom in loft and garage conversions, or if you’re really lucky maybe you splashed out on a “shed quarters” at the bottom of the garden.

Over half of CISOs across all regions agree that targeted attacks on their organizations have increased since adopting mass hybrid working. Small organizations seem more affected, with 59% of companies with 500 or fewer employees saying their workforce has been targeted more since they implemented hybrid working. At the other end of the scale, only 48% of enterprises (5,000 employees and above) agree.¹²

Many of you reading this report will be seasoned remote workers. But recent events have created millions of new home and hybrid workers. Despite this, many companies haven’t provided employees with clear guidance on what’s expected.

¹² Proofpoint, 2022 Voice of the CISO, 2022

¹³ Absolute, The Future of Work, 2022

¹⁴ Thales, 2022 Thales Data Threat Report, 2022

Bring your own device (BYOD).

The number of companies that said that they allow employees to use their own devices dropped since the previous edition of this report. But in that report, over half of the 70% of companies with a BYOD policy said that they'd adopted it during lockdown. It seems likely that some will have done so only as a temporary measure and rescinded it because it didn't suit their company culture, caused security problems or proved to be unpopular.

Securing BYOD devices can be considerably more difficult than securing company-owned ones with a mobile device management (MDM) solution in place. Rigorous policies and thorough enforcement will be required. See our discussion of Zero Trust approaches on page 56.

One challenge of securing BYOD devices is getting users to follow company policy on a device that they see as their property. Employees that receive a stipend may be more willing to countenance their employer setting rules about how they use devices and intrusions to their privacy. Over two-thirds (68%) of the respondents to our survey whose company had a BYOD program said that this included such a payment.

Bring your own applications.

It's not just devices that people bring into the business. News reports have brought to light incidents of officials—both in the U.S. and the U.K.—using encrypted messaging apps like WhatsApp and Telegram to carry out government business. And it's not just in the public sector. It's been reported that major organizations have let people go for using unauthorized messaging apps. In 2021, one of these, a major bank, was fined \$200 million for insufficient monitoring and record keeping associated with employees using unapproved messaging apps.

No matter what security measures you put in place, you can't stop an employee using an app like this on a personal device to conduct business conversations. And if they do, it's a lot harder, even impossible, to spot phishing attacks and sensitive data being sent outside the company. It could also have serious compliance implications.

This underlines the importance of making sure that security measures aren't too intrusive and that users understand why they are in place. The more draconian and arbitrary security measures seem, the more likely users are to try and find ways around them.

60%

Allow employees to access email on their own phones/tablets.

A further 31% are considering doing so.

41%

Allow employees to use their own phones/tablets to access corporate systems and data (BYOD).

A further 41% are considering doing so.

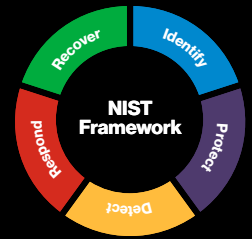
50%

Allow employees to use their own laptops for work-related tasks (bring your own PC, or BYOPC).

A further 35% are considering doing so.

Figure 14. BYOD policies, current and under consideration. [n=623]

How to secure BYOD devices



These recommendations are structured around the five functions in the NIST Cybersecurity Framework.

To find out more, visit nist.gov/cyberframework

Identify

Develop a detailed BYOD policy that clearly lists responsibilities in plain language – this may involve translating it into local languages.

Protect

Educate users on the importance of managing the permissions granted to apps – users often aren't aware of how some permissions can be exploited for nefarious purposes.

Implement an MDM solution to help remotely secure, manage and support personally owned devices.

Consider restricting what resources devices not controlled by the company can access.

Ensure that users understand the importance of keeping the operating system (OS) and apps up to date.

Educate users on the dangers of malware and how to reduce the risks – malware can obviate protections like containerization.

Consider implementing a Zero Trust approach; this can reduce the reliance on end users making informed and security-conscious decisions – see page 56 for more details.

Detect

Consider introducing endpoint detection and response (EDR); this uses behavioral-based analysis to provide threat protection and can provide valuable insight.

Consider implementing data loss prevention (DLP) to detect and block the exfiltration of information.

Give users an authorized – and easy-to-use – means to share files outside the company.

Respond

Make sure that your team has the training – or the third-party support – to handle greater device variety.

Make sure that staff know what to do if a device is lost or stolen, or they spot something suspicious – this should be part of your general security policy, but it's worth reiterating here.

Make reporting concerns easy – it shouldn't be something people have to look up – and remember, the employee might not be able to access company systems when reporting an issue.

Recover

Use mobile threat defense (MTD) combined with unified endpoint management (UEM) to help bring devices that are out of compliance back into line through self-remediation.

Develop a clear policy, in consultation with your legal team, that covers the tricky issues around performing digital forensics on an employee-owned device.

Work profiles

Non-remote workers

Employees that work inside a company-controlled environment, the perimeter, like an office, store or plant.

Back office

Commuters

Office-bound:

This includes a wide range of workers, from call center staff to lawyers. They might be required to work from the office or choose to do so—not everybody likes or has the right conditions to work from home. These workers typically rely on a local area network (LAN) or wireless LAN (WLAN) within the perimeter. They might work from home a few times a month.

Front of house

Tethered

Floor workers:

This category includes many roles in retail, hospitality, manufacturing, etc. These workers aren't fixed to a desk, but their location doesn't change much. They are more likely to use a specialized device. They will rarely use a network not controlled by the company.

Corridor warriors:

Employees that are never at their desks, but their roaming is mainly limited to one of the company's sites. They primarily use the company's WLAN.

Remote workers

Employees that operate outside the perimeter, whether on the road or at home.

Omniworkers

Home workers:

People based at home or who work from home a lot. This label can apply to a wide variety of roles. They typically use home Wi-Fi, perhaps with a virtual private network (VPN).

Flexible workers:

Employees that work from home a few days a week—there are all kinds of reasons why. They commonly use home Wi-Fi, perhaps with a VPN.



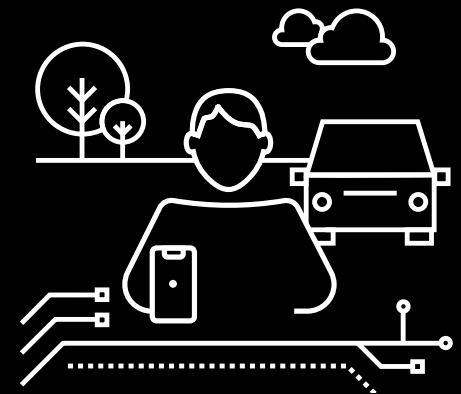
Nomads

Road warriors:

These are the classic “remote workers:” sales people, consultants, CxOs of big companies, etc. They need to be able to work from multiple locations and work on the move. They have complex requirements and use multiple types of networks. They are likely to need to use third-party Wi-Fi and cellular connectivity.

Field workers:

Another well-established category. It includes roles like service engineers. People in this group often need to use custom apps and work on the move—so cellular connectivity is key. Their primary device may be a customized or ruggedized device.



Training and acceptable use policies

Lack of clarity on expectations

Some behavior is clearly unacceptable, such as accessing adult, extreme or illegal content on company devices. This could not only damage your organization's reputation, this type of behavior could put your company at risk. But there are many gray areas in defining appropriate use, especially when it comes to mobile devices. What if employees want to use their work devices to check personal emails, stream music or scroll through social media? Many people think this is a reasonable allowance in a flexible, modern workplace.

Personal tasks carried out on work devices

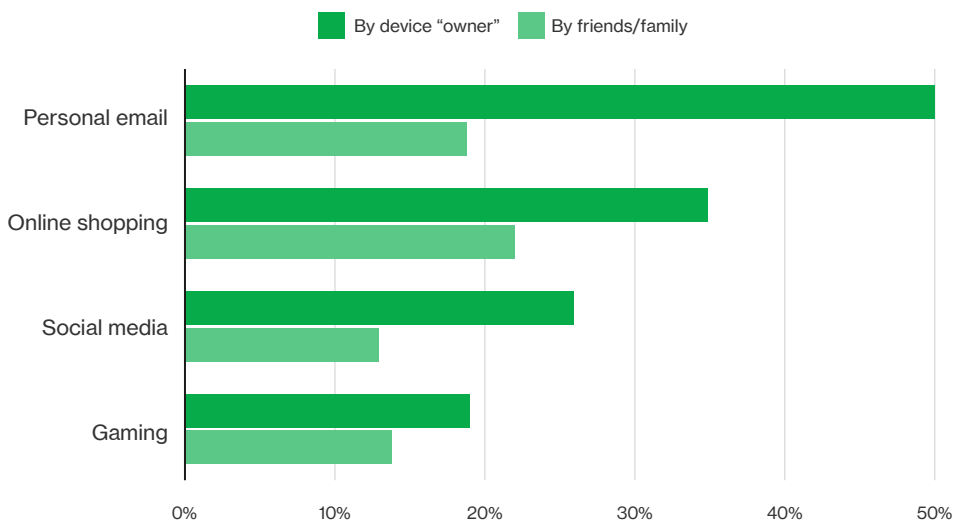


Figure 15. Personal tasks carried out on work devices, by user and user's friends/family. Data from Proofpoint.¹⁵

Part of the problem is that many companies struggle to develop an effective acceptable use policy (AUP) – 48% didn't have one at all, an improvement from 57% in our last report. Defining what counts as misuse of a work device can be tricky, especially if your employees need to access social media and other content to do their jobs, but creating clear guidance, including rules for mobile-specific content, is crucial for helping prevent misuse.

Plus, with many employees now working from home, the lines are blurred even further.

79%

Nearly four-fifths (79%) of people admitted to using a work device for a personal task, such as checking personal email, shopping or streaming.¹⁶

48%

Nearly half of respondents said their organization didn't have an acceptable use policy in place.

^{15, 16} Proofpoint, 2022 State of the Phish, 2022

Lack of training

Many companies set high expectations on their employees but don't give them sufficient training to meet those standards.

44%

Don't give employees security training on a regular basis.

51%

Don't give employees security training when their working arrangements change (e.g., start working from home).

Lack of remote working guidance

We've seen a massive shift in working practices—even if only temporary for some people—yet less than half of companies said that they have given employees training on how that affects cybersecurity.

64%

We have guidelines on what are suitable locations for remote working (e.g., home is okay, coffee shop isn't).

47%

We issue guidance on maintaining privacy when working remotely (e.g., when working in a shared apartment).

It's not our place to say how companies should manage abuse, but we advocate creating a positive security culture. Creating a blame-free environment is likely to encourage employees to report suspicious activity and mistakes that they may make—enabling the organization to mitigate the damage.

How to work from home, securely

A guide for users

Reduce risky behavior.

Read and understand your company's policies. Ask for further guidance on anything you're unsure about.

Try to keep your private and work life separate.

Consider where you keep work devices and any sensitive data—are these stored safely when not in use?

Make sure that you've set a password or PIN—or enabled Touch ID where applicable—for access.

Configure your devices to lock automatically after a few minutes of inactivity.

Create a unique strong password for each account, including email and web applications

Turn on two-factor authentication wherever possible.

Think about who can see or hear what you are saying or typing on your screen.

Sign up to newsletters from trusted organizations to improve your cybersecurity skills and knowledge.

Manage your apps.

Be careful what apps you install on your devices, especially when those devices have access to corporate resources.

Make sure you understand your company's AUP and any other restrictions that may be in place.

Install updates promptly—it can be a bother, but failing to do so could put your device, and the company, at risk.

Be frugal with which permissions you give apps. Consult company policies on what to limit on which apps.

Secure your devices.

Don't share devices—you may be allowed to perform personal tasks, but that doesn't apply to your friends and family.

As with apps, install OS updates when asked to do so.

If you lose a device, or it gets stolen—these things happen—report it immediately.

Be smart about networks.

Change the default password on your home router—and any smart home devices connected to it.

Set up separate Wi-Fi networks for smart home devices, visitors and work use—many wireless access points include this functionality in the admin console.

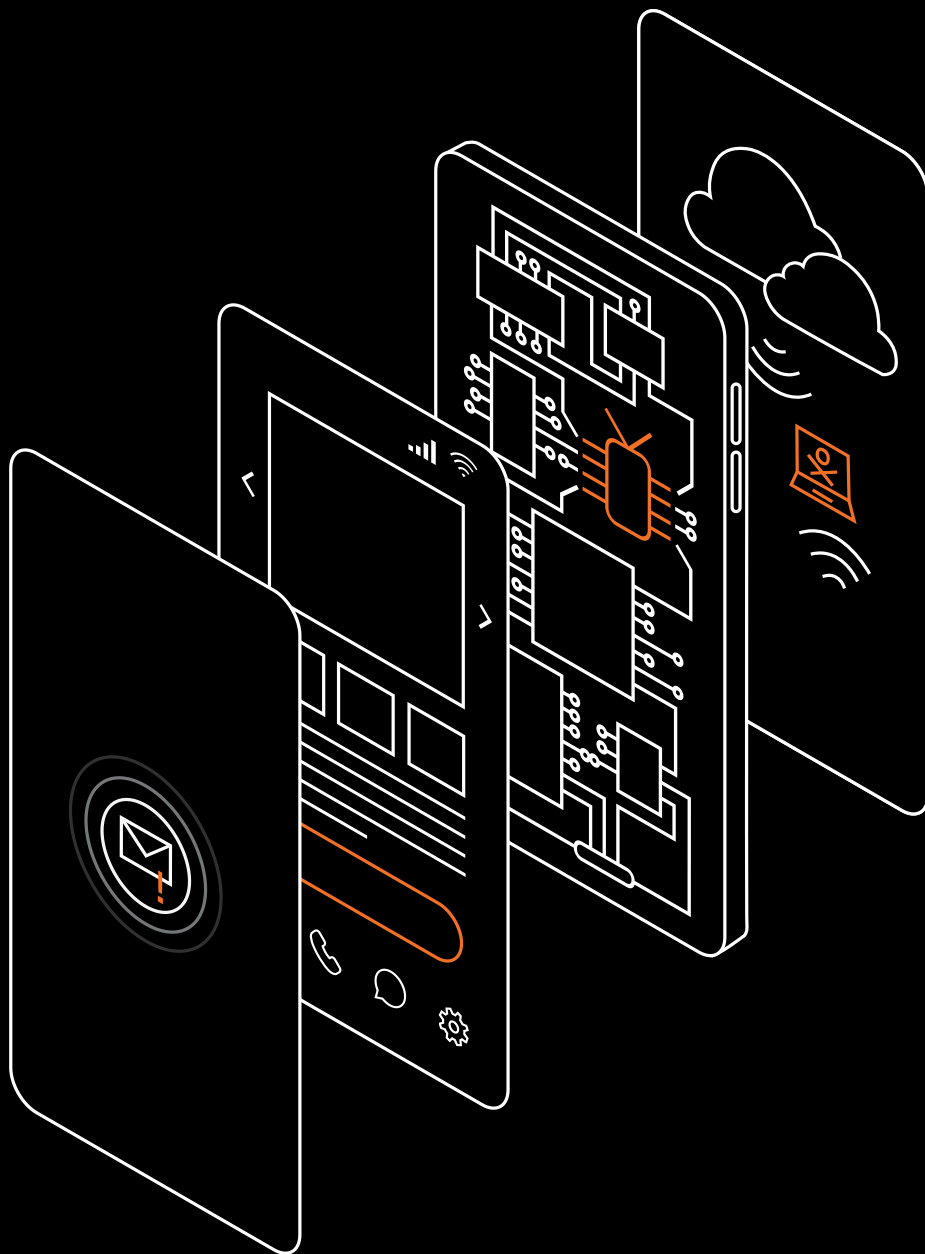
If your company provides a VPN, use it.

Be wary of public Wi-Fi networks—even ones associated with brands you know and trust.



Threats and defenses

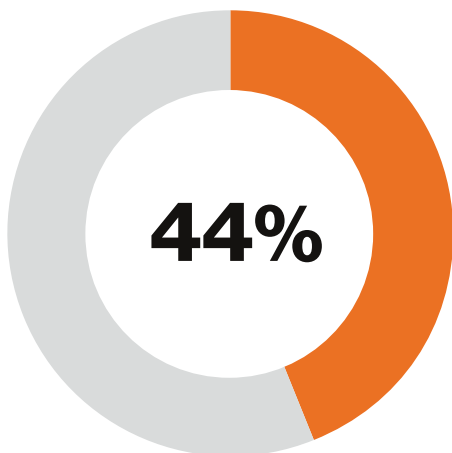
3



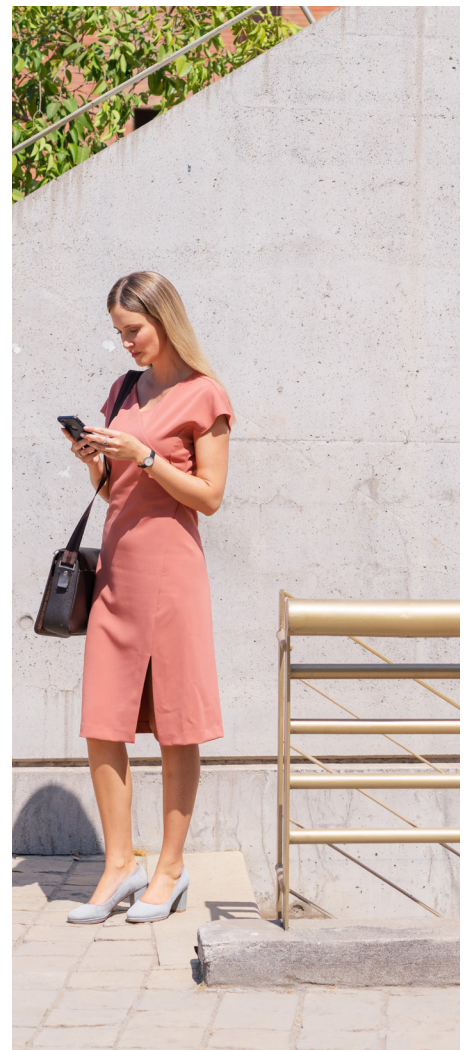
3.1 Users and behaviors

Whether they're deliberately breaking policy or inadvertently opening up vulnerabilities, users are a threat. Social engineering remains one of the most powerful tools in the cybercriminal's arsenal. And attackers are finding increasingly innovative ways to exploit and manipulate users.

The human element continues to drive breaches. Over four-fifths (82%) of breaches analyzed for the 2022 DBIR involved the human element. Whether it is the use of stolen credentials, phishing, misuse or simply an error, people continue to play a very large role in incidents and breaches alike.¹⁷



Over two-fifths (44%) of those that had suffered a mobile-related security breach said that user behavior was a contributing factor. Those in the manufacturing sector were most likely to list this as a factor, 57%.



¹⁷ Verizon, Data Breach Investigations Report, 2022

Passwords

Yup, passwords again. Despite the thousands of articles about the importance of passwords, the sad fact is that many attackers don't hack into systems. They log in. And users make it easy for them.

Long, complex passwords can be a pain on a device with a keyboard, even more so on a small screen with a virtual keyboard—and don't get us started on trying to enter a strong password on a smart TV! But it's critically important as attackers have many tools and techniques at their disposal.

Attackers exploit a range of social and technical vulnerabilities to steal or crack credentials:

They guess:

Publicly available information such as name, date of birth and relatives' names provide a head start.

They trick people into revealing them:

Social engineering, including phishing and old-fashioned scamming, can be very effective.

They “credential stuff:”

This involves using usernames and passwords leaked from data breaches on other sites; this exploits people's tendency to reuse passwords.

They “password spray:”

This involves simply trying some of the most commonly used passwords across a huge number of sites.

They use “brute force:”

This is automated guessing, but the easy availability of large amounts of computing power and techniques honed over many years make it a more powerful technique than you might think.

They “shoulder surf:”

Which is exactly what it sounds like—it might also include reading the sticky notes stuck around a monitor.

They exploit network vulnerabilities:

This can enable them to intercept passwords when users log in.

They use a keylogger:

This enables them to capture a record of every keypress a user makes.

These and other techniques are widely documented on the web—you can even download tools to help.

The sad fact is that many attackers don't hack into systems. They log in.

For years, vendors have foretold the imminent demise of passwords, but each year it seems like we need more passwords rather than fewer. Password managers and alternatives like fingerprint scanning can help, but for the foreseeable future it's important to make sure that employees understand what makes a strong password.

Remember that poor password practices at home can be a threat to the business. If a user uses the same password across multiple accounts, this could increase the risk of a successful credential stuffing attack.

Authentication is a fundamental component of a Zero Trust approach to mobile device security; see page 56.

What makes a password strong? LUCID.

We, security professionals that is, often talk about password strength, but how many users actually know what that means?

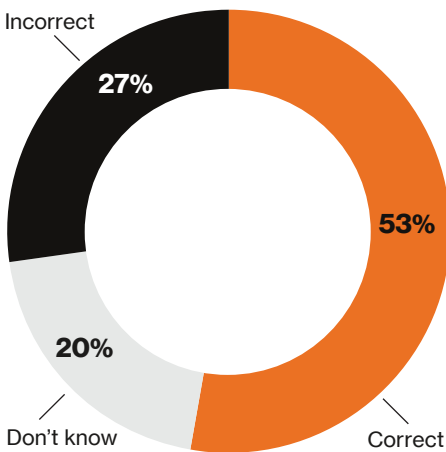
Long	With passwords, it's all about entropy, and length is one of the key components. A simple (mix of upper- and lowercase letters) 8-character password would take about 22 minutes to crack; a 12-character one, 300 years.
Unique	Don't reuse passwords. We can't stress this enough. Password stuffing is popular with hackers because it works.
Complex	Complexity is the other component of entropy. Throw a "special character" into that 12-character password and the time to crack leaps to 400,000 years.
Impersonal	Brute-force attacks can be smarter than they sound. Hackers can use social engineering to make more educated guesses. That's why it's a bad idea to include any personal information in a password. A password with the same entropy as "Cassie%12032005" would take 5,000,000,000 years to crack, but it would be a lot easier for a hacker that read about your daughter Cassandra's birthday on Facebook.
Different	Yes, that's the same as unique, but it's that important a point.

Phishing

Another old “favorite.” We’ve been writing this report for five years and phishing has been a major topic every year. Our colleagues who create the Verizon DBIR have been covering the rise of phishing attacks for 15 years.

Despite the prevalence of phishing attacks over many years, a large number of employees are unable to correctly define the term. As we’ve discussed in previous editions of this report, email is not the only place where we see phishing attacks, and attackers continue to innovate, so let’s start by getting our definitions straight.

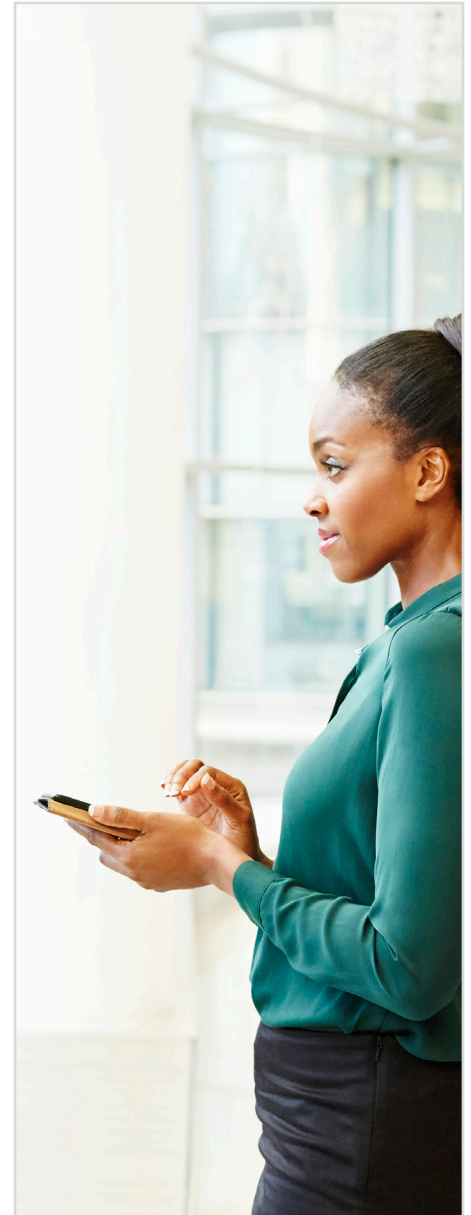
Users’ understanding of “phishing”



83%

In 2021, five out of six organizations experienced a successful email-based phishing attack in which a user was tricked into risky action, such as clicking a bad link, downloading malware, providing credentials or executing a wire transfer. That’s a huge increase from 2020, when the number was “just” 46%.¹⁹

Figure 16. Share of working adults able to correctly define “phishing.”¹⁸



18, 19 Proofpoint, 2022 State of the Phish, 2022

Types of phishing

Name	Description	Means	Scale	Common intent
Bulk phishing	The most familiar type of phishing, commonly used in both business and consumer environments. Research from Proofpoint shows that many major brands are seen in bulk phishing attacks.	Email, in-game chat, etc.	Big, unfocused. It's all about the numbers. Success rates are low, but send out enough messages and somebody will click or tap.	Get the target to click on a link, either to capture credentials or get additional biographical information or payment details.
Smishing	Similar to bulk phishing, but using text messages. A common recent example is the "You have a parcel" message.	SMS		
Vishing	Many, though not all, users have learned to be suspicious of emails. But a phone call must be legit, right? It's still relatively rare, but deepfake technology has been used to go a step further and actually impersonate key individuals. As artificial intelligence/machine learning (AI/ML) becomes more accessible, this may increase.	Phone calls or voice messages	Small, targeted – for now. The nature of these attacks is often like bulk phishing, but they are labor-intensive, so they are often focused on high-value targets, making them more like whaling attacks.	Get the target to visit a website through which malware is then deployed, give information over the phone or allow the attacker to take over control of the device – the "support scam" is a common version of this.
Spear phishing	Spear phishing is to organically fed, free-range chicken as bulk phishing is to factory farming. Instead of going for the widest audience possible, attackers focus on a specific company and tailor the approach to increase the chances of success.	Email	Small, targeted.	Sometimes part of a concerted information-gathering campaign to help gain access to accounts, often a direct attack with the goal of financial enrichment.
Whaling	Also called business email compromise (BEC), whaling targets high-level employees. The difference between whaling and spear phishing is that whaling exclusively targets those in the highest echelons of the organization.	Email		

\$2.4 B

According to the FBI, BEC schemes in the U.S. resulted in 19,954 complaints in 2021, with losses estimated at nearly \$2.4 billion. The amount of money lost through BEC scams continues to grow, with identified global exposed losses increasing 65% between July 2019 and December 2021.²⁰

²⁰ FBI, 2021 Internet Crime Report, 2021

A little learning can be a dangerous thing.

We often talk about the need for users to be more alert, wise to “obvious” signs of attacks. This is probably most common when it comes to phishing. Surely users can spot a phishing email—they are all full of typos, have bad grammar and fit into a standard pattern, like “Your account has been compromised” or “You’ve been chosen to receive millions.”

But what about the opposite hypothesis? In the U.K., there was a series of campaigns aimed at teaching children about the dangers of strangers. There were TV ads, lessons in school and more. Some years later, it was discovered that all this effort had an unintended consequence. It had made kids confident that they could spot a dangerous stranger: They looked like the one in the ads—a man in a gray trench coat with a bag of sweets. The problem with that was it left many thinking that anybody not meeting that specific model wasn’t a threat—surely a woman wasn’t dangerous?

Is the same happening with phishing awareness? Are users falling into a false sense of security? Phishing attacks come in many forms; attackers are constantly adapting their technique. And, as we discussed in the previous edition of this report, perpetrators are very quick to respond to current events, like COVID-19.

It’s important to teach users that not only do attacks come via different channels, they can take many different forms. A reasonably informed user would be suspicious of a message from a Nigerian prince, regardless of whether it came by email, SMS or Facebook. But what about a message about a parcel held up waiting additional address information—especially if they were waiting for a parcel or it was around their birthday or other gift-giving occasion? And what about a “fun” quiz that involves answering questions about your childhood and favorite things?

Going back to our opening discussion, mobile phones have broken down the barriers. We don’t separate work and leisure the way that we used to. What if instead of your regular social media site, it was a business-related message, and it asked about the city where you went to school, what your first job was, etc.? And what if it arrived after a long day, maybe as you were enjoying a beer and watching TV?



**I wish more people did these.
It’s fun to learn odd little things:**

First job - **Stop**

Current job - **Sending**

Dream job - **Your**

Favorite food - **Potential**

Favorite dog - **Passwords**

Favorite footwear - **Or**

Favorite chocolate bar - **Memorable**

Favorite ice cream - **Data**

Your vehicle color - **To**

Favorite holiday - **People**

Night owl or earlybird - **Who**

Favorite day of the week - **Collect**

Tattoos - **This**

Favorite color - **For**

Do you like vegetables - **Social**

Do you wear glasses - **Engineering**

18%

**of clicked phishing emails
come from a mobile device.²¹**

²¹ Verizon 2022 Data Breach Investigations Report. [verizon.com/dbir](https://www.verizon.com/dbir)

Complacency can be dangerous.

Right now you might be thinking “what idiots,” but not everybody is a cybersecurity specialist and most of us like to think that most people are pretty decent. A lot also think that the people who do understand security are so far ahead of them that they must be able to outwit the bad guys. Nearly half of respondents in a Proofpoint study said that they thought their organization’s safety measures would prevent any dangerous emails getting as far as their inbox.

49%

Nearly half of global users thought that their organization’s safety measures would prevent any dangerous emails from getting through to their inbox.²²

Phishing and mobile devices

Attackers will take advantage of any opportunity to make their phishing attacks more successful. The design of apps on mobile devices can, unintentionally, make phishing harder to detect, helping attackers to get past people’s normal defenses.

Cybercriminals have become adept at designing campaigns to take advantage of the nature of mobile devices and users facing numerous distractions.

43%

More than two-fifths thought that their personal email provider would stop any dangerous emails getting through to their account.²³

53%

More than half of people encountered an unsafe link while using a mobile device during the third quarter of 2021.²⁴

Why phishing campaigns are harder to spot on mobile devices

- The smaller screen and aspects of user-interface design make it harder to evaluate the legitimacy of an email or website:
 - The URL is truncated and hard to read
 - The URL disappears on scrolling to make room for more content
 - You can’t hover over a link to check the destination before tapping
- Users are more likely to check email on a mobile device when on the move, surrounded by distractions

“Attackers continue to produce ever more convincing phishing sites and increasingly target mobile users. Our research shows that as many as one in ten mobile users click on the links in phishing emails.”

–Michael Covington, Ph.D.,
VP Portfolio Strategy, Jamf

22, 23 Proofpoint, 2022 State of the Phish, 2022

24 Lookout, Predictions 2022: Five Threats That Will Impact Your Personal Data and Privacy, 2022

Zimperium conducted an analysis of more than 500,000 phishing websites over a two-and-a-half-year period. It found that the share of sites that specifically targeted mobile devices and delivered content tailored for the mobile format rose from just under half in the first quarter of 2019 to over three-quarters during the last quarter of 2021.²⁵

Phishing sites specifically designed for mobile

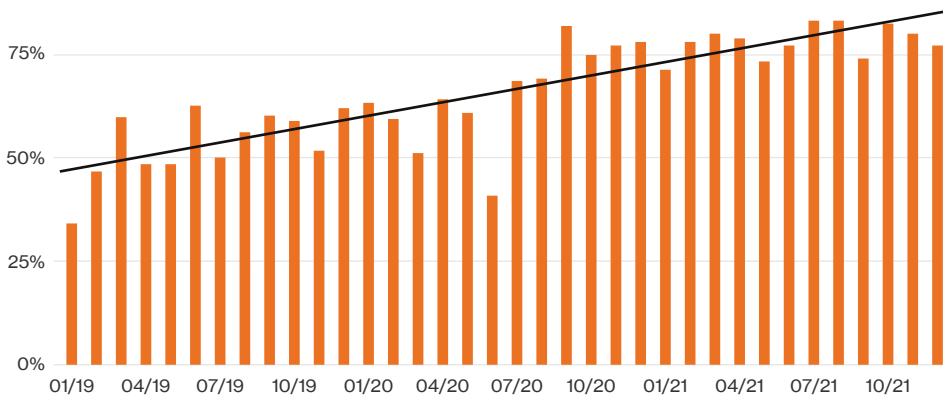


Figure 17. Share of phishing sites specifically designed for mobile.²⁶

Why does phishing remain so prevalent? Because it works. Despite the proliferation of attacks and increased awareness, research suggests that the success rate of phishing campaigns is going up.

Increase in effectiveness of phishing



Figure 18. Change in success of phishing attacks over a 12-month period. Data provided by Jamf.²⁷

25, 26 Zimperium, 2022 Global Mobile Threat Report, 2022
 27 Jamf, data provided, May 2022

Inappropriate content

It might seem hard to believe that anybody would watch porn during the working day, but it happens. We know because there have been highly publicized cases, including a well-known journalist and a member of the U.K. Parliament. In the latter case, at least one incident was in a shared space. A couple of anecdotes don't mean much, but the data shows that it's not an uncommon problem.

Increased working from home could actually be responsible for accessing inappropriate content becoming a bigger problem. Devoid of the constant presence of others, employees may visit websites that they wouldn't when in the office. Maybe not adult content, but what about gaming or gambling sites? Or other non-work-related sites, such as social media or online shopping?

Are adult websites more dangerous?

It might be awkward to talk about, but porn exists. And it's popular. There are two adult websites in the top 10 by visitor count. They get billions of visitors each month – far more than sites like netflix.com. But surely that's all outside of office hours? Wrong, Pornhub reports a peak in traffic around 4 PM each day.²⁸

We were unable to find any evidence that adult sites were any more likely to be infected or exploited to spread malware, but there are a couple of factors that could make these sites more of a risk.

Firstly, users may be more willing to hand over personal information – perhaps for age verification – than they would on, say, a news site. This could be exploited for social engineering. But, far more worryingly, it's reasonable to assume that users would be much less likely to report that their device is suffering adverse effects after visiting adult sites.

Most visited websites

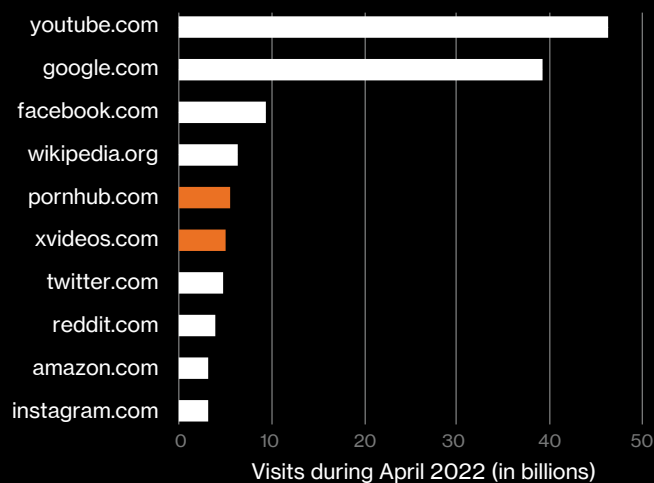


Figure 19. Most popular websites by number of visitors.²⁹

28 Pornhub, 2021 Year in Review, 2021

29 Semrush, Most Visited Websites by Traffic in the world for all categories, April 2022, 2022

The great exfiltration

Much has been written about the “great resignation.”³⁰ There’s much debate about whether it’s a real phenomenon, and which age groups and industries are affected. While it may not be the global exodus that some have suggested, some companies have definitely seen a spike in exits.

What’s that got to do with mobile security? Well, according to research by Lookout, when leaving a job, about one in six employees uses a personal instance of a cloud storage app to take company data with them.³¹

Netskope studied departing employees and found that between 2020 and 2021, 29% of them downloaded more files from managed corporate app instances and 15% of users uploaded more files to personal app instances in their final 30 days than usual. Of the users who uploaded more files, half uploaded more than 5x the normal volume, 8% uploaded 100x more and 1% uploaded 1,000x more.³²

Mobile devices, working from home and cloud-based apps can all make this easier. This underscores the importance of having good reporting and monitoring tools. A data-loss prevention tool could also help to prevent this.

16%

When leaving a job, about one in six employees uses a personal instance of a cloud storage app to take company data with them.³³

Increase in data uploaded in 30 days prior to leaving the company

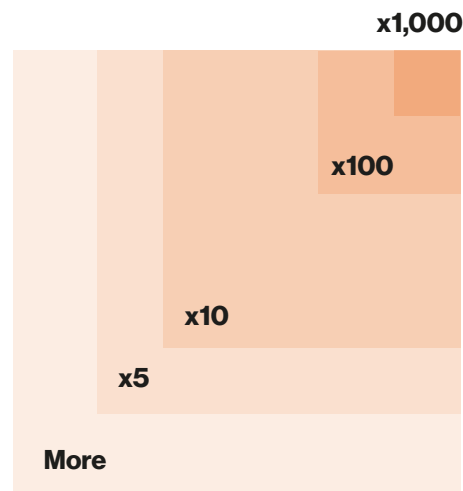
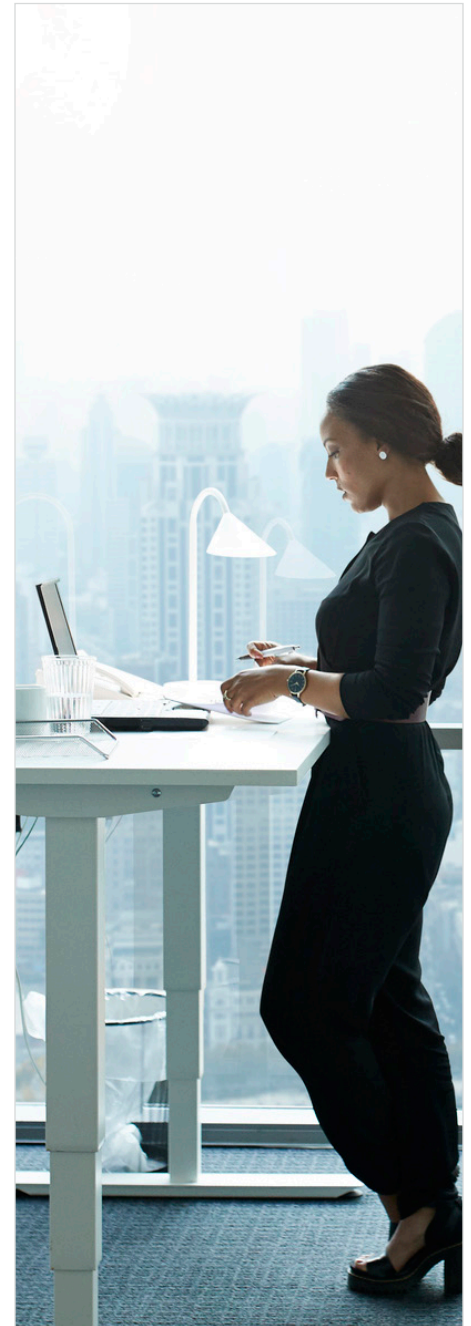


Figure 20. Increase in volume of data uploaded to a personal cloud service in the 30 days prior to leaving the company. Data provided by Netskope³⁴

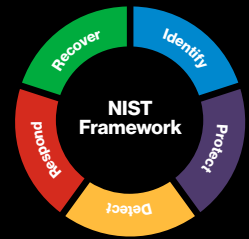


30 Bloomberg, How to Quit Your Job in the Great Post-Pandemic Resignation Boom, 2021

31 Lookout, data supplied, May 2022

32, 33, 34 Netskope, Cloud and Threat Report - January 2022 Edition, 2022

How to secure against phishing



These recommendations are structured around the five functions in the NIST Cybersecurity Framework. To find out more, visit nist.gov/cyberframework.

Identify

Identify the very attacked people (VAPs) in your organization – these aren't always the VIPs – and provide them with additional awareness training.

Carry out “real world” attack simulations that mimic the sort of interactions employees have regularly.

Protect

Carry out regular employee training and attack simulations so that employees, especially VAPs, know the signs and how to avoid becoming the weakest point.

Make sure that your phishing training and simulations aren't limited to email.

Implement controls to verify requests for changes in account information – this could be as simple as sending a confirmation message before changes come into force.

Use a web isolation solution to restrict suspicious and unverified URLs to a protected container, like a sandbox – consider using this to isolate personal activity, like shopping and checking personal email, too.

Detect

Implement a solution that blocks inbound email threats before they reach employees' inboxes.

Use an MTD solution to help detect and block phishing attempts however they are instigated.

Set devices to allow full email addresses and URLs to be viewed.

Configure your mail system to flag emails from outside your domain – many companies add a prefix, like [E], to the subject line.

Respond

Create an incident response (IR) plan – 44% of respondents to our survey, down from 51% in 2021, said their organization didn't have one.

Take a copy of the email (complete with headers) and ensure that all logs are retained.

Search email logs to identify everybody that may have received the message and notify them.

Where necessary, terminate live sessions, lock accounts and force password changes.

Update your email filters to block similar messages in the future.

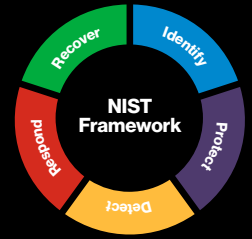
Recover

Show employees examples of actual attacks the company has faced to show that the danger is real.

Remind employees about their obligation to read and follow the company's acceptable use policy.

Use MTD and UEM to help bring non-compliant devices back into line through self-remediation.

How to create an effective incident reporting process



Penalizing employees for security mistakes is now quite common. For example, according to a Proofpoint study, more than half (55%) of organizations “discipline or punish” employees that fall for phishing emails—including ones sent by the company as part of a simulation. A further 18% were considering implementing such a policy. That number was even higher in the U.K. (77% + 15%) and Australia (78% + 6%).³⁵

Consequences ranged from mandatory training or a meeting with the infosec team all the way up to termination.

Users should not be worried about reporting potential security issues. By creating an easy, blame-free way to report incidents, you can make employees become part of your early warning system against cyberattacks.

This can help:

- Foster a companywide commitment to tackling cybercrime and fraud
- Limit the severity of compromises—the sooner an attack is spotted, the more you can do to mitigate it
- Maintain regulatory compliance—timeliness is increasingly part of security frameworks and regulations such as ISO27001, DPA 2018 and GDPR

Follow these four steps to create an effective incident reporting process.

1. Make it easy.

To be effective, an incident reporting system should be easy to use. That means making it easy to access—remember the employee may not have access to their email account, intranet, etc., that might be part of what they need to report.

It’s important to capture enough details to enable the infosec team to take action, but keep it simple for the user. Avoid jargon and complex terminology.

2. Define multiple workflows.

Different types of incidents will need different responses. An incident reporting system should allow multiple escalation paths and then route incident reports to the correct path based on type, severity, location and other relevant factors.

Ideally, these paths should be easy to configure so that administrators can keep them up to date as new threats emerge and organizational changes happen.

3. Leverage automation.

Automated systems that send alerts to the right people can help speed response and mitigate the damage caused by an incident. This doesn’t have to be a big and complex project. You could do it using a Google Form.

4. Create an audit trail.

Obviously, the primary purpose of an incident reporting process is to enable employees to report incidents and action those reports. But the information gathered as part of this process can be invaluable to later forensic analysis. It’s important to record everything that you can: What was reported, when and by whom. Consider using existing tools to record the progress of a report. Though not specifically designed for the purpose, applications like Jira and Slack are easy to use, record a journal of activity and enable you to set up automated notifications.

Penalties for security mistakes

60%

Meeting with manager or infosec team

52%

Negative mark on performance review

45%

Disciplinary action, such as a written warning

31%

Monetary penalty

15%

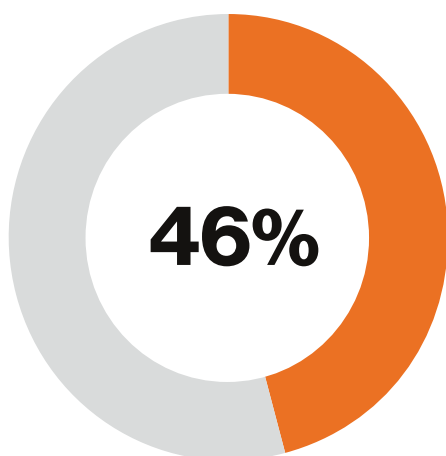
Termination

Figure 21. Penalties for falling for a phishing email, real or simulated, reported by respondents. Data from Proofpoint.³⁶

35, 36 Proofpoint, 2022 State of the Phish, 2022

3.2 Apps

The number of apps, especially web-based apps, continues to grow apace. Malware remains a major problem, but even non-malicious apps, including those downloaded from official stores, can be a threat.



Nearly half of those that had suffered a mobile-related security breach said that app threats were a contributing factor. Those in the energy and utilities sector were most likely to list this as a factor, 55%.

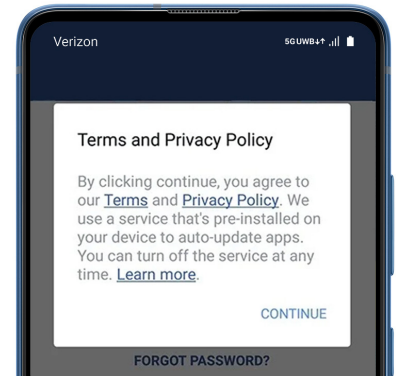


App permissions

Hands up, who has ever read the terms and conditions when making a purchase or installing an app on a mobile device? We're guessing that there aren't many hands up right now.

As we've discussed in previous editions of this report, giving applications access to the camera, microphone, photos, location data and other data and device functions can be a significant security risk.

It's very easy to just click accept, but users should be careful about applications requesting permissions that they don't really need. For example, according to Jamf research, 53% of finance applications request permission to access location data. Only 62% of navigation apps ask for the same access!



Percentage of apps per category requesting specific iOS permissions

Photos	66%	78%	69%	63%	65%	79%	71%	49%	68%	53%	50%	62%	96%	75%	87%	84%	67%	52%	65%
Camera	60%	75%	54%	54%	58%	74%	56%	44%	68%	39%	48%	43%	90%	70%	83%	83%	54%	52%	61%
Location	58%	63%	42%	57%	53%	81%	61%	43%	66%	46%	62%	61%	68%	47%	81%	72%	64%	60%	55%
Microphone	34%	44%	40%	40%	24%	32%	15%	19%	36%	41%	21%	41%	64%	44%	33%	69%	21%	20%	38%
Calendar	29%	28%	22%	38%	18%	31%	56%	23%	31%	36%	27%	31%	18%	23%	26%	35%	41%	33%	25%
Contacts	27%	37%	19%	20%	36%	46%	9%	15%	31%	13%	22%	21%	44%	37%	37%	59%	20%	27%	26%
Bluetooth	25%	26%	21%	39%	17%	42%	18%	23%	29%	35%	22%	25%	31%	22%	25%	26%	31%	20%	26%
Voice processing	9%	14%	15%	3%	9%	10%	2%	7%	8%	7%	6%	3%	8%	12%	13%	18%	5%	7%	9%
Health	2%	1%	1%	1%	1%	3%	2%	23%	3%	1%	1%	1%	0%	1%	1%	1%	4%	1%	1%
Local network	1%	1%	1%	1%	0%	0%	0%	0%	1%	0%	0%	0%	1%	1%	0%	2%	0%	0%	1%
	All	Business	Education	Entertainment	Finance	Food and drink	Games	Health and fitness	Lifestyle	Music	Navigation	News	Photo and video	Productivity	Shopping	Social networking	Sports	Travel	Utilities

Figure 22. Permissions requested by Apple iOS apps. Data from Jamf.³⁷

³⁷ Jamf, An Analysis of iOS App Permissions, 2021

Malware

The 2022 Verizon Data Breach Investigations Report found that over 30% of breach cases involved some form of malware.³⁸ And according to Jamf, the percentage of organizations that experienced the installation of malware on a remote device doubled in 2021, going from 3% to 6%.³⁸

Over the years, one of the problems we've faced when writing this report is a lack of mobile-specific stats on threats and compromises. In fact, that's why we started producing this report. Often, people will talk about the actions that attackers use, such as phishing, and the asset that was the eventual target, say a server, but not the device that provided the opening for the attack in the first place.

As we've shown, attackers do design phishing campaigns specifically targeting mobile devices, and they build malware specifically for mobile devices too.

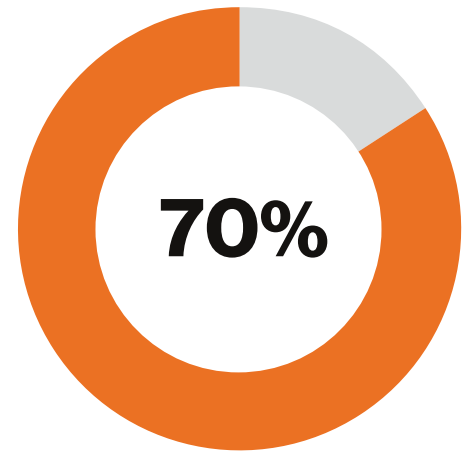
The built-in security features on some phones and the degree of control associated with using official app stores, such as Google Play, do offer some protection. But attackers manage.

Check Point Research recently tracked the development of a new form of malware. "Rogue" is a form of mobile remote access Trojan (MRAT) that can gain control over the host device and exfiltrate data such as photos, location, contacts and messages; modify the files on the device; and download other malicious payloads.

Rogue is particularly adept at digging in and avoiding removal:

- It adopts the services of the Firebase platform to disguise and masquerade as a legitimate Google service
- Once it gets all the required permissions, it hides its icon to make it harder for the user to get rid of it
- It registers itself as a device administrator; if the user tries to revoke this permission, they are presented with an "Are you sure to wipe all the data?" dialog

Malware comes in many forms, but in recent years ransomware has become the most common.



Ransomware was present in almost 70% of malware breaches analyzed for the 2022 Data Breach Investigations Report.³⁹

³⁸ Jamf, Security 360 Annual Trends Report, 2022
³⁹ Verizon, Data Breach Investigations Report, 2022

Ransomware

You must have been hiding under a rock for the last few years if you haven't heard about ransomware. It's been behind some of the most high-profile compromises in the past decade. But just in case you have been busy, here's a quick definition.

Ransomware is a form of malware that denies a user or organization access to files on their computers. Files are encrypted and a ransom demanded for the decryption key. Ransomware is no longer limited to individual machines and many attackers target servers or cloud services. Some variants have added additional functionality—such as data theft or exposure—to further incentivize victims to pay up.⁴⁰

In previous editions of this report, we have discussed some of the variants of ransomware, including doxware. We won't go over those again here, but we saw a new angle during 2021.

Several companies reported employees receiving emails soliciting them to become accomplices in a ransomware attack. The emails targeted users with access to company servers and offered a substantial return if the attack was successful.

Think you're covered? Think again.

According to the U.S. Government Accountability Office (GAO), the percentage of companies with cyber coverage increased from 26% in 2016 to 47% in 2020.⁴¹ But insurance is no panacea. As payouts have increased,⁴² insurers have tightened up policies, reduced coverage and increased premiums.⁴³ Between 20Q1 and 21Q3, renewal premiums increased more than 2.5-fold. Not only are premiums increasing, the rate at which they have increased has grown.

75%

Three-quarters of ransomware attacks start with email phishing.⁴⁴

Percentage change in renewal premiums

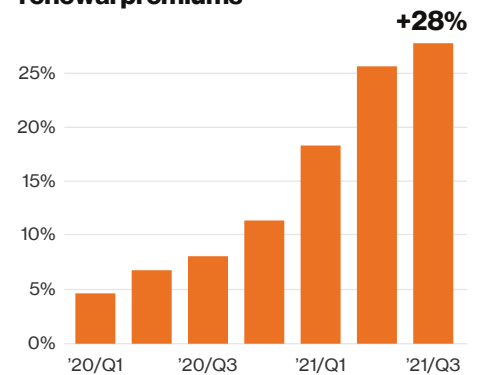


Figure 23. Increase in cyber insurance renewal premiums.⁴⁵

40 Proofpoint, Stopping Ransomware Hub, 2022

41 U.S. Government Accountability Office, Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market, 2021

42 Fitch, Sharply Rising Cyber Insurance Claims Signal Further Risk Challenges, 2021

43 ACA Group, Cyber Insurance: Top Five Trends for 2022, 2022

44 Check Point, What is Ransomware?, 2022.

45 The Council, Commercial Property Casualty Market Index: Q3/2021, 2021

To pay or not to pay?

There are several reasons why companies choose to pay the ransom:

Reduce downtime

Downtime is costly, so paying the ransom and avoiding lengthy disruption can look like an attractive option.

Protect reputation

Some people may think that paying up quickly could help keep the compromise quiet, even obviate the need to publicly admit “we’ve been hacked” and damage customer and investor confidence.

Avoid recovery costs

The ransoms stated in some of the stories that hit the headlines can be tens of millions, but they are usually a lot lower—21% of ransoms paid were under \$10,000.⁴⁶ If the costs of bringing in the experts, replacing hardware, rebuilding devices and servers, etc., are higher, doesn’t paying up make business sense?

Protect privacy

Companies don’t want their dirty linen, or their data, exposed. For some, the ransom is a more palatable loss.

But there is widespread agreement among experts that paying the ransom is a bad idea:

- The attacker won’t send the unlock code at all—this happens quite often
- The unlock code may not work—according to a Sophos study, only 4% that pay up get all their data back; the average was 61%⁴⁷
- There are technical issues with decrypting files—this has been reported by many users
- The attacker may demand a further payment or payments—sometimes this is linked to not publishing the files, an attack known as doxware

Those are the selfish reasons for not paying. There’s also a social reason. Paying up incentivizes attackers to carry out more attacks. Unfortunately, it’s a bit like when we’re faced with a traffic jam; we wish that everybody else would turn around and give us a clear road ahead.

There might soon be another reason not to pay up; it might be against the law.

64%

Nearly two-thirds of respondents in a Proofpoint study said that their organization had paid a ransom to try and resolve a ransomware incident.⁴⁸

46, 47 Sophos, The State of Ransomware 2022, 2022.

48 Verizon, Data Breach Investigations Report, 2022

Paying up may be illegal.

The U.S. government has already communicated that paying up could be contrary to existing laws intended to block the funding of groups involved in crime or terrorism.

Bills to specifically outlaw the payment of ransoms have been discussed in several countries, including the U.S. On March 15, 2022, U.S. President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) into law. It places mandatory reporting obligations in connection with cybersecurity incidents on a broad range of private and public-sector entities operating in “critical infrastructure” sectors. Companies covered by the act must report “substantial” cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours. And if they pay a ransom, they must report doing so within 24 hours. Similar laws are being considered in several other countries.

“Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC [Office of Foreign Assets Control] regulations.”⁴⁹



“The FBI does not advocate paying a ransom, in part because it does not guarantee an organization will regain access to its data. In some cases, victims who paid a ransom were never provided with decryption keys. In addition, due to flaws in the encryption algorithms of certain malware variants, victims may not be able to recover some or all of their data even with a valid decryption key.”

Paying ransoms emboldens criminals to target other organizations and provides an alluring and lucrative enterprise to other criminals. However, the FBI understands that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers.”

– FBI⁵⁰

49 U.S. Department of the Treasury, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, 2021

50 FBI, 2021 Internet Crime Report, 2021.



Hank Schless

Senior Manager, Security Solutions
Lookout

Ransomware has been a thorn in the side of cybersecurity teams for the past several years. It's not just big companies that should be concerned about ransomware; companies of all sizes in all industries have been attacked. And mobile devices are a common component of attacks.

The remote environment is primed for ransomware.

As organizations continue to support remote or hybrid work, they no longer have the visibility and control they once had inside their perimeter. Attackers are exploiting this weakness and profiting. Here are three reasons they're able to do so:

- Most organizations now have employees working from anywhere
- These employees expect seamless access to all resources from unmanaged and personal devices on networks outside the traditional perimeter
- This greatly reduces the visibility and control that security teams have and can make it difficult to understand risks posed by users and the devices they're working from

Mobile devices make it easier for attackers to phish credentials.

Attackers are always looking for ways into your infrastructure. Compromising an employee's credentials enables them to gain legitimate access and remain undetected. Their primary tactic for stealing credentials is to phish employees on mobile devices. Because phones, tablets, etc., are used for both work and personal tasks, employees can be targeted through multiple apps such as SMS, social media platforms and third-party messaging apps. The simplified user interfaces of a phone or tablet hide signs of phishing and make them ripe targets for socially engineered phishing campaigns.

VPNs enable lateral movement.

Organizations rely on VPNs to give their employees remote access to resources, but this approach has a number of security shortcomings. First, a VPN may grant individuals the capability to traverse to any app across your network from a single point of entry. Second, VPNs don't evaluate the context under which users or devices connect. Context is necessary to detect activity that's indicative of a compromised account or device.

Ransomware groups now operate like businesses. There is more evidence of organized groups carrying out scalable campaigns that increase their success rate and enable them to reinvest in new tools and procedures. Regardless of where or how we work, these groups continue to take advantage of vulnerable architecture to extort money from victims. Many organizations have taken steps to protect themselves from ransomware attacks, but attackers continue to evolve their tactics, and companies must respond.

How to secure apps



These recommendations are structured around the five functions in the NIST Cybersecurity Framework.

To find out more, visit nist.gov/cyberframework

Identify

Audit company systems and processes for vulnerabilities to malware.

Subscribe to a threat intelligence service to stay abreast of the latest malware threats.

Conduct regular network penetration tests to identify possible vulnerabilities – and act on the findings.

Protect

Deploy anti-malware functionality to all devices.

Add content filtering to all external gateways to make it more difficult for attackers to deliver malicious content to users via their web browser and email.

Where possible, prevent the use of removable media such as USB drives – at the very least, disable auto-run functions and set up devices to automatically scan removable media for malicious content.

Ensure that your backup policies are effective – backups should not be connected to the computers and networks they are backing up; for example, store them offline.

Verify your backups often – an emergency is a bad time to find out that there's a problem.

Use deny listing on external gateways to block access to known malicious websites.

Detect

Implement an MTD solution to quickly identify potential threats.

Educate users on how to identify and report unexpected system behavior – something a user may just see as an annoyance, like a device constantly needing charging, could be an indicator of malware infection.

Monitor devices for unusual behavior – including excessive data transfer and out-of-hours use.

Respond

Identify all infected devices and physically disconnect them from the network.

Suspend the login credentials of any accounts that may have been compromised.

Notify all users of the compromised app and what action to take – deleting the app may not always be the best course of action, as this could destroy important forensic data.

Recover

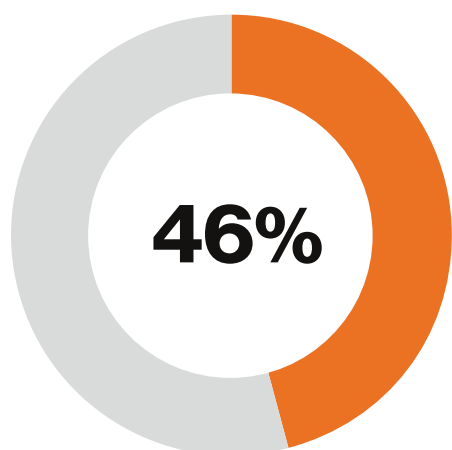
Reset all credentials, especially those with administrator privileges, that may have been compromised.

Wipe all infected devices and reinstall from the OS up.

Conduct a postmortem exercise to determine how the malware managed to get through and where controls, processes and technology fell short, and then distribute an “after action” report.

3.3 Devices and things

With the volume of devices a modern enterprise relies on, keeping them all up to date can seem like a Sisyphean task. With more and more devices, the danger of lost or missing devices grows. But it's not just the quantity of devices that's growing, the variety is growing too. Today there are smartphones, laptops, tablets, hybrids (like Microsoft Surface), Chromebooks, wearables and a seemingly endless range of connected devices.



Over a third of those that had suffered a mobile-related security breach said that device-based threats were a contributing factor. Those in the healthcare sector were most likely to list this as a factor, 47%.



Lost or stolen devices

People leave phones, tablets and laptops in taxis, on trains, at restaurants—the list goes on and on. Some of these will end up in a lost-and-found box, and others will find a new owner—or rather a new owner will find them.

One of the reasons so few organizations are worried is because loss/theft is one of the types of attack that's easiest to mitigate. Protections like device encryption and remote wipe are now standard with most types of user devices and MDM. But that doesn't mean that companies, or their employees, are using them. Whole-disk encryption and PIN security codes should be activated as a standard precaution on all devices. With these simple precautions in place, even if a device is stolen, the data it holds will be—for all intents and purposes—worthless to the attacker.



Mobile device management

MDM is not mobile security. MDM solutions were never designed to protect against sophisticated cyberattacks. The purpose of these solutions have always been management—the clue is in the name. The security capabilities of these solutions have always been quite limited. They can be useful in ensuring applications are kept up to date and some other policies are being followed. But devices are prone to threats like phishing even with MDM in place, as this data from Lookout shows. This shows that the difference in encounter rate is small, and on occasion devices with MDM even faced more attacks.

Encounter rate of phishing attacks on devices with/without MDM

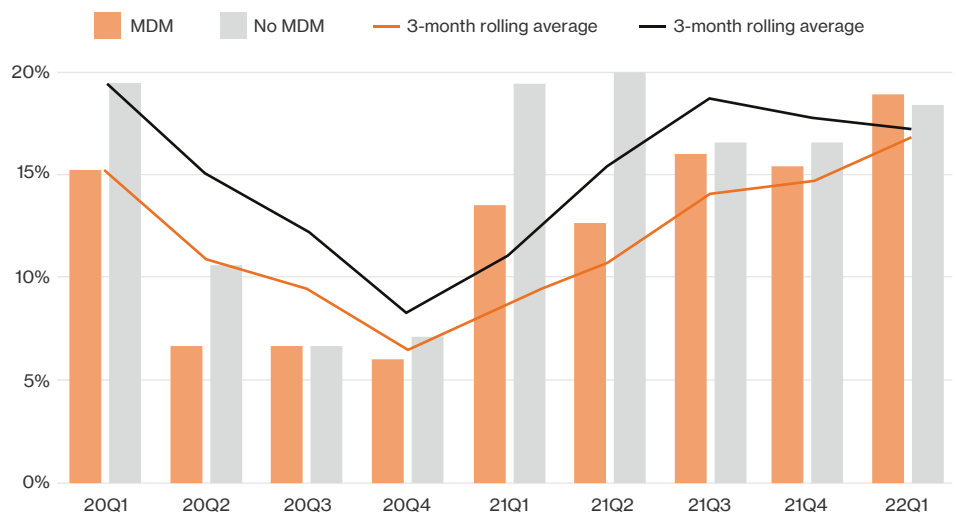


Figure 24. Incidence of phishing attacks on devices with/without MDM in place. Data from Lookout.⁵¹

⁵¹ Lookout, data supplied, June 2022

The case for MTD



Pete Nicoletti
Field CISO
Check Point

Unified endpoint management (UEM) solutions—or their predecessors, mobile device management (MDM) solutions—were designed to help mobilize businesses by streamlining processes, managing device life cycles and creating a managed workspace on smartphones and tablets. Today, UEM solutions have evolved into consolidated solutions that work with other endpoints beyond mobile devices, including PCs.

UEM enforces some device-level policies—such as device encryption and remote wipe—to maintain a basic hygiene and some have a basic jailbreak/root detection function too. But these basic features don't provide the protection needed to withstand even the most basic mobile malware attack. UEMs do not scan for mobile-related threats like malicious apps, vulnerable operating systems or network-based attacks, nor do they protect users against phishing and other social engineering attacks. Even with a UEM solution in place, organizations remain exposed to credential theft, data leakage or device takeover.

A mobile threat defense (MTD) solution is essential to keep corporate data on mobile devices secure, protected from all attack vectors.

To find out more, read the Check Point white paper, *Mobile Management Solutions Are Not Security*.⁵²

UEMs do not scan for mobile-related threats like malicious apps, vulnerable operating systems or network-based attacks, or protect users against phishing and other social engineering attacks. As a result, users and organizations remain exposed to credential theft, data leakage or device takeover.

Features	MDM/UEM	MTD
Device life-cycle management	•	
App management and containerization	•	
Remote access	•	
Conditional access	•	•
Jailbreak/root detection	Partial	•
Malicious app detection		•
Download prevention		•
Anti-phishing (known and unknown sites)		•
Anti-bot (blocking C&C communications)		•
Man-in-the-middle attack prevention		•
URL filtering		•
Real-time threat intelligence		•

⁵² Check Point, *Mobile Management Solutions Are Not Security*, 2021

The dangers of things

One of the challenges of securing IoT projects is the lack of centralized coordination of projects. In many organizations, IoT projects are led by the lines of business and don't even have to follow standard security requirements.

Remember, an IoT device can be an attack vector (a weak point that can be exploited to mount an attack), a vehicle for attacks (like a part of a botnet used to carry out a distributed denial-of-service (DDoS) attack) or a target in its own right.

42%

Lines of business/business units initiate their own IoT projects.

59%

IT has oversight of all IoT projects.

48%

There is central coordination of all IoT projects.

53%

We have defined IoT security standards that apply to all projects.

The nature of IoT devices themselves also presents distinct challenges compared to securing other mobile devices. These fall into three broad areas:

Variety

The sheer volume and diversity of IoT devices can present enormous logistical obstacles to effective device security. It doesn't help that many IoT products have been found to have extremely weak cybersecurity—including security devices such as smart locks, doorbells and, ironically, security cameras.

Distance

Many IoT devices are out in the field. This can make them vulnerable to physical tampering or network attack and harder to update or replace. Isolation can also make devices vulnerable to SIM theft, one of the simplest types of attack to carry out—often all that's required is a screwdriver. All the hacker has to do is break open the connected device, such as a smart lamppost, and remove the SIM. This can then be put into another device, giving the user free calls and data at the organization's expense.

Longevity

In the survey for the previous edition of this report, we found that over half (54%) said that some of their IoT devices had an anticipated lifetime of five years or more—up from 36% in our previous report. This would be very old for a smartphone or laptop. Combined with the difficulty of updating devices, this can make it hard to keep IoT protected against constantly evolving threats.

How to secure IoT devices



These recommendations are structured around the five functions in the NIST Cybersecurity Framework.

To find out more, visit nist.gov/cyberframework

Identify

Thoroughly review the security before you purchase anything.

Ask potential vendors to supply details of their security measures, and review them for robustness.

Protect

Harden all devices, including ensuring they are tamper-resistant and tamper-evident.

Change all default or vendor-supplied passwords.

Change all default or vendor-supplied passwords, really.

Shut down anything you don't need – if you're not using a port or protocol, block it.

Keep devices patched – use over-the-air (OTA) updates to help keep devices secure, especially those in remote or difficult-to-access locations.

Bind SIMs to devices, limiting the potential damage of SIM theft.

Use private, non-routable IP addresses to make it harder for attackers to access IoT devices.

Consider using a private cellular network to keep devices off the public internet.

Encrypt data in transit and at rest.

Create an IoT security assurance process that regularly analyzes IoT risk data in your organization.

Ensure that users developing or purchasing IoT programs work with the information security team to factor in the cost and resources required to secure devices and applications.

Detect

Use network intrusion detection tools to monitor all traffic, incoming and outgoing, for unusual activity and put in place a process to handle any alerts promptly.

Subscribe to a threat intelligence service to get early warning of emerging threats.

Analyze logs for signs of suspicious behavior.

Integrate MTD with EDR or security incident event management (SIEM) to help simplify monitoring and, should it be necessary, forensic analysis

Respond

Put controls in place to contain the spread of infection and prevent the attacker from gaining any additional access or access to sensitive data.

Implement network blocks to limit an attack from infecting more devices or the attacker from accessing more critical systems.

Recover

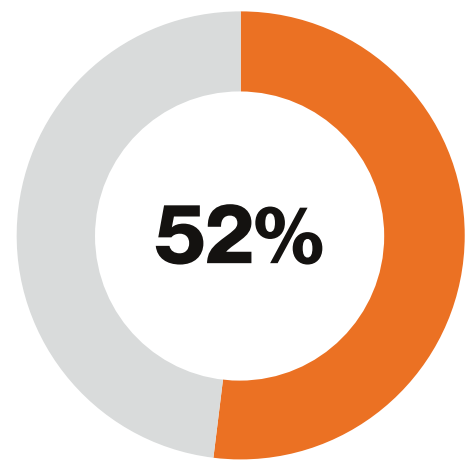
Conduct a postmortem to determine how the attack managed to get through and where controls, processes and technology fell short, and then distribute an "after action" report.

3.4 Networks and clouds

Insecure networks remain a serious threat to mobile device security. Attackers can intercept traffic through man-in-the-middle (MitM) attacks or lure employees into using rogue Wi-Fi hotspots or access points. Cloud-based services are now used for many mission-critical tasks. They are also one of the reasons that mobile devices have become more critical to business. That brings a whole new range of problems.

“There is a distinct imbalance between protecting a network and attacking it, and this imbalance continues to grow as more effective hacking resources become available at a significantly lower cost. But without continuous investment and commitment to cyber resilience, organizations will be more vulnerable to cyberattacks and thus more likely to endure reputational, financial, operational and safety impacts.”

—World Economic Forum, 2022⁵³



Over half of those that had suffered a mobile-related security breach said that network threats were a contributing factor. Those in the financial services sector were most likely to list this as a factor, 61%.

⁵³ World Economic Forum, Global Cybersecurity Outlook 2022, 2022.

Public Wi-Fi

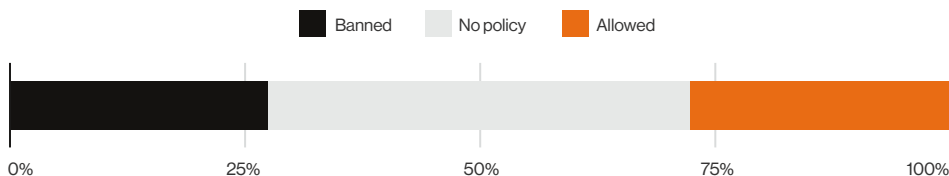
Another familiar topic. With traveling off the agenda, public Wi-Fi may not have been on your list of most pressing issues last year, but it remains a critical issue. Reports suggest that corporate travel is at less than 50% of pre-pandemic norms and experts suggest that it will take years to recover—if it ever does. But the dangers of public Wi-Fi aren't limited to executives jetting around the world, or even employees traveling by plane, train or automobile.

There's a lot of disagreement about working models, how they have changed and how they may change in the future. But it's safe to say that fewer people are now following the traditional model of commuting to the office five days a week. For a lot of people, that means working from home a couple of days a week or more. Maybe that includes the odd afternoon in a coffee shop for a change of scenery. Or whether you work from home or not, who hasn't checked their email when at the mall or in a restaurant or other public place. With reliable, high-speed mobile internet now widely available, you might do this on a cellular connection. But whether for performance or to avoid data caps, people still use public Wi-Fi, with all its attendant dangers.

Less than a third of organizations (32%) ban the use of public Wi-Fi, and only about half (52%) of those actually do anything to enforce that policy.

In fact, 43% of respondents working for companies that banned the use of public Wi-Fi admitted breaking the rule themselves.

Public Wi-Fi policy



Blocking of public Wi-Fi

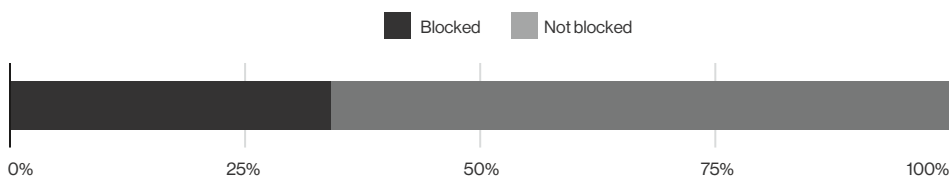


Figure 25. Public Wi-Fi policy. [n=632]

Ah, you might say, but it's okay as long as you use a virtual private network. VPNs do offer a degree of protection, but many companies still rely on an "honor approach." Even among the informed audience that made up our survey respondents, 8% admitted to not using a VPN when using public Wi-Fi. It's quite likely that this is an underestimate—many people will forgive themselves the odd slipup. It's highly likely that this number is much higher among employees that don't work in cybersecurity.

x2

In 2021, the number of devices connecting to a risky hotspot per week doubled from 0.5% to 1%.⁵⁴

46%

Nearly half of VPN clients are misconfigured or out of date.⁵⁵

See our discussion of Zero Trust approaches on page 56.

54 Absolute, The Future of Work, 2022

55 Jamf, Security 360 Annual Trends Report, 2022.

Home Wi-Fi

With fewer people working in the office five days a week, it's inevitable that more business is being done over home Wi-Fi and home broadband connections. It's unsurprising then that nearly four-fifths of businesses allow employees to use their home networks.

Home Wi-Fi policy

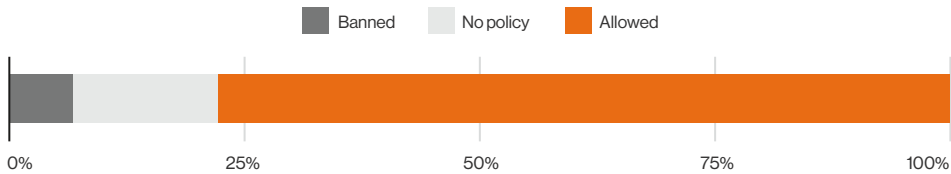


Figure 26. Use of home Wi-Fi. [n=632]

While likely to be less risky than public Wi-Fi (see our 2019 report), home Wi-Fi is still a concern. Ask yourself how many employees have:

Changed the default password on their home router?

Shared their router password with dozens of friends and family members – maybe even neighbors?

Updated their router firmware since receiving it?

Looked at router logs for signs of intrusion?



Proofpoint surveyed 3,500 working adults across Australia, France, Germany, Japan, Spain, the U.K. and the U.S. It found that most hadn't taken basic security measures to protect their home Wi-Fi network.⁵⁶

Of those who hadn't taken steps to secure their home Wi-Fi, 62% said that was because they weren't concerned about the security of their home network. Close to 90% of the rest said it was because they didn't know how to.

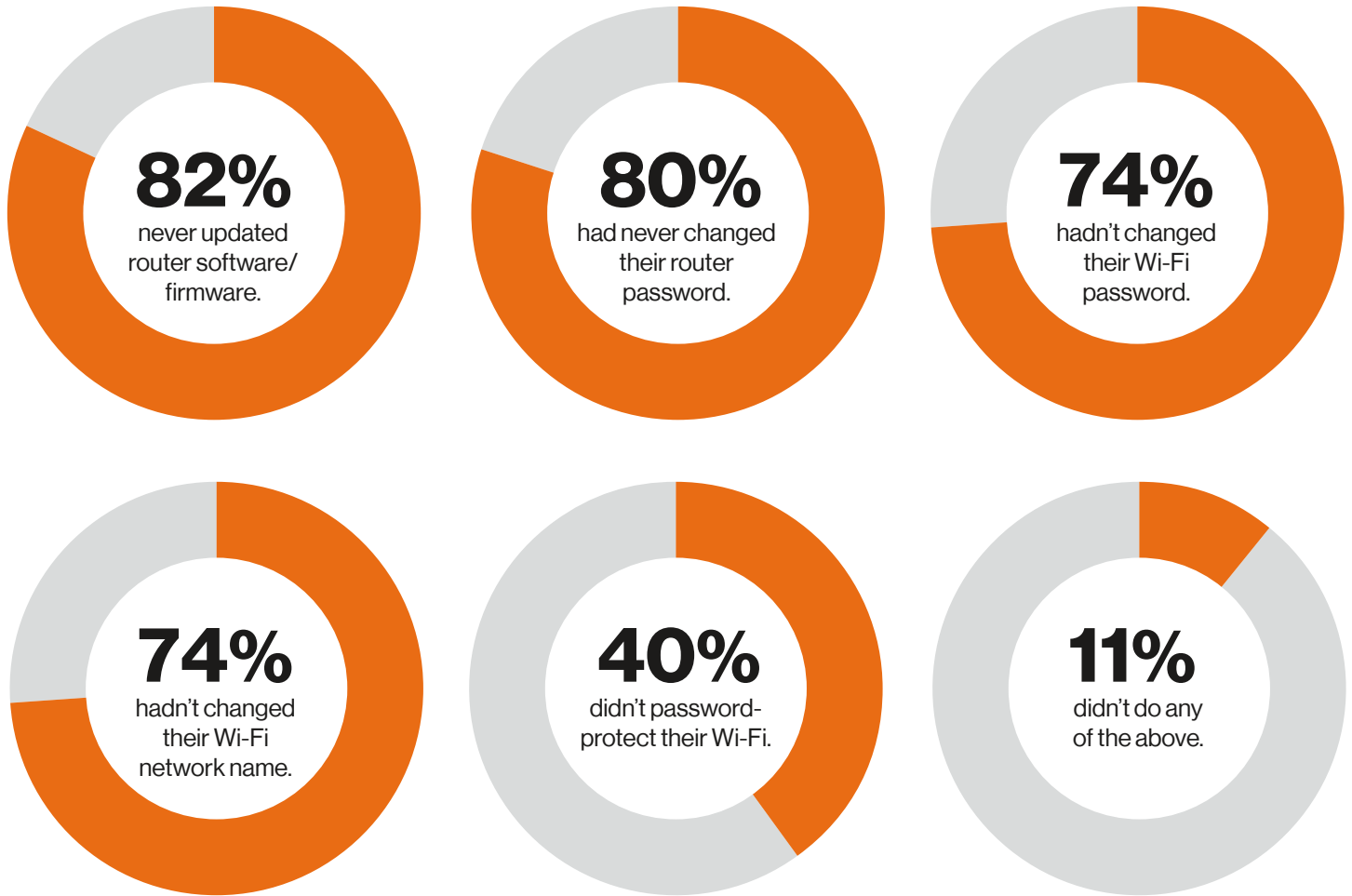


Figure 27. What measures working adults took to protect their home Wi-Fi network.

⁵⁶ Proofpoint, 2022 State of the Phish, 2022

How to secure networks



These recommendations are structured around the five functions in the NIST Cybersecurity Framework.

To find out more, visit nist.gov/cyberframework

Identify

Remember that mobile devices could provide an entry point for a wide range of attacks; consider ways that attackers could disrupt operations as well as expose data.

Protect

Re-architect your network into smaller segments, isolating the hosts and services that hold sensitive data.

Implement a “least privilege” access policy—if people don’t absolutely need access, they shouldn’t have it, and access should be revoked when no longer required.

Secure all wireless access points; allow only known devices to connect to corporate Wi-Fi services.

Educate users on the dangers of Wi-Fi, including rogue access points.

Consider providing users with a fixed wireless access (FWA) device—sometimes called mobile broadband—exclusively for use when working from home.

Confirm that employees chose a home broadband solution that includes regular firmware updates to patch any new vulnerabilities.

Consider putting systems like MDM or endpoint protection in place to block the use of public Wi-Fi entirely.

Implement MTD to monitor and mitigate the risk of MitM attack.

Consider using a cloud access security broker (CASB) or secure web gateway (SWG) to help secure all connections to cloud-based systems.

Detect

Use network intrusion detection tools to monitor all traffic, incoming and outgoing, for unusual activity and put in place a process to handle any alerts promptly.

Subscribe to a threat intelligence service to get early warning of emerging threats.

Analyze logs for signs of suspicious behavior.

Integrate MTD with EDR or SIEM to help simplify monitoring and, should it be necessary, forensic analysis.

Respond

Create an IR plan that covers how to qualify and categorize incidents, what should be done and who the responsible parties are.

Recover

Conduct a postmortem to determine where controls, processes and technology fell short and then distribute an “after action” report.

Consider updating policies; at the very least, remind users about your AUP and their responsibilities.

Zero Trust

4



Zero Trust network access (ZTNA) is an approach to network security that assumes every device, application or system that connects to your network potentially could be compromised. It involves granting authorized users access only to the applications they need to perform their jobs. It also isolates specific applications, devices and systems to certain parts of the network and doesn't make the internal network visible to the internet, which could otherwise make it easier for hackers to infiltrate.

Zero Trust network access

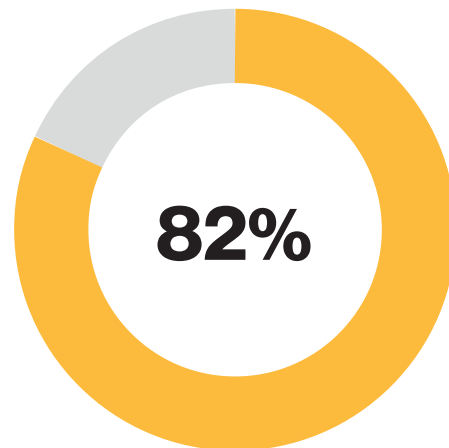
ZTNA can be an effective alternative to the traditional approach to network security, which typically involves using a VPN to connect workers from remote locations and implicitly trusting these connections.

A Zero Trust security approach can bolster endpoint, network and remote work security by minimizing the company's exposure. With this model, dozens or potentially hundreds of devices, applications and users would not have wide-ranging access to the company's network or sensitive data—they could only access the systems and information to which they are authorized.

Though ZTNA can strengthen a company's security policy and make it more resilient, it's also important to balance this approach with delivering a user-friendly digital experience that helps remote employees remain productive. If employees can't easily access the applications and systems they need to do their work, they may not be as productive.

It's a delicate balance, but you can deliver a frictionless remote work experience while also helping to keep the organization secure. For example, intelligent, analytics-driven identity access management solutions can automate the process of determining when to grant a specific user access to certain applications. AI-driven threat detection solutions can also help your organization detect anomalies or suspicious user behavior and network activity and isolate these threats before a breach occurs. This way, employees don't have to deal with onerous authentication requirements; they aren't unintentionally blocked from accessing the systems they need to do their jobs and also aren't given unauthorized access to sensitive data.

As companies embrace remote and hybrid work, a ZTNA model can help combat security threats while giving employees the flexibility to work from anywhere and on any device they choose—whether it's their desktop, tablet or phone. With an approach focused on verification rather than implicit trust, companies can establish a strong security perimeter, deliver a better employee experience and remain agile in the increasingly complex threat environment as they adapt to the future of work.



A large majority of respondents said that they had adopted or were actively considering adopting a Zero Trust approach to security.

A continuous Zero Trust mindset



Sanjay Beri
Founder and CEO
Netskope

47%

Nearly half of respondents that experienced a mobile-related compromise said that cloud-based systems/apps were compromised as a consequence.

The White House's executive order (EO) highlights many specific areas of interest for not only federal government security, but how we should be thinking about security and network architecture everywhere.⁵⁷

As the EO notes: "To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, the Federal Government must take decisive steps to modernize its approach to cybersecurity, including by increasing the Federal Government's visibility into threats, while protecting privacy and civil liberties."

According to the EO, agency heads are required to update existing agency plans, develop a plan to implement Zero Trust Architecture based on current NIST migration steps, and report on progress – within 60 days of the order. This is powerful, not least because it helps bring Zero Trust back down to earth from how over-marketed the term has become in recent years. It helpfully frames Zero Trust in architecture terms – something Netskope has also underscored and that we're seeing as common to the success of our many customers worldwide.

In a modern architecture, Zero Trust principles should be judiciously applied, adaptively and continuously. But today, many organizations don't have much more than isolated "Zero Trust projects" focused on networks, users, devices or isolating servers. The main miss on most of these projects is that they are focused on application-level access and other pieces, but not focused on the data. Architecturally, we must go beyond access control and isolation to provide continuous Zero Trust: real-time access and policy controls that adapt on an ongoing basis based on users, devices, apps, threats and data context.

This data-centric approach is the only effective way to dynamically manage risk across a mix of third-party applications and a remote-first workforce that needs always-on access to cloud apps and data to stay productive. As the EO calls out in Section 10, item K:

"Zero Trust Architecture embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting data in real-time within a dynamic threat environment. This data-centric security model allows the concept of least-privileged access to be applied for every access decision, where the answers to the questions of who, what, when, where, and how are critical for appropriately allowing or denying access to resources..."

Proper application of Zero Trust principles is also a critical step toward Secure Access Service Edge (SASE) architecture. SASE isn't specifically mentioned in the EO, but as the order explains, applying Zero Trust at an architectural level means "a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgment that threats exist both inside and outside traditional network boundaries." In other words – and crucial to SASE – yesterday's security and network technologies and designs won't even start to address the prevalence of cloud-delivered threats or attacker abuse of cloud apps, or the increasingly acute need for security and networking teams to more effectively converge and collaborate.

⁵⁷ The White House, Executive Order on Improving the Nation's Cybersecurity, 2021

Conclusion

While preparing this report, at the end of each interview, we asked the same question: Are you optimistic or pessimistic about the future of mobile device security? Without exception, every one of the experts said that they were optimistic. When we asked them why, they had a variety of reasons. Some cited the growing awareness of the issue among business leaders; others talked about the advances in technology, including the introduction of AI; some talked about improved regulation and industry standards.

It's been said that sunlight is the best disinfectant.⁵⁸ As cybersecurity becomes more high-profile, it is receiving more attention from consumers, business leaders and legislators. This increased attention is driving companies to take the issue more seriously and legislators to improve guidance for organizations. In the past, many cybersecurity regulations were criticized for being too "outcome-based" and offering little clear guidance. Our panel of experts said that they see that changing.

But having rules and tools in place is only part of the story. Our experts weren't surprised to hear that over half of respondents had said that they'd sacrificed mobile device security. And when we asked them for a single piece of advice for our readers, the majority of them said that they wished more companies used all the tools that they were paying for.

Based on our experts' advice, we have strived to pack this report with lots of practical advice. We hope that you find it useful and that it helps you to educate your employees, inform your leadership and get more out of your cybersecurity investments.

We too are optimistic about the future of cybersecurity, because people like you got through a whole 58 pages.

You didn't cheat and skip to the last page did you?

64%

Nearly two-thirds of respondents said that public awareness of cybersecurity risks will increase in the future.

66%

Nearly two-thirds of respondents said that they'd come under pressure to sacrifice mobile-device security "to get the job done." And 79% of those (52% of all respondents) had succumbed to that pressure.

58 Louis Brandeis, *Other People's Money*, 1914

Appendices

5

In compiling this report, we interviewed a number of leading security experts among our contributors. Talking with these highly experienced security professionals was fascinating and really helped us to shape this report. We are really grateful to them for their time.

Terminology used in this report

Organization descriptions

Throughout this report, when we refer to companies, businesses or organizations, we include both public- and private-sector entities of all sizes. We use the term “enterprise” to refer to organizations with 500 or more employees, and “small and medium-sized businesses (SMBs)” for those with fewer.

Security terms

Security terms like “attack” and “breach” are often used interchangeably. For clarity and precision, we have used the following definitions throughout this report:



Attack

A general term covering any deliberate action toward a system or data that is unauthorized. This may be as simple as attempting to access it without permission.



Compromise

A successful attack that results in a system's defenses being rendered ineffective. This could involve data loss, downtime, other systems being affected or no detrimental effects at all. It could be malicious or accidental.



Data breach

An incident that results in the confirmed disclosure – not just potential exposure – of data to an unauthorized party.



Exploit

A definition, often in the form of a script or code, of a method to successfully leverage one or more vulnerabilities to access a system without proper authorization.



Incident

This covers any form of security event, malicious or not, successful or not. This could be anything from a failed authentication attempt to a successful compromise and data breach. It includes non-malicious events, such as the loss of a device.



Risk

A measure of the likelihood of a threat, an organization's vulnerability to said event and the scale of the potential damage.



Threat

Any danger that could impact the security of systems or privacy of data. This can apply to a technique, such as phishing, or an actor, such as an organized criminal group.



Vulnerability

A weakness that could be exploited. It may be known or unknown – to the manufacturer, developer, owner or the world.

Survey methodology

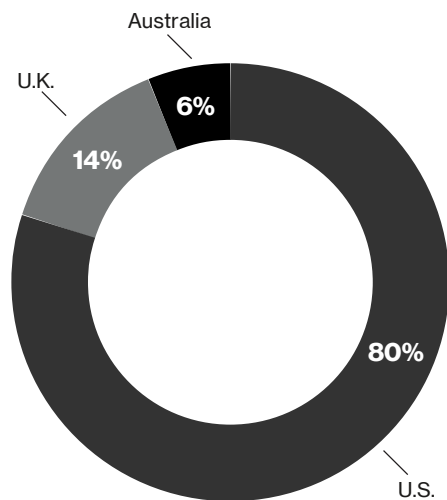
We contracted an independent research company to survey senior professionals responsible for the procurement, management and security of mobile devices.

In total, 632 professionals responsible for the buying, managing and security of these devices responded. The charts below break down the demographics of these respondents. Our sample included both small companies and large enterprises.

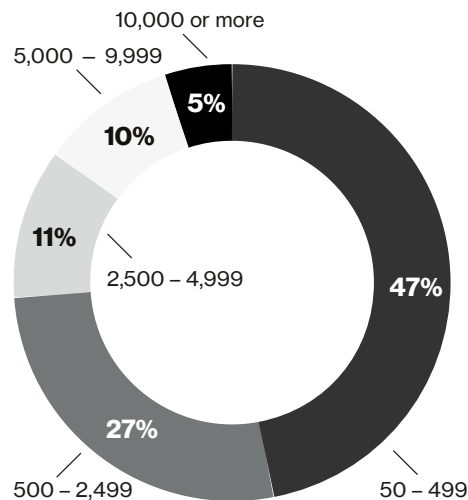
Company size was not a strong indicator for most of our questions. Unless stated otherwise, all data in this report is from this survey.

Unless stated otherwise, stats quoted in this report are from this survey.

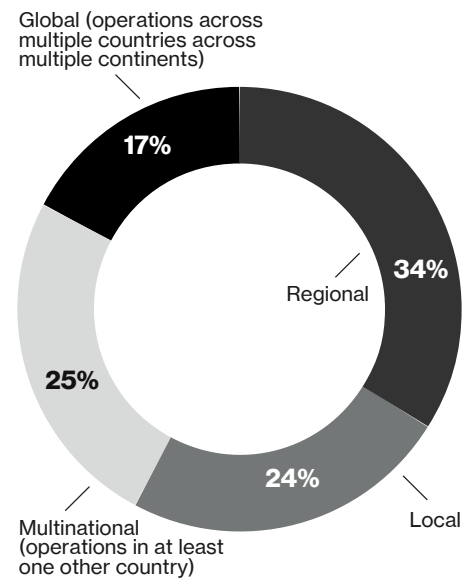
Respondents by country



Respondents by company size



Respondents by company operations



Data from contributions

Details of the source of data and statistics supplied by our contributors are given in the next section.

Contributors

ABSOLUTE

Absolute

Maintain secure remote access, without sacrificing on experience. Kick off or continue your journey to SASE with a cloud-first security platform that improves the remote working experience. NetMotion by Absolute provides optimized remote access with a Zero Trust security posture alongside context-aware policy enforcement for all endpoints on any network. It also enables complete visibility of remote devices and the employee experience.

absolute.com



Check Point

Check Point is a leading provider of cybersecurity solutions to governments and corporate enterprises globally. Its solutions protect customers from fifth-generation cyberattacks with a leading catch rate of malware, ransomware and other types of attacks. Check Point offers multilevel security architecture, “Infinity” Total Protection with Gen-V advanced threat prevention, which defends enterprises’ cloud-, network- and mobile device-held information. Check Point provides one of the most comprehensive and intuitive “one point of control” security management systems. Check Point protects over 100,000 organizations of all sizes.

checkpoint.com

IBM MaaS360

IBM

IBM Security MaaS360 with Watson transforms how IT is securing smartphones, tablets, laptops, desktops, wearables and IoT without sacrificing a great user experience. AI and predictive analytics keep you alerted to potential endpoint threats and provide remediation to avoid security breaches and disruptions. MaaS360 protects apps, content and data so organizations can rapidly scale their remote workforce and BYOD initiatives.

The MaaS360 Mobile Metrics feature offers cloud-sourced benchmarking data and best practices to enhance productivity and improve security. Benchmarking data is generated by leveraging multiple data values from MaaS360 client implementations to build aggregated metrics.

ibm.com/security/mobile/maas360



Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT applications and data over various networks to stay productive as they work from anywhere. The Ivanti Neurons automation platform connects the company's unified endpoint management, Zero Trust security and enterprise service management solutions, providing a unified IT platform that enables devices to self-heal and self-secure and also empowers users to self-service. Over 40,000 customers, including 96 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end-user experiences for employees, wherever and however they work.

ivanti.com



Jamf

Jamf's purpose is to simplify work by helping organizations manage and secure an Apple experience that end users love and organizations trust. Jamf is one of the only companies in the world that provides complete management and security solutions for an Apple-first environment that is enterprise secure, consumer simple and protects personal privacy. Today, more than 62,000 customers rely on Jamf to manage and secure more than 27 million devices worldwide.

jamf.com



Lookout

Lookout is a leading provider of endpoint and cloud security solutions. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and various partners across telecommunications and technology.

Powered by one of the largest data sets of mobile code in existence, the Lookout Security Graph provides visibility into the entire spectrum of mobile risk. The installed base of Lookout's personal and enterprise mobile endpoint products is over 205 million mobile devices worldwide. This acts as a global sensor network that provides visibility into the threat landscape, including over 170 million apps—and that's growing by up to 90,000 apps a day

lookout.com



Netskope

Netskope safely and quickly connects users directly to the internet, any application, and their infrastructure from any device, on or off the network. With CASB, SWG, and ZTNA built natively in a single platform, the Netskope Security Cloud provides the most granular context, via patented technology, to enable conditional access and user awareness while enforcing Zero Trust principles across data protection and threat prevention everywhere. Netskope's global security private cloud provides full compute capabilities at the edge.

Netskope's Security Cloud protects 25% of Fortune 100 companies, including:

- Three of the world's six largest airlines
- Three of the world's four largest banks
- Five of the world's seven largest healthcare providers
- Two of the world's largest telecommunications companies

Netskope is fast everywhere, data-centric and cloud-smart, all while enabling good digital citizenship and providing a lower total cost of ownership.

netskope.com

proofpoint.

Proofpoint

Proofpoint, Inc., is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyberattacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web.

proofpoint.com

THALES

Thales

Thales is a global high-technology leader investing in digital and "deep tech" innovations—connectivity, big data, artificial intelligence, cybersecurity and quantum technology—to build a future we can all trust, which is vital to the development of our societies. The company provides solutions, services and products that help its customers—businesses, organizations and states—in the defense, aeronautics, space, transportation, and digital identity and security markets to fulfill their critical missions, by placing humans at the heart of the decision-making process.

thal.es/group.com

