

THE MOBILE

BYOD

SECURITY
REPORT



New research on Bring Your Own Device (BYOD) trends for today's workforce and the security risks for organizations.

In This Report

As demonstrated in many major breaches in 2022, the growing use of personal devices and personal apps in 2022 resulted in many high-profile corporate breaches. With the widespread use of personal mobile devices in the workplace, it is increasingly difficult for employers to ensure the security of sensitive information.

In the report you will learn:

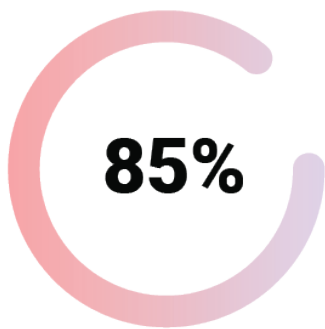
- How much work employees do on their personal devices
- Types of work tasks employees do on their personal devices
- The prevalence of corporate-related attacks directed to personal devices
- How much employees trust their company to install a data security app on their personal devices
- How common it is for companies to require installation of security apps
- The prevalence of company passwords being stored on personal devices
- How security leaders are balancing data security and employee privacy
- How technology is used to block attacks and keep employees happy
- The types of threats IT leaders are most concerned about

Report data and methodology: The report data is taken from survey results of 300 IT Security Professionals and employees in organizations with over 1,000 employees. The threat data is taken from a sample of threats detected by SlashNext security products. SlashNext analyzed over a billion link-based, malicious attachments and natural language threats scanned in email, mobile and browser channels. The organizations in our sample ranged in size from 500 to 100,000 users. The organizations spanned a variety of industries in North America.

Employers Strive to Strike the Right Balance to Meet Mobile BYOD Needs

Employers are highly concerned about both securing corporate data and maintaining employee privacy. Many major breaches in 2022 were caused by the direct use of personal devices and personal apps. With the widespread use of personal mobile devices in the workplace, it is increasingly difficult for employers to ensure the security of sensitive information. Despite the availability of tools and options for securing data, many employers

Use of Business Apps Is Increasing on Personal Mobile Devices



85% of employers require work related apps to be installed on personal devices of employees

are not confident in their ability to effectively manage the risk of personal mobile devices to avoid data breaches and privacy violations. This is further compounded by the fact that employees often use both corporate and personal devices for work, effectively doubling the attack surface for cyber criminals. Phishing is a major concern for both employees and employers, as it is a common tactic used by cyber criminals to steal sensitive information. Despite efforts to educate employees on how to identify and avoid phishing scams, many employers do not believe that training alone is enough to prevent these types of attacks. As the threat of phishing continues to grow, it is becoming increasingly important for employers to find new and effective ways to secure their corporate data and protect employee privacy.

Employers today face a significant challenge in balancing the need to secure corporate data and maintain employee privacy. In addition to the security and privacy concerns mentioned earlier, employers who have employees using their personal mobile devices for work face a number of other challenges. For example, there may be difficulties in enforcing company policies and procedures on personal devices, as well as difficulties in ensuring that these devices are updated and maintained in accordance with security best practices. Furthermore, there may be legal and compliance issues associated with storing sensitive data on personal devices, particularly if the devices are lost or stolen.

Additionally, there may be issues related to data ownership and access, particularly if employees leave the company or change roles within the organization. Given these challenges, it is becoming increasingly important for employers to have a comprehensive strategy in place for managing the use of personal devices in the workplace and ensuring the security and privacy of sensitive data.

Employers Want to Protect Sensitive Company Information While Maintaining Employees' Privacy

90% 63% 89%



90% of security leaders say protecting employees' personal devices is a top priority

63% say they definitely have the tools to adequately do it

89% of IT and security leaders acknowledge legal concerns about having access to employees' private data

Employees Rely on BYOD for Productive Hybrid Work Life

Employees are clear that they sincerely want to protect sensitive company information on their devices, but not at the cost of their privacy. Here's what employees told us about striking the right balance.

There are several reasons why employees use their personal mobile devices for work. One of the main reasons is convenience and flexibility. Personal mobile devices, such as smartphones and tablets, allow employees to work from anywhere and at any time, which can be particularly important for those who need to work outside of traditional office hours.

Employees also prefer to use their personal devices because they are already familiar with the operating system and the apps they use, which can increase productivity and reduce the learning curve associated with using a new device. Finally, many employees today view their personal devices as essential tools for staying connected and informed, and they may feel more comfortable and secure using a device that they own and control. These factors all contribute to the growing trend of employees using their personal devices for work, which presents both opportunities and challenges for employers.

5

Most Performed Work Tasks on Personal Mobile Devices



01

Read and send email

02

Text messaging

03

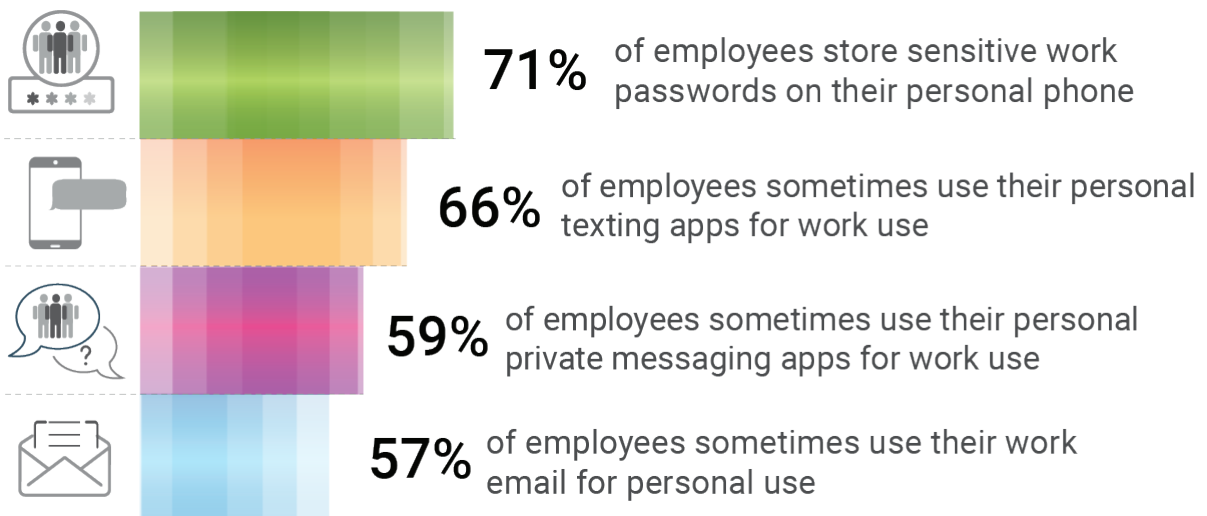
Make and Receive Calls

Security Gaps and Risky Behavior Make BYOD Mobile Devices Ripe for Cybercrime

With the convergence of work from home and the rising popularity of using mobile devices for everything from sending a work-related SMS to attending a Zoom call, it was only a matter of time before cybercriminals seized the opportunity to target users through the least protected and most popular communication medium.

Cybercriminals know that more sensitive information is stored and accessed through mobile devices, so they have shifted their attention to mobile devices for attacks as employees continue to use their personal devices for work. Mobile device attacks have become increasingly attractive targets for cybercriminals because using personal devices for work can create security vulnerabilities. Employees may not be as vigilant about protecting their devices as they would be with a company-issued device. Many mobile devices have weaker security features than desktop computers, and mobile operating systems often need to be updated more frequently, leaving devices open to attack.

Majority of Employees Engage in Risky Behavior on Personal Mobile Devices



Finally, the increasing use of mobile devices for online banking, shopping, and other activities has created a larger pool of potential victims, making mobile devices an attractive target for cybercriminals looking to steal sensitive information. Given these factors, employees and employers must be proactive in protecting mobile devices and their sensitive information.

SlashNext Threat Labs sees many mobile-specific phishing attacks daily, with 50% happening outside of email. These attacks are customized for mobile delivery and designed only for iOS or Android. What makes them particularly dangerous is the attack vector is not email but SMS, malicious in-app ads, and messages, where security is not as effective. The most popular types of mobile-specific phishing attacks include the following:

- Business Text Compromise (BTC)
- SMS-based money transfer & gift scams
- Rogue software, including fake VPNs, used to conduct man-in-the-middle attacks
- Account Take-Over (ATO)
- Multi-stage phishing, including SMS, voice, and links for fake fraud alerts or technical support scams

Employers Prefer That Employees Use Company Issued Devices

81%



of employers say the solution for employee mobile data security and privacy is to give employees a separate phone just for work

81% of employers prefer that employees use company-issued devices. Even when employees are offered a separate corporate device, they still admit to using their personal device for work, doubling the attack surface, with 71% of employees storing sensitive work passwords on their personal phones.

Given the expanded threat surface, it's justifiable that employers feel they need to be more confident they have the necessary tools or options for securing corporate data and maintaining employee privacy regarding employees' personal devices. While phishing is a major concern, and they expect that threat to grow over the next year, employees still engage in risky behavior, with 43% of employees having been the target of a work-related phishing attack on their personal devices.

Most IT and security leaders (95%) say phishing attacks via private messaging apps are an increasing concern, as some of the biggest breaches in 2022 involved personal devices and apps. Yet they don't believe training is enough to stop phishing, with 98% of employers saying that employees are still susceptible to phishing and other attacks, even with regular training.

Employees Risky Behavior Concerns Security Leaders



of employees have been the target of a work-related phishing attack on their personal device



of security leaders say that phishing attacks via private messaging apps is an increasing concern

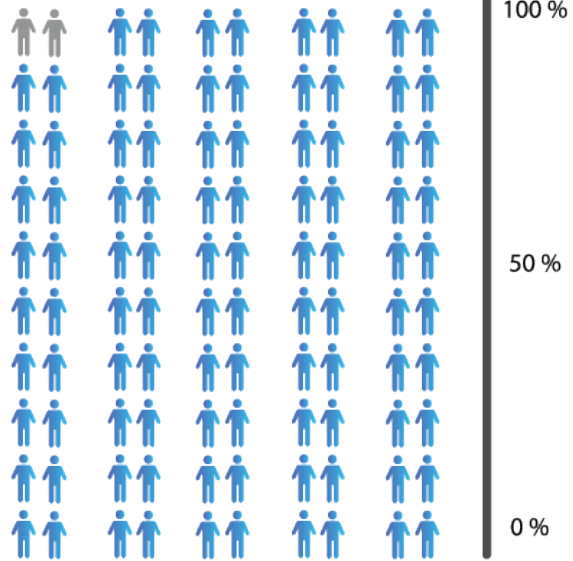
Employers don't feel confident they have the necessary tools/options for securing corporate data and maintaining employee privacy regarding employees' personal devices. While most security leaders say protecting employees' personal devices is a top priority, only 63% say they have the tools to do it adequately. They acknowledge legal concerns about having access to employees' private data.

Still, our research reveals that employees and employers are close to agreement on securing mobile devices. More employees are worried about being the target of a corporate phishing attack than employer surveillance on their personal devices, and 85% of employers require work-related apps to be installed on employees' personal devices.

Training Does Not Stop Risky Behavior



98% of employers say that even with regular training, employees are still susceptible to phishing and other attacks



Conclusion

For a good reason, employers are concerned about mobile phishing attacks on private messaging apps. Cybercriminals are launching phishing attacks on personal apps and successfully reaching business systems, leading to headline-making breaches and having a big impact on businesses. The vast majority of mobile devices have no special security protection other than the protections natively built into iOS and Android. While employers are worried about finding the right balance between protection and privacy on mobile BYOD, employees are more worried about being the target of a corporate phishing attack than surveillance on their personal devices. So, finding a solution for protecting BYOD devices is within reach.

The Verizon MIS report shows 83% of organizations report mobile device threats are growing more quickly than other device threats. As organizations embrace the expanding remote workforce, it will be important to have a mobile BYOD security strategy that strikes the right balance between security and privacy to keep the BYOD workforce secure from cybercriminals launching attacks on mobile devices using tactics including SMS/text phishing (Smishing), and non-linked based phishing.

It will be critical to implement phishing protection that protects users without degradation in user experience and doesn't transmit personal data to meet the needs of securing business systems while providing employee privacy.

SlashNext Mobile Security Stops Threats and Maintains User Privacy

Organizations know the sheer number of unprotected devices that can access their corporate data, and until now, there has not been a BYOD solution that addresses the privacy concerns of the user with the enterprise level protection organizations expect.

SlashNext Mobile Security gives another layer of security to users on their personal devices and gives businesses the opportunity to protect both company data and maintain employees' privacy. SlashNext is the only on-device solution to block link and natural language SMS phishing attacks, the first attack stage in Business Text Compromise (BTC). SlashNext HumanAI™ leverages natural language processing and behavioral analysis to improve efficacy to 99.9% for peace of mind against the growing threat of phishing and fraud attempts on SMS/text, Links, and apps while offering total privacy for users' data.


There are three mobile security products to meet the complex needs of any organization to protect iOS and Android users from smishing and targeted threats in all apps.

- For Business: Centrally managed, with multiple deployment options, incidents written to CMS, and supports all device types.
- For Personal BYOD: Activate using the SlashNext voucher code—no incidents recorded in CMS.
- For Home: Direct to consumers with purchase available on Apple Pay and Google Pay—no incidents recorded in CMS Family sharing for five devices.

About SlashNext

SlashNext protects the modern workforce from malicious messages across all digital channels. SlashNext's patented HumanAI™, a combination of computer vision, natural language processing, and behavioral contextualization, detects threats in real time with 99.9% accuracy. SlashNext Complete™ integrated cloud messaging security platform stops zero-hour threats in email, mobile, and web messaging apps across M365, Gmail, LinkedIn, WhatsApp, Telegram, Slack, Teams, and other messaging apps to detect and prevent threats before they become a breach.

Contact Us

 6701 Koll Center Parkway, Suite 250
Pleasanton CA 94566

 Contact Sales 1(800) 930-8643

 Start a Free Trial <https://www.slashnext.com/free-trial-request/>