Dashlane State of Credential Security Report

How AI and the Evolving Workforce Amplify the Threat of Credential Breaches

DASHLANE

Table of contents

Introduction

The daunting challenge in a shifting cybersecurity landscape

As businesses face the growing challenges of an AI-driven world, the landscape of cybersecurity threats has shifted dramatically, with hybrid work adding another layer of complexity.

Artificial intelligence (AI) has intensified risks to password security, enabling large-scale yet highly effective phishing attacks that bypass traditional defenses, such as rule-based threat detection. Meanwhile, changes in workplace behavior, including the mixing of personal and professional devices, have widened the attack surface for hackers. Shadow IT further expands vulnerabilities within businesses.

IT leaders now face the daunting challenge of managing these escalating threats. They are balancing the demands of training, organizational changes, and compliance requirements—all while confronting the growing risk of a breach.

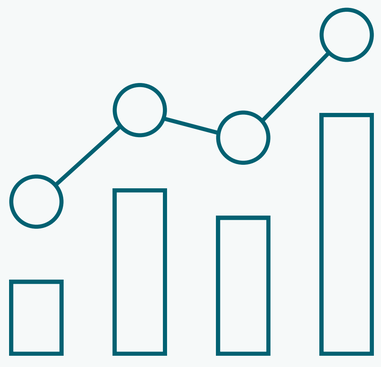
“Credential security is truly at an inflection point right now,”

says Dashlane Chief Technology Officer Frederic Rivain. “The average employee can face several phishing attempts in just one day, and IT teams need the tools to monitor, support, and empower employees to mitigate risks. And while the passwordless future promises to remove much of the risk and pain felt because of passwords, we’re not there yet.”

Recognizing the limitations of traditional approaches, many IT teams are urgently seeking more comprehensive, proactive solutions to address these growing risks.

To understand how the burden of credential management affects IT teams, we surveyed both employees and IT leaders. This report, based on those surveys, examines the state of credential security across organizations. We also discuss how password managers need to evolve from passive to proactive risk detection to prevent data breaches and support IT teams and their security counterparts.

Methodology



Findings are based on a Dashlane-commissioned survey of a scientific random sample of 1,000 U.S.-based employed adults and 500 U.S.-based IT decision makers, conducted by DKC Analytics.

Section 1

AI-powered phishing: The imminent danger to your security

AI is enabling cybercriminals who want to access your organization's data. It now makes it easier than ever for these criminals to launch phishing and spear phishing attacks cheaply and on a mass scale. Attackers are using a new generation of phishing kits, including those leveraging tools such as EvilProxy and incorporating large language models and generative AI, to send highly personalized, convincing messages. These kits also use advanced tactics, including deepfakes and AI-generated content, to carry out increasingly sophisticated scams.

IT leaders and employees report that this rise in AI and the subsequent sophistication of phishing attacks have increased the risk to credential security:

74%

of IT leaders say AI poses an increased threat to password security

60%

of employees agree that AI poses an increased threat to password security

Our data also reflects the growing threat of phishing:

88% of **employees** say phishing attempts targeting their organization are on the rise

80% of **IT leaders** say phishing attempts targeting their organization are on the rise

84% of **IT leaders** report an increase in phishing volume, sophistication, or both

Section 2

Traditional approaches to security strategies fail the modern workforce

Traditional security strategies, built around protecting a well-defined network perimeter and utilizing security training as a core means of defense, are failing in the modern workplace.

Remote and hybrid work continue to reshape the cybersecurity landscape, introducing new risks as employees blur the lines between personal and work devices. The expanded attack surface—driven by weak password practices and unsecure home networks—has created a perfect storm for cybercriminals.

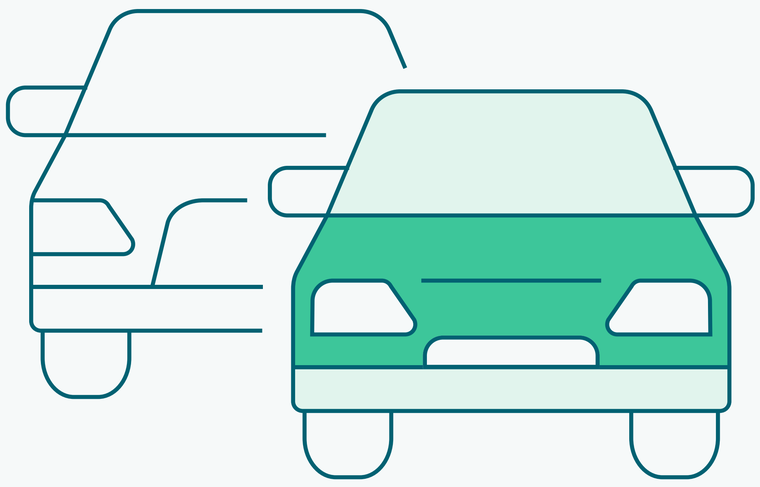
Employees often connect to enterprise systems from unsecure Wi-Fi networks. Many of these networks lack proper security measures like updated routers, VPNs, or strong passwords. With no clear perimeter to defend, organizations now face a significantly more complex challenge in protecting themselves.

Security awareness and training programs are common tools for mitigating human risk, including phishing, and enterprise companies invest a lot of time and money into them—but employees do not see the same value in these training sessions.

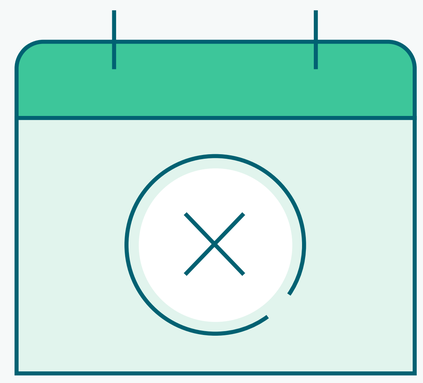
A company with 1,000 employees could spend $12,000 to $24,000 annually on basic online training. Larger enterprises (10,000+ employees) could see costs in the hundreds of thousands or even millions annually, especially if they use in-depth training, phishing simulations, and compliance-focused education.

Added security training also gets in the way of productivity. 57% of our surveyed IT leaders say that employees see security training as a burden.

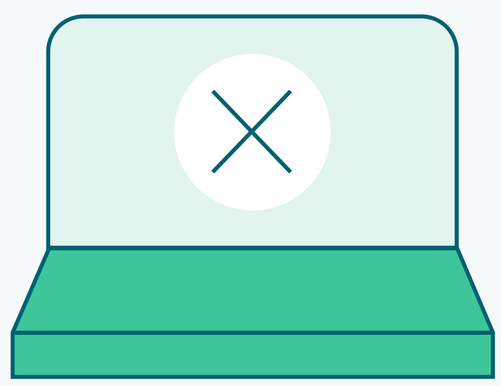
43% of employees would take extreme measures to avoid security training



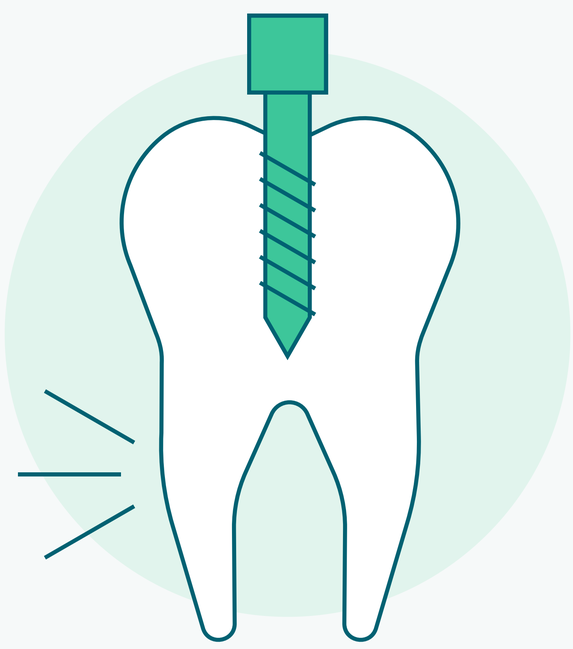
22% | would rather be stuck in a long line of rush-hour traffic



15% | would give up a vacation day to avoid the training



13% | would prefer to give up using computers altogether if that gets them out of training

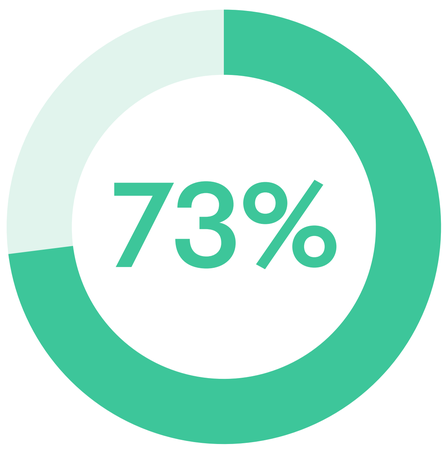


11% | Would rather have a root canal than attend training

IT leaders agree: 51% think employees at their organization see security training as a burden. This alignment is a clear sign that security training is not achieving the desired outcomes in protecting organizations from human vulnerabilities.

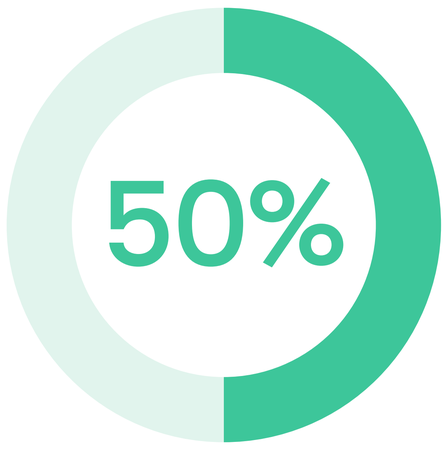
IT leaders report three common password issues

Employees' poor password hygiene amplifies the risks. Nearly all IT leaders (96%) report having to deal with credential-related issues. The three most common issues are:



Employees forget passwords and/or need a password reset

Employees create weak and vulnerable passwords



Employees share passwords using unsecured methods (such as Slack or email)

These poor habits lead to tangible losses. IT leaders say their organizations suffered intellectual property theft due to weak or compromised passwords (37%), while compromised accounts have resulted in stolen money (19%).

Password-related issues not only expose organizations to security breaches but also lead to significant operational costs. Forrester Research estimates that each password reset costs around $70, factoring in IT staff time and productivity losses. Additionally, up to 40% of help desk calls are related to password issues, which creates a substantial support burden. Employees also spend an average of 11 hours annually on password resets, further impacting their productivity. As a result, organizations spend an estimated average of $5.2 million annually on password-related support and infrastructure.

Section 3

Shadow IT: The hidden risk to your organization's security

Shadow IT creates significant risk for organizations. The problem is even bigger as employee adoption of generative AI tools skyrockets. These tools are especially risky because they connect to a lot more systems and apps within an enterprise and can process massive amounts of sensitive information.

This risk isn't going away. Some of these apps empower employees to be more productive and help the business achieve its goals.

Our data shows that the threat of shadow IT is real:

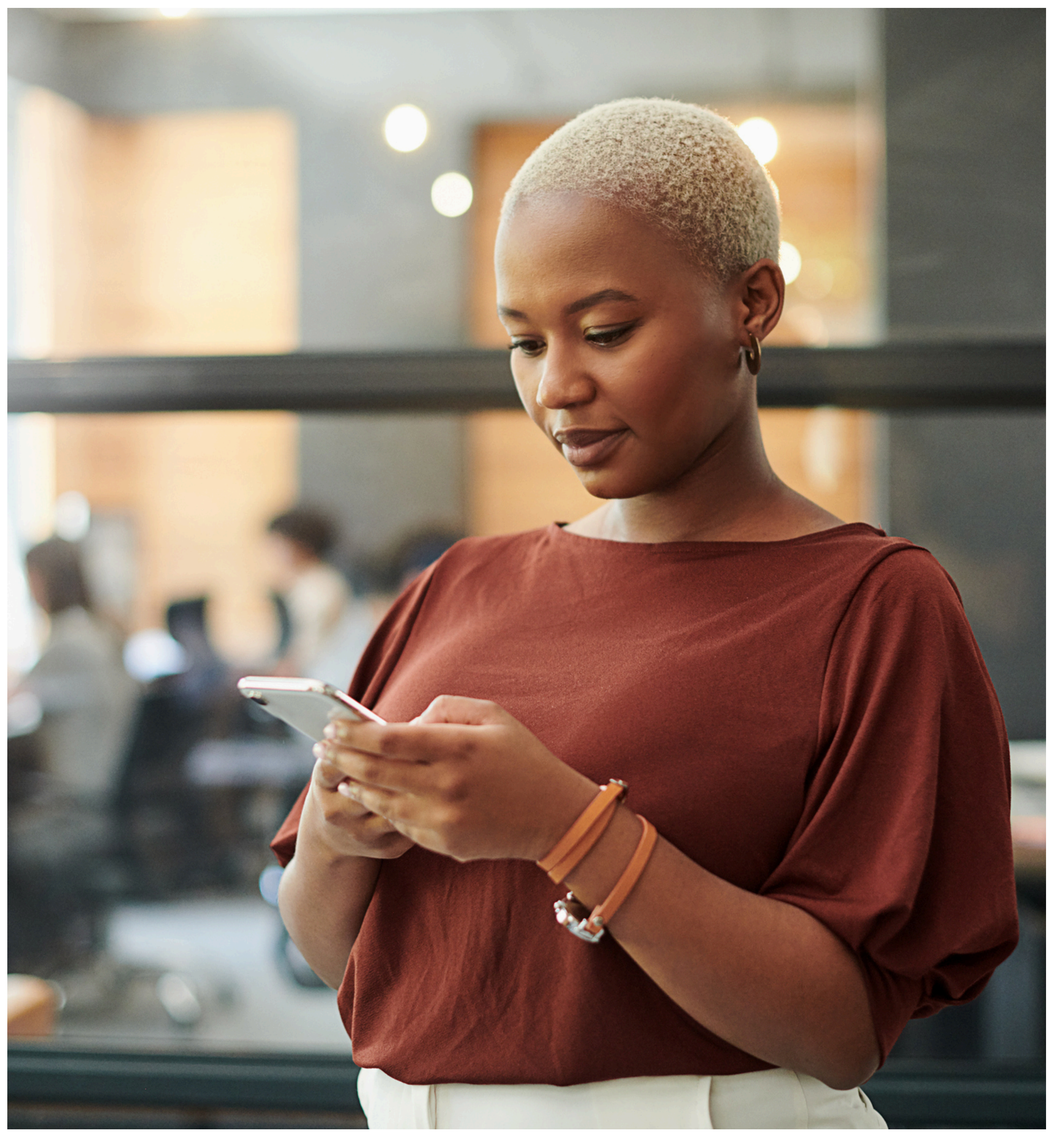
39%

of employees use apps not managed by their company on work devices

37%

of their corporate apps are not behind single sign-on (SSO)

Shadow IT creates numerous problems, including an increased attack surface and potential compliance violations.



Without visibility into the devices, apps, and services that access corporate resources, IT teams can't secure company data and ensure that only authorized users are accessing sensitive information and systems. This fragmented visibility makes it difficult to detect external and insider threats.

Consequently, shadow IT ultimately leaves organizations vulnerable to cyberattacks and data loss or compromise. However, the potential damage goes far beyond financial losses, including reputational damage that may take a lot of time and resources to repair.

Section 4

The burden of credential security falls on overwhelmed IT teams

Burnout has become an epidemic among IT teams. Research shows that 58% of IT practitioners report being overwhelmed by their daily job responsibilities and tasks. Additionally, the average IT worker reports having the capacity to support only 85% of the tickets received each day.

Our data shows that manual credential management adds greatly to this burden. As noted earlier, 96% of IT leaders say they have to deal with credential-related issues, with password resets and weak passwords being the most common problems.

The time drain due to these issues can be substantial, contributing to burnout. More than three-quarters (78%) of IT leaders say their teams deal with employee password issues at least weekly. For 28%, password problems come up daily or even multiple times a day.

Additionally, IT teams face other burdens related to their work: Running training sessions, adapting processes to organizational changes, meeting executive expectations, addressing the threat of breaches, and more. Add to that the mounting credential risks and the fallout from employees' aversion to security training, and it's easy to see why IT teams are overwhelmed.

96% of IT leaders say they have to deal with credential-related issues

78% of IT leaders say their teams deal with employee password issues at least weekly

28% of IT leaders say password problems come up daily or even multiple times a day

"Burnout amongst IT leaders has been an issue for years," says Rivain. "This problem is only going to get worse with the threat of AI-powered phishing attacks."

Conclusion

New solutions for new challenges

Empower IT teams to detect and respond to credential threats

As we work toward a passwordless future, the next evolution in securing credentials and supporting IT teams is proactive credential security, which provides full visibility into potential vulnerabilities and alerts admins to risky behavior—without requiring additional staff or resources.

This approach provides IT teams with real-time, actionable data so they can:

- Detect hidden threats like shadow IT and risky human behaviors stemming from poor password hygiene
- Respond to threats automatically with in-context, in-the-moment prompting and training
- Protect their organization with a solution they can trust, and employees can embrace

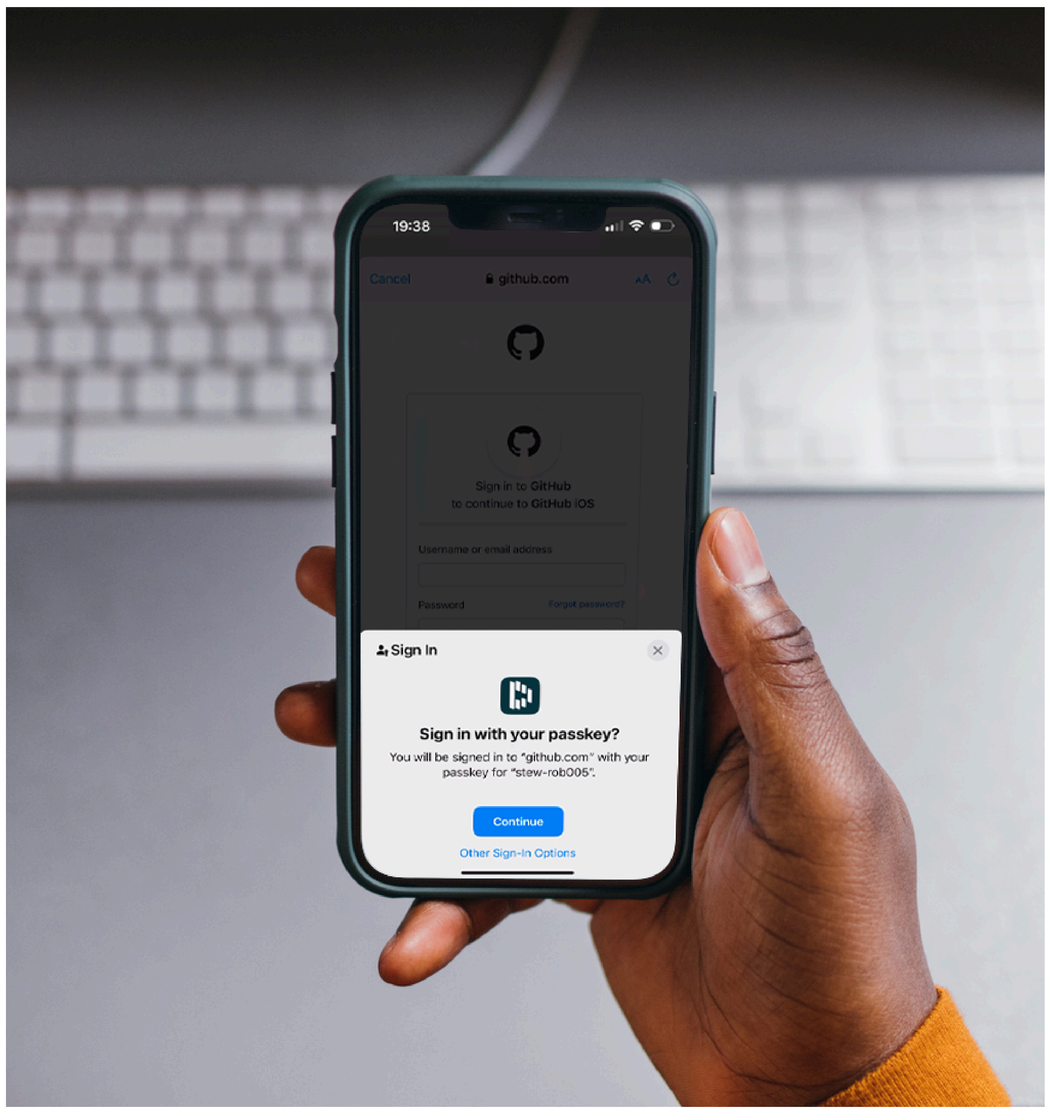
Credential security has reached an inflection point. It's clear that simply managing credentials is no longer enough—today's new challenges require new solutions. For IT leaders who want to gain real-time visibility into risky credential behavior across the organization and empower their teams to act quickly, proactive credential management is an opportunity for a paradigm shift.

"Good password hygiene isn't just going to happen," says Dashlane customer Abhilash Rajan, Senior Director of Technology, Systems, and Facility Operations at New America. "You need the tools to support it."

Passwordless: The key to building a phishing-resistant enterprise

The password is at the heart of many risks facing enterprises. It's also a burden felt by both admins and employees. Since it was first invented more than 50 years ago to protect a mainframe computer, the password has served as a poor security control that's subject to social engineering and credential-stealing malware.

Now, organizations are seriously considering what comes after the password. According to our report findings, 61% of IT leaders say their company will eventually go passwordless, with 16% of organizations already implementing some form of passwordless authentication. Most promisingly,



76%

of **IT leaders** say their C-Suite is pushing for passkey adoption,

illustrating how passwordless use by consumers is translating into awareness with enterprise leaders.

Despite the promise of a more secure and simpler passwordless future, businesses may never eliminate passwords entirely due to the complexity of enterprise environments. The need for a comprehensive, multi-layered approach to mitigating credential risk is imperative.

"It's easy to blame employees when incidents happen," says Rivain. "But shouldn't we instead blame the poor technology that opens employees up to risk in the first place?"

Explore Dashlane's proactive credential security platform to learn how our solution can help address your organization's credential security and human risk challenges.

About Dashlane

Dashlane is the leading credential security platform that secures access and proactively protects against breaches. Over 24,000 brands worldwide, including Air France, Forrester Research, and Sephora, trust Dashlane for industry-leading innovations that keep them ahead of evolving threats. The company pairs patented, enterprise-grade security with consumer-grade design in a top-rated platform, empowering everyone to be part of the credential security solution.

Visit dashlane.com/blog for more resources, digital security tips, and Dashlane product news.

DASHLANE

Visit dashlane.com