DASHLANE

PASSWORD MANAGEMENT 101

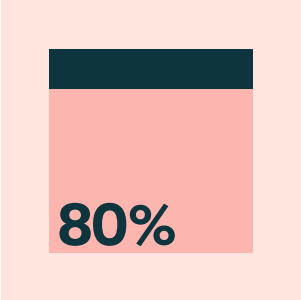
WHY PASSWORDS ARE THE WEAK LINK IN COMPANY SECURITY

CALL IT THE PASSWORD PARADOX

PASSWORDS WERE ORIGINALLY DEVELOPED AS A SIMPLE WAY TO SAFEGUARD SENSITIVE INFORMATION. YET THEY NOW REPRESENT THE SINGLE BIGGEST THREAT TO DATA SECURITY.

The increasing frequency of cybersecurity incidents shows no signs of abating. Fifty-nine percent of global organizations report they experienced a significant data breach over the past 12 months, a 9% jump over the year before, according to consulting firm EY.[1] Significantly, stolen passwords and user credentials account for the most frequent — and costly — incidents.

In total, more than 80% of all hacking-related data heists involve the use of stolen credentials or passwords, according to the Verizon Data Breach Investigations Report (DBIR) 2020.[2] Among cybercriminals, the go-to technique for stealing credentials is social engineering scams like phishing. More than half (51%) of businesses say they experienced a phishing attack in the past year, which makes phishing by far the most common type of incident, according a study by the Ponemon Institute.[3]



In total, more than 80% of all hacking-related data heists involve the use of stolen credentials or passwords.

Verizon, Verizon Data Breach Investigations Report, May 2020

These security incidents frequently carry hefty price tags. Globally, the average total cost of a data breach is $3.86 million.[4] [5] And costs are even higher among organizations that were attacked through the use of stolen or compromised credentials.

This type of incident raised the average cost of a breach to $4.77 million, a 24% premium compared with all data heists, according to Ponemon.

It seems all but certain that security incidents attributed to weak passwords will continue to mount. Consequently, businesses should be prepared to integrate password management solutions into their IT security stack.

WHAT ARE PASSWORD MANAGERS?

PASSWORD MANAGERS HELP USERS GENERATE AND STORE STRONG, SECURE PASSWORDS THAT CAN BE SYNCHRONIZED ACROSS MULTIPLE DEVICES, WHETHER DESKTOP OR MOBILE.

Password managers typically offer spaces for employees to separate personal and business credentials to help ensure employees don't leak or leave with sensitive business information and intellectual property. The best password managers also help IT monitor and measure security performance by creating a security score based on metrics like password reuse across business and personal accounts. Password managers free employees from having to remember (or write down) dozens of passwords. They also enable co-workers to securely share passwords, lessening the likelihood of a data breach.

TYPES OF CYBERATTACK EXPERIENCED

51%	**Phishing**
16%	**Ransomware**
12%	**Credential theft**
8%	**Man-in-the-middle attack**
13%	**Do not know**
32%	**Haven't experienced cyberattacks**

Ponemon Institute, The 2020 State of Password and Authentication Security Behaviors Report, February 2020

DATA BREACH COSTS ADD UP

Data breach cost calculations typically include expenses related to incident response and remediation, legal counsel, forensics, audit services, regulatory fines, and lost revenues. Another financial consequence stems from reputational damage, which can create subtle, yet potentially ruinous, impacts that are difficult to accurately appraise.

Consider, as an example, the recent attack on Twitter. A team of youthful amateur hackers, including a 17-year-old boy, allegedly used social engineering to gain control of an internal support tool for the social media platform.[6] Doing so enabled the budding criminals to commandeer more than 130 accounts, including those of high-profile elites and celebrities like Elon Musk, Barack Obama, Joseph R. Biden, Bill Gates, and Kanye West, to name a few.

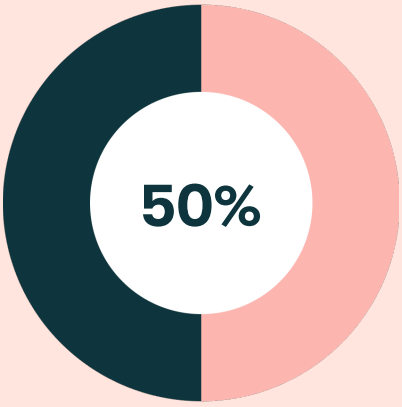
The hackers tweeted a series of messages that encouraged followers to make Bitcoin deposits that account owners would double and return to the email respondents. The tweets were comparatively harmless but could have been calamitous had the hackers posted politically or socially inflammatory content that might spur individuals, and even nation states, to action. The impact to Twitter, meanwhile, was essentially a very visible slap to its reputation at the hands of young, inexperienced troublemakers.

A WHOLE NEW WORLD OF RISKS

Over the past decade, organizations have plotted an often-scattershot path toward a world where previously uncommon digital tools and services are commonplace. This digital transformation has become significantly more urgent, however, as more people work from home or live in geographically dispersed areas.

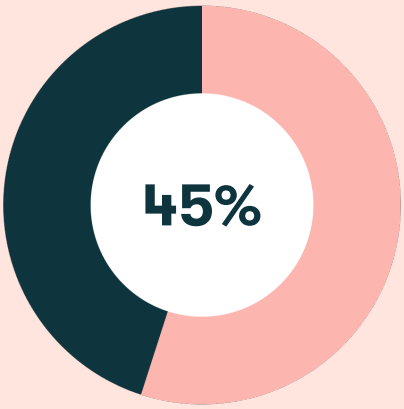
Among U.S. employees who are working from home, more than half (57%) say they are using new or more technically advanced products and services. These include tools for video conferencing, VPNs, anti-malware protection, password managers, and online banking and grocery shopping, according to a survey by Dashlane.[7] Compounding risks, more than half of home-bound employees are using personal devices and equipment to access business systems. Yet only 45% employ multi-factor authentication when they log in to work apps on their mobile device.[8] Similarly, just 45% of businesses say they have taken steps to protect information stored on employees' phones and devices.[9]

The best defense against today's heightened cyber-risks is up-to-date security safeguards. These include strong password policies, secure and tested remote-access connectivity (VPNs), multi-factor authentication, and deployment of anti-malware and intrusion-prevention software. Equally critical is employee training and awareness that focuses on email-based techniques like phishing and ransomware, as well as threats that are specific to the particular business and industry.



of IT security staff reuse passwords for workplace accounts

Ponemon Institute, The 2020 State of Password and Authentication Security Behaviors Report, February 2020



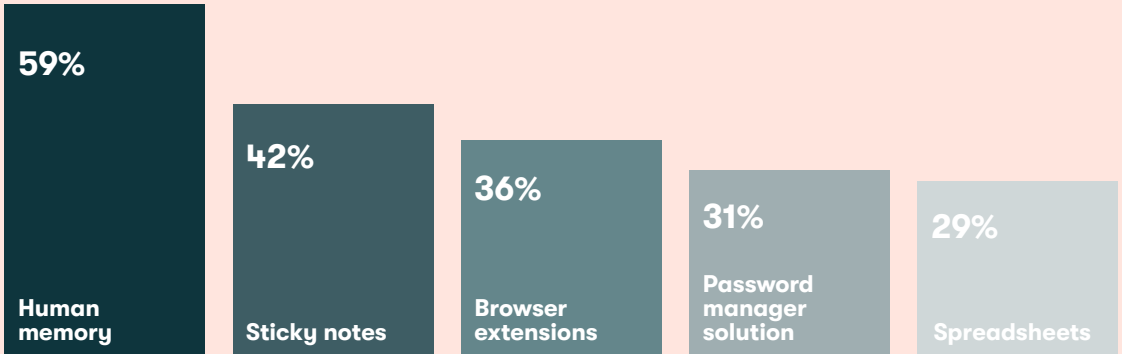
of businesses say they have taken steps to protect information stored on employees' phones and devices

Ponemon Institute, The 2020 State of Password and Authentication Security Behaviors Report, February 2020

Employees sharing passwords via unsecure processes such as email, sticky notes, or an Excel document stored on the network adds to the list of risks. Password sharing can make data more vulnerable to attacks and obfuscate the audit trail, which can hinder investigations of security incidents. Other people-generated risks include changing a shared password without notifying others and theft of enterprise passwords by disgruntled employees who have one foot out the door.[10]

HOW COMPANIES MANAGE PASSWORDS

Ponemon Institute, The 2020 State of Password and Authentication Security Behaviors Report, February 2020



At the same time, the migration of applications and workloads to the cloud has compounded security vulnerabilities. In general, cloud services provide sophisticated security technologies and practices that exceed the capabilities of most small- and medium-size companies.

But certain risks exist in the cloud. In fact, Verizon found that 77% of cloud security incidents were attributed to the use of stolen cloud credentials.[11] Each cloud application requires login credentials, which are often shared or reused among admins and other IT employees. If a single password is compromised, hackers can more easily gain access to other services and systems that use the same or similar credentials.

THE ADOPTION AVERSION PROBLEM

Despite steadily rising risks and costs associated with password-related security incidents, IT leaders may find it difficult to justify the time and costs needed to implement a password management solution. Here are the four most common roadblocks to the adoption of password managers.

1. **INITIAL VALUE COMPREHENSION**

It's challenging to quantify the value of certain security technologies because business leaders cannot accurately predict the likelihood, extent, or cost of a data breach. Often, the deciding factor in deploying a password management solution is a breach to the organization itself or high-profile attacks on industry peers. Ponemon, in fact, found that 65% of businesses updated password management capabilities only after an attack.[12]

2. **RISK OF PROJECT FAILURE**

Another concern, one that most IT leaders know all too well, is the risk of project failure. In general, a fast and efficient software implementation elicits little response. But a problematic, disruptive deployment is likely to spark comments across the enterprise, from new employees to seasoned C-suite executives.

3. **SOLUTION ADOPTION**

Even the simplest implementations are not immune to resistance. Initially, some employees will find password managers frustrating to use, while others simply may not trust the technology. No matter the misgiving, user adoption is critical to success and is an initiative that warrants careful planning and employee training.

4. **EXECUTIVE BUY-IN AND SUPPORT**

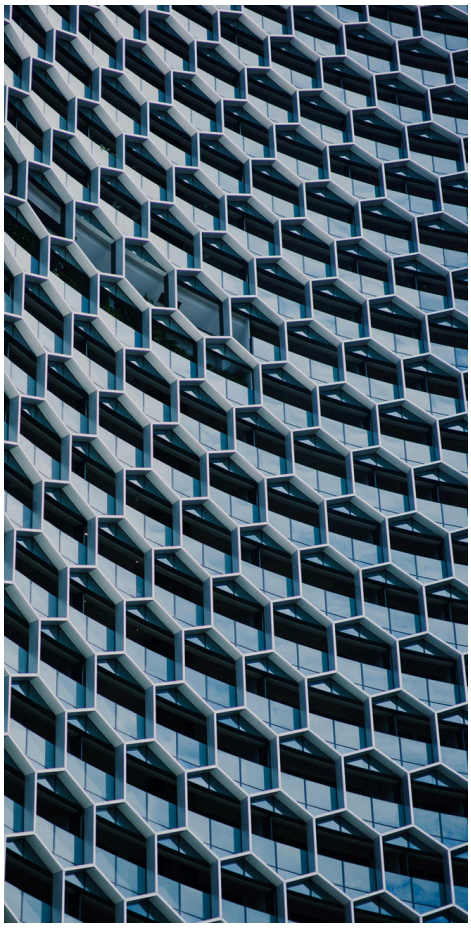
Another people-related challenge lies in obtaining buy-in and support from executive leaders and the board of directors. Security is an enterprise-wide risk-management effort; it requires proactive support that starts in the C-suite and cascades down to all divisions and employees.

WHAT TO LOOK FOR IN A PASSWORD MANAGER

Despite these barriers to password manager adoption, the key features of best-in-class solutions can help build a strong business case, ensure adoption, and support successful implementation. Password managers represent the first line of defense against unauthorized access and data breaches. As such, an effective password management solution must function seamlessly across device types, operating systems, and browsers.

The ability to create unique, complex passwords for each account and sync these passwords across multiple systems is a defining feature of password management solutions. Password management tools should allow users to easily save new credentials. They also should enable secure sharing of passwords among individuals or groups without transmitting them via unsecure platforms like email or instant messaging apps.

A capable solution can also help employees improve their password management knowledge and skills. A state-of-the-art password manager should rate the strength of user passwords and help identify and support best practices for creating more robust credentials. In general, strong password policies should:



- Use a mix of character types, such as at least one number, uppercase letter, and symbol
- Have a minimum of eight characters; longer passwords are less vulnerable to brute-force attacks
- Avoid words that can be found in a dictionary, are variations on a user's name, or riffs on personal information such as the name of a child or pet

The storage of these passwords — either on premises or in the cloud — is a critical decision. IT leaders should balance the pros and cons of each method to better align password management tools with existing security systems and processes. While there's no universal approach, a password manager that offers a choice between cloud and local storage can provide enhanced flexibility.

Best-in-class password protection solutions use zero-knowledge architecture that syncs encrypted data in the cloud and decrypts it on the user's local device. Passwords

saved in a zero-knowledge architecture allow the business to evaluate the strength of any password without actually knowing any information about the password itself. What's more, a zero-knowledge approach limits access to data encryption keys to the business; the service provider cannot access encryption keys and therefore cannot access stored data.

BUSINESS BENEFITS OF PASSWORD MANAGERS

- No need to memorize passwords
- Guarantees secure, complex, passwords
- Allows groups to securely share passwords
- Enhances employee productivity
- Early alerts to data breaches
- Saves on help desk costs
- Offers insight into individual security posture
- Streamlines establishment and enforcement of password policies

Ponemon Institute, The 2020 State of Password and Authentication Security Behaviors Report, February 2020

Organizations that opt for local storage should understand that the company is ultimately responsible for the security of their local storage devices. That means businesses must be prepared to address any flaws in processes or technologies that could expose a security vulnerability. Cloud-based password management solutions, on the other hand, can take advantage of the security expertise of leading cloud providers. These include highly secure facilities, end-to-end encryption, protection against DDoS attacks, and detailed network activity logs and audit trails.

Whether on premises or in the cloud, a password manager should include self-service password reset and account recovery capabilities. Also critical is an account recovery feature that allows users to reset their master password and recover data stored on an authorized device.

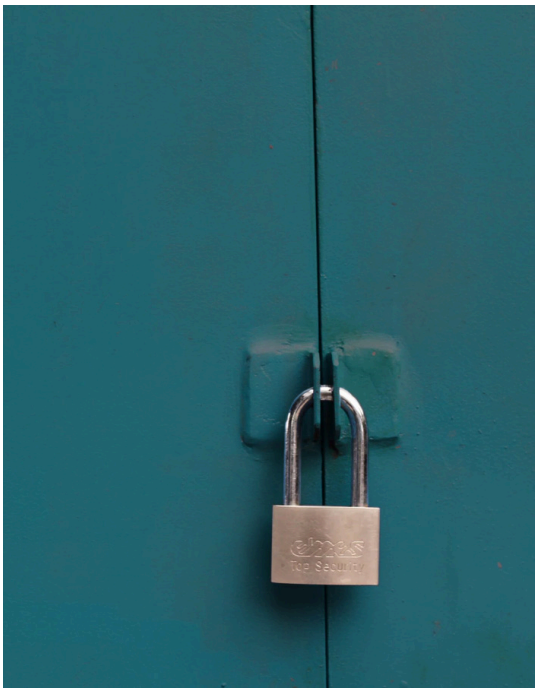
When choosing a password manager, remember that an intuitive user experience is critical to adoption. If employees think the security software is burdensome, they simply won't use it. Password management is among the strongest defenses against compromised business data and, as such, should not be weakened by inadequate user adoption.

Cybercriminals typically sell stolen customer data in the murky depths of the internet. That's why it's paramount that the password management solution is able to scan the dark web for credentials pilfered in previous breaches. The National Institute of Standards and Technology (NIST) recommends that businesses perform scans for exposed or compromised passwords against a list that contains values known to be commonly used, expected, or compromised.[13] This list should include passwords lifted in previous breaches, dictionary or common words, and context-specific words like the name of the company or username. If compromised company credentials are identified, the password manager should be able to send automatic alerts to users.

Other key features to look for in a password management solution include:

- Two-factor authentication (2FA)
- SAML-based provisioning
- SAML-based single sign-on (SSO)
- AES 256-bit encryption
- Public WiFi VPN
- Enterprise mass deployment

One more thing: Businesses must be prepared to perform thorough due diligence on potential password management vendors to ensure their digital infrastructure and data have not been breached or compromised.



PRIORITIZE PASSWORD PROTECTION

Core IT security programs typically protect data by applying security controls to email servers, cloud configurations, antivirus software, firewalls, encryption, and VPNs, to name a few. But what about passwords, one of the weakest links in security programs? Today, only 31% of companies use a password management solution to protect data.[14]

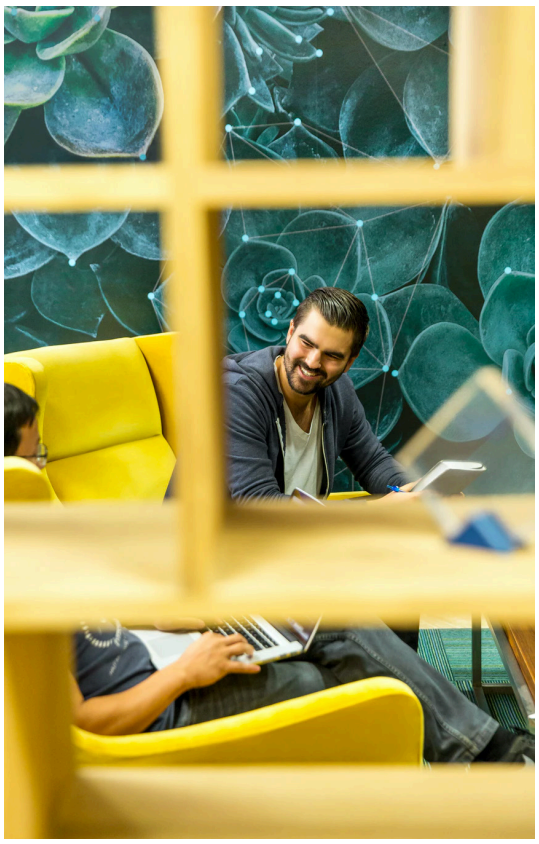
One explanation for this modest adoption rate is that it's often difficult to convince corporate executives like CFOs that password managers should be implemented as a core component of IT security. A successful conversation should weigh the potential disruptions and costs of a cybersecurity incident against the benefits of the password management system. Consider the following as starting points for a discussion with your CFO and other decision-makers:

- Point out increasing frequencies of email-based cybercrimes like phishing, ransomware, and business email compromise
- Discuss the average costs of cyberattacks in your industry, among peers, and by geography and company size
- Demonstrate how password management solutions can add value by freeing up IT admins and security teams to perform more strategic, forward-thinking work
- Discuss how a password management solution can kick-start employee productivity and job satisfaction
- Explain the importance of monitoring the dark web to help quickly identify and respond to theft of customer and employee data

It's also persuasive to mention that effective password management solutions offer centralized mass deployment that automates installation and provides software updates to help drive efficiencies and boost user satisfaction. Mass deployment is faster and more reliable than manual implementation, which is prone to human error. What's more, software updates and patches are immediately available to all, which can save time and money and ultimately yield higher user satisfaction and productivity.

THE KEY TO ADOPTION IS ENGAGED EMPLOYEES

Using a password manager may initially seem burdensome to some employees, particularly longtime workers who have committed tried-and-true methodologies to memory. Business executives and IT leaders must approach password management in context with real-world risks associated with password security and the criticality of adoption.



Secure password management is most likely to flourish in a corporate culture that prioritizes employee engagement and a proactive commitment to security. That's why it's critical to foster a sense of ownership and pride in participation. Employees must fully grasp the real-world consequences of poor cybersecurity hygiene, which can potentially entail millions of dollars in financial losses. Each employee, regardless of job title, must also know their singular role and responsibilities in the collective effort to protect data assets, applications, and networks.

TOTAL DATA PROTECTION

Inadequate password management has become a leading risk to data security, but it doesn't have to be. Dashlane, an advanced, easy-to-use business password management solution, simplifies and streamlines data protection.

The award-winning solution is built on a patented security architecture that integrates two-factor authentication, single sign-on, and AES 256-bit encryption. IT administrators can efficiently onboard new employees and manage password permissions from a centralized console. It also allows secure sharing of encrypted passwords and other information among employees. Dashlane can help you protect valuable data from password-related security compromises and, ultimately, raise employee productivity and lower help-desk costs. As the frequency and financial impacts of data breaches continue to rise, password management should be considered an integral component of IT security — and a top security priority.

For more information on how Dashlane can help you or your organization manage passwords:
Sign up for our 30-day trial or visit dashlane.com/business.

---

[1] EY, Global Information Security Survey 2020, February 2020
[2] Verizon Enterprise, Verizon Data Breach Investigations Report, May 2020
[3] Ponemon Institute and IBM Security, Cost of a Data Breach Report 2020, July 2020
[4] Ibid.
[5] It's worth noting that the U.S. holds the dubious distinction of having the highest data breach costs of any nation in the world: $8.64 million, according to the Ponemon IBM study.
[6] The New York Times, Florida Teenager Is Charged as 'Mastermind' of Twitter Hack, Sept. 1, 2020
[7] Dashlane, New Dashlane Survey: Majority of Americans Feel More at Risk Online Due to COVID-19, April 29, 2020
[8] Ponemon Institute, The 2020 State of Password and Authentication Security Behaviors Report, February 2020
[9] Ibid.
[10] Ibid.
[11] Verizon Enterprise, Verizon Data Breach Investigations Report, May 2020
[12] Ibid.
[13] National Institute of Standards and Technology, NIST Special Publication 800-63B
[14] Ponemon Institute, The 2020 State of Password and Authentication Security Behaviors Report, February 2020

ABOUT DASHLANE

Dashlane offers businesses a password management solution that is as easy to use as it is secure. Admins can easily onboard, offboard, and manage employees with the assurance that company data is safe. And employees can manage their work and personal accounts using a solution that is enjoyed by millions of users. Our teams in Paris, New York, and Lisbon work together to improve the digital experience and ultimately help realize the promise of the internet. Dashlane has empowered more than 15 million users and over 20,000 companies in 180 countries to dash across the internet without compromising on security.

dashlane.com

- LinkedIn
- Twitter
- Instagram
- Blog