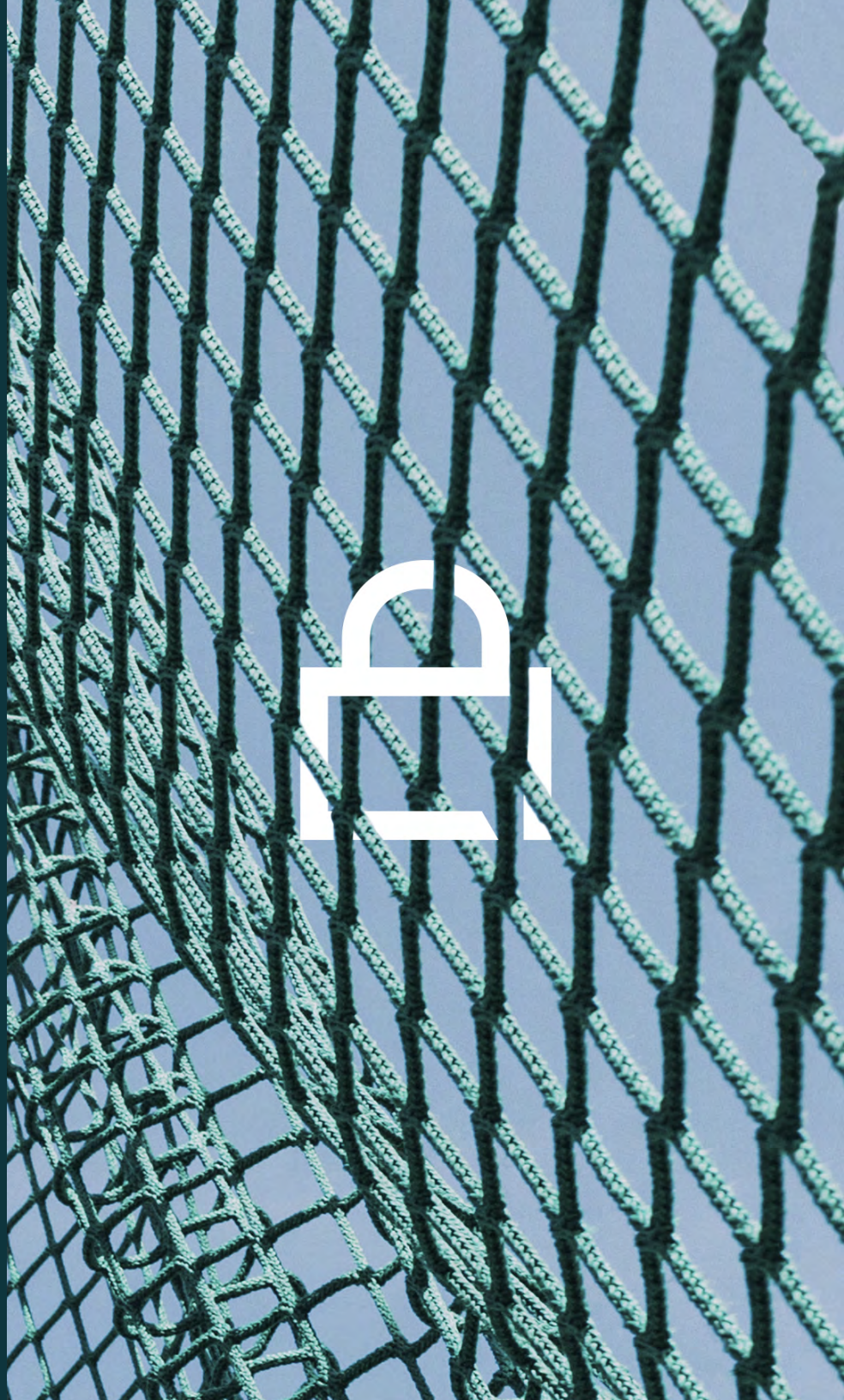
DASHLANE

HOW TO SAFEGUARD SENSITIVE DATA FOR BUSINESSES

ALL YOU NEED TO KNOW ABOUT THE BENEFITS AND FEATURES OF PASSWORD MANAGERS



WHAT'S INSIDE

SECTION 1:

INTRODUCTION

PASSWORDS ARE AS UBIQUITOUS AS EVER. AND PEOPLE STILL USE WEAK PASSWORDS. EVEN AT WORK.

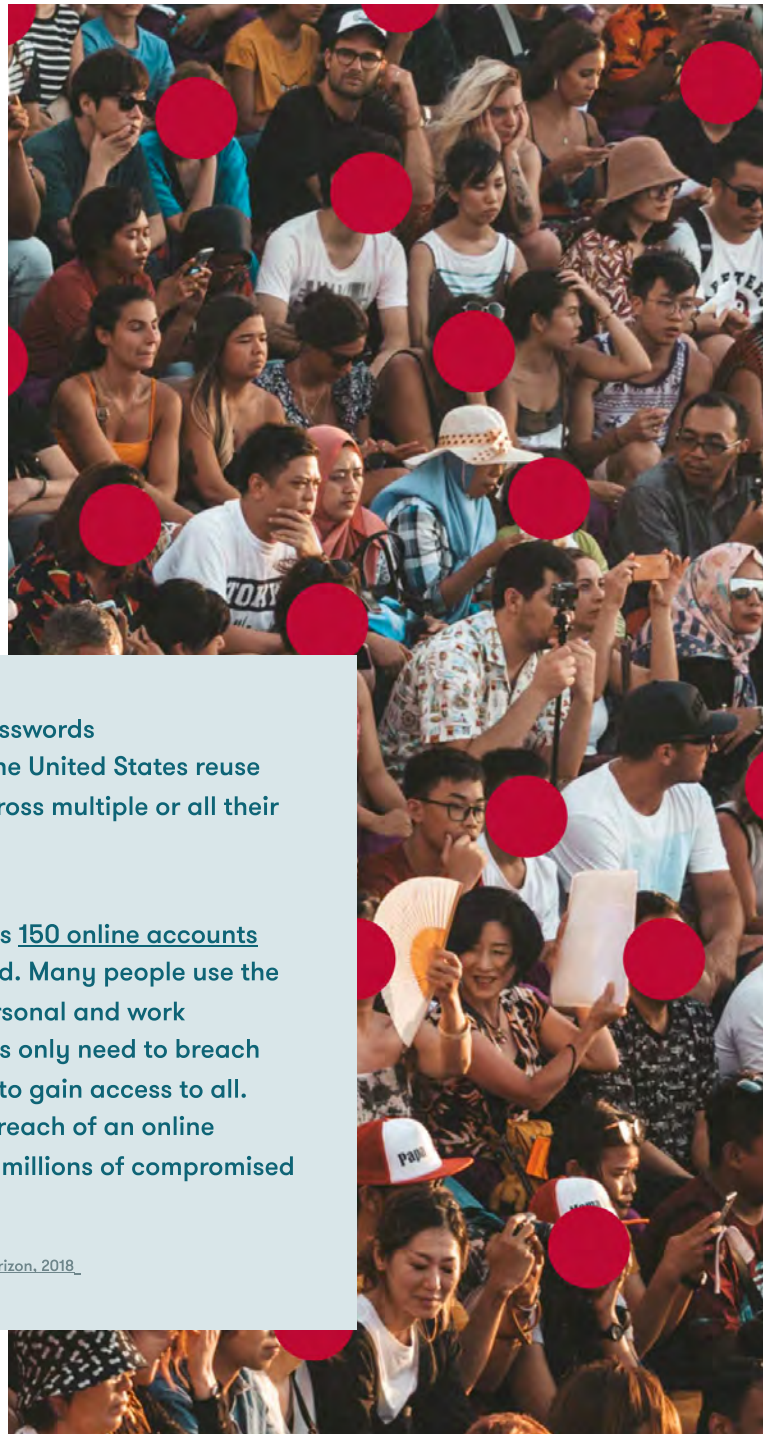
NO WONDER WE NEED STRONGER SECURITY MEASURES.

BACK IN 2004, BILL GATES SAID AT AN RSA CONFERENCE THAT "OVER TIME, PEOPLE ARE GOING TO RELY LESS AND LESS ON PASSWORDS."

Despite the former Microsoft chairman's prediction about their demise, passwords are as ubiquitous as ever. In fact, one estimate shows that the "universe of passwords" will grow to 300 billion passwords by 2020, up from 90 billion in 2017.[1]

Password security, on the other hand, has not kept up with this growth. Use of stolen or brute-forced credentials is the cause of more than 80% of hacking-related breaches.[2] Poor password security practices, including weak and reused passwords, are an invitation to hackers looking for an easy way in.

Implementing a password manager is an easy, convenient, and secure way to protect your organization's access to online assets and accounts. In this guide, we'll break down what features you should consider and how to ensure a successful rollout.



The perils of reused passwords
70% of individuals in the United States reuse the same password across multiple or all their accounts.[1]

The average person has 150 online accounts that require a password. Many people use the same password for personal and work accounts—and hackers only need to breach one of those accounts to gain access to all. Just one high-profile breach of an online service provider yields millions of compromised passwords.

1. Source: U.S. Data Breach Report, Verizon, 2018

1. "The World Will Need to Protect 300 Billion Passwords by 2020," Cybersecurity Ventures, 2018
2. 2020 Data Breach Investigations Report, Verizon, 2020

THE GROWING RISKS IN A CONNECTED WORLD

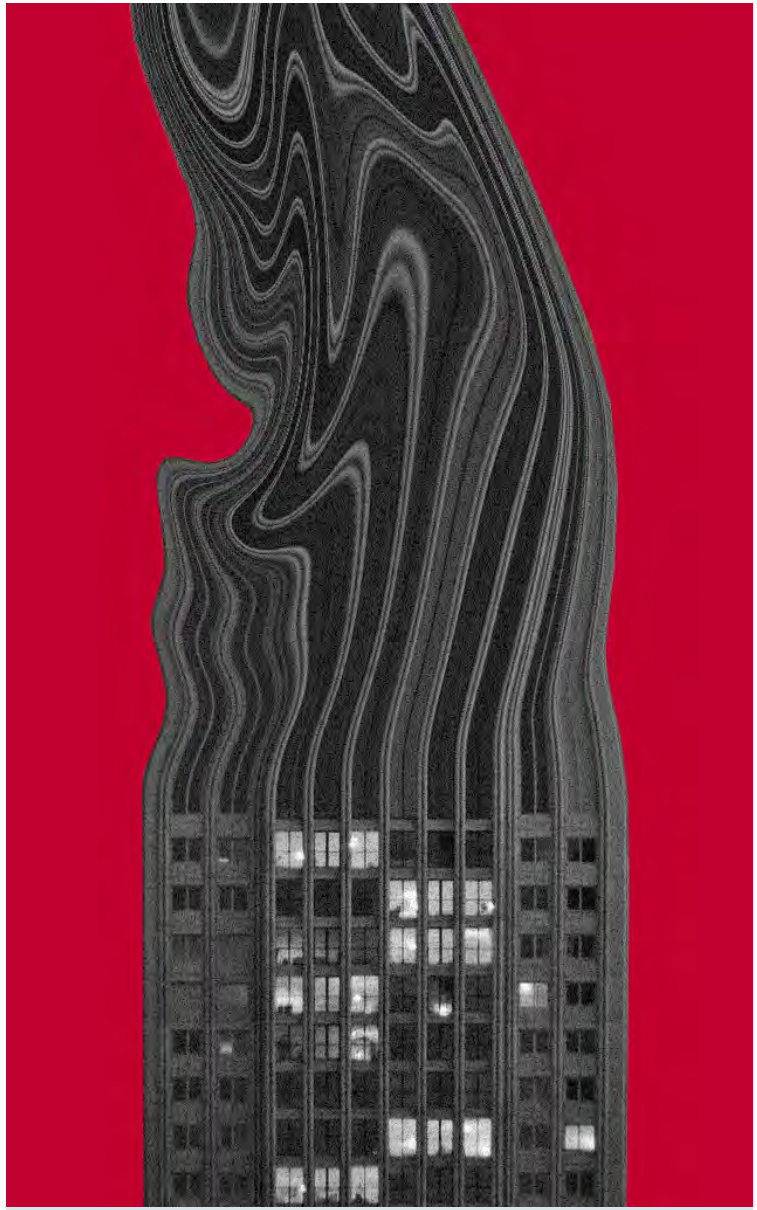
A growing remote workforce. More devices and apps. A distributed network. Today's always-connected world places new demands on your ability to protect and secure sensitive data. And in the digital economy, competitive differentiation requires continuous innovation — but 80% of organizations are pursuing digital innovation faster than they can improve their security practices to defend against cyberattacks.[3]

As their frequency and damage have grown, cyberattacks have climbed to the top of business risks globally.[4] The risks will continue to grow with the rapid shift to remote work environments where:

- Reliance on remote-access solutions adds new vulnerabilities
- Employees may be more susceptible to phishing and social engineering
- Employees may be accessing your organization's data and accounts from unsecured personal devices

Many leaders at small and medium businesses (SMBs) view passwords as one of their first lines of defense against data breaches. But consider how many breaches are related to compromised passwords. Although organizations pour an increasing amount of money into cybersecurity, compromised credentials continue to be a weak spot.

3. Ninth Annual Cost of Cybercrime Study, Accenture, March 2019
4. Allianz Risk Barometer 2020



80% of organizations are pursuing digital transformation and digital innovation faster than they can improve their security practices to defend against cyberattackers

Source: Ninth Annual Cost of Cybercrime Study, Accenture, March 2019

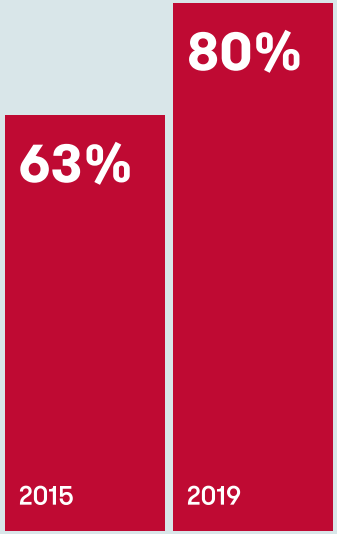
SECTION 2:

PASSWORDS: THE WEAKEST LINK

PASSWORDS ARE THE PATH OF LEAST RESISTANCE FOR CYBERCRIMINALS.

Why should they try to force their way into your IT environment when they can simply log in? And many security solutions are only designed to detect intrusions; once attackers are inside, it takes an average of 280 days to identify and contain a data breach.[5]

Among confirmed 2019 breaches, the use of stolen credentials was the No. 2 threat action (after phishing), according to Verizon's 2020 Data Breach Investigations Report.[6]



"USE OF CREDENTIALS HAS BEEN ON A METEORIC RISE."

Hacking-related breaches due to weak, stolen, or default passwords

2020 and 2016 Verizon Data Breach Investigations Report

A variety of internal or external factors could end up exposing your corporate passwords. Here are three of the most common causes behind compromised information.

1. Weak credential storage and sharing: Sharing passwords via Slack or email. Storing them in plain text in unsecure Excel spreadsheets or cloud databases. These are some of the many risky protocols organizations still use to manage their user credentials.

2. Malicious or careless insiders: The frequency of insider-related incidents has tripled since 2016 — and credential theft is the costliest type of inside threat (per incident).[7]

3. Hacking: Malware, unsecure connections, and brute-force attacks — where an attacker may submit multiple passwords or passphrases with the hope of eventually guessing correctly — are just a few of the tools in the bad actors' arsenal for stealing passwords. Among malware varieties, "password dumpers" — used to steal credentials — were in the top spot in 2019, involved in about 40% of confirmed breaches.[8]

5. Cost of a Data Breach 2020, IBM Security
6. 2020 Data Breach Investigations Report, Verizon, 2020
7. Cost of Insider Threats Global Report, IBM Security, 2020
8. 2020 Data Breach Investigations Report, Verizon, 2020

IN THE WILD: THE EVOLUTION OF TRICKBOT

In the last couple of years, malware has shifted focus from consumers to businesses. TrickBot is among the most common malware families targeting companies.

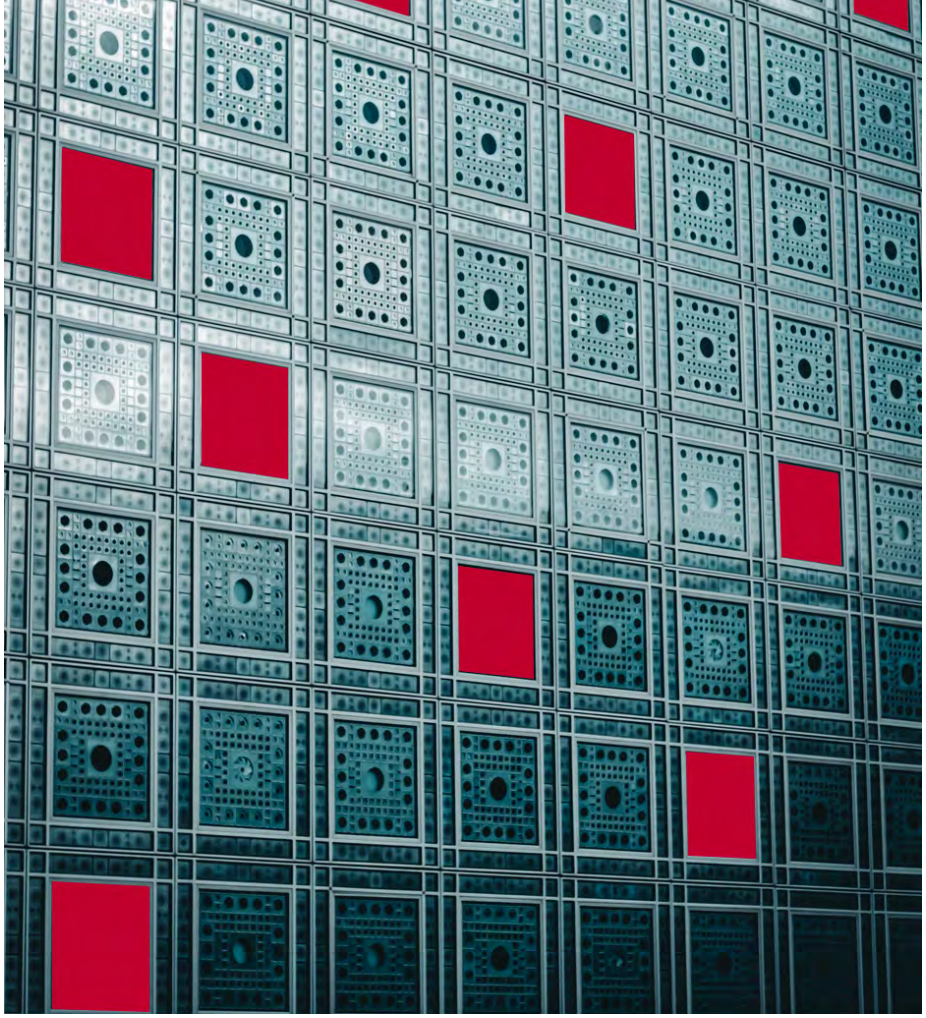
Originally a banking Trojan, TrickBot has evolved to steal other types of credentials, including email addresses. Newer variants can also:

- Steal website browser credentials and use them to authenticate account access
- Steal credentials from remote access platforms such as Remote Desktop Protocol (RDP) and Virtual Network Computing (VNC)
- Sidestep multifactor authentication

Security researchers believe that TrickBot is responsible for compromising more than 250 million email accounts alone.[1] In 2019, Malwarebytes saw a 52% increase in TrickBot detections among business customers.[2]

Bad actors often distribute TrickBot via phishing, but the malware can also get into a network by using EternalBlue exploits and gaining admin access through brute force.

1. "Trickbooster: TrickBot's Email-Infection Module," Deep Instinct, July 2019
2. 2020 State of Malware Report, Malwarebytes Labs, February 2020



MISCONFIGURATIONS: A COMMON CULPRIT

EIGHTY-SIX PERCENT OF RECORDS COMPROMISED IN 2019 WERE DUE TO MISCONFIGURED SERVERS.[1]

NEARLY 34 MILLION RECORDS WERE EXPOSED IN THE TOP FIVE UNSECURE DATABASE BREACHES ALONE IN 2019. FOUR OF FIVE OF THE BREACHES EXPOSED USER CREDENTIALS.[2]

1. X-Force Threat Intelligence Index 2020, IBM
2. 2019 End-of-Year Data Breach Report, Identity Theft Resource Center)

THE DARK WEB MARKETPLACE

Cybercriminals may not even have to hack your IT environment to take over your user accounts. Other bad actors do the dirty work of stealing passwords and making them available on the dark web. The dark web functions like an underground economy, with an abundance of stolen user accounts available for sale or lease — including credentials of privileged users such as IT admins.

Some cybercriminals even give away compromised passwords for free. Researchers have found more than 15 billion exposed credentials (from more than 100,000 breaches) being freely shared on the dark web.[9]

MITIGATING THE RISKS

The best way to protect your corporate accounts and sensitive data is by implementing a password manager. This solution does much more than securely store passwords. A password manager can:

- Make it easy for employees to follow best practices for passwords
- Give IT admins insights into the health of passwords across the organization
- Monitor the dark web for compromised personal information so you can protect your accounts

In addition to protecting your organization's data, password managers empower employees to be part of the solution rather than part of the problem. They also ensure that employees don't leave the company with corporate passwords and accounts.

9. "From Exposure to Takeover: The 15 billion credentials allowing account takeover," Digital Shadows, July 2020

BUSINESS EMAIL COMPROMISE GETS COSTLY

Business email compromise (BEC) is a much too familiar problem for IT pros. And according to the FBI, it's one of the costliest types of internet-enabled crimes. In 2019, BEC resulted in more than $1.7 billion in losses reported to the FBI in the U.S., or about half of all losses reported over the year.[1]

Account takeover (ATO)—where the bad actor impersonates the victim by getting direct access to the email account—is a common way of perpetrating BEC. A recent report found that BEC campaigns have been targeting business executives' Office 365 accounts through spear phishing, successfully compromising credentials of high-level employees around the globe.[2] Another report found that BEC attacks are bypassing multifactor authentication and other protocols[3], indicating that cybercriminals are growing more sophisticated.

1. "2019 Internet Crime Report Released," FBI, February 2020
2. "Water Nue Phishing Campaign Targets C-Suite's Office 365 Accounts," Trend Micro, August 2020
3. "How Attackers Bypass MFA and Conditional Access to Compromise Email Accounts," Abnormal Security, August 2020

SECTION 3:

HOW TO EVALUATE PASSWORD MANAGERS

NOT ALL PASSWORD MANAGERS ARE CREATED EQUAL

The marketplace for password management is robust, but not all solutions offer the same capabilities. When you're evaluating your options, consider the features beyond password storage that you'll need to round out your information security strategy.

FIVE FEATURES TO LOOK FOR IN A PASSWORD MANAGER

PASSWORD GENERATOR

This basic, built-in tool generates strong, unique, and randomized passwords. You should also be able to customize the generated passwords.

ADMIN DASHBOARD

Insights into employees' password security are critical. An admin dashboard should allow you to easily and efficiently monitor password health, view admin activity, set policies, manage users, and create and manage groups.

GROUP SHARING

This feature allows IT admins to securely share encrypted passwords and other sensitive information with user groups. When you email passwords, they are stored in plain text on the email servers or user devices — and this feature eliminates that risk, as well as the risk of employees leaving your company with passwords.

DARK WEB MONITORING

You need more than alerts about publicly known breaches. A tool that constantly scans the dark web for leaked personal data allows you to take immediate action to secure compromised accounts.

PASSWORD HEALTH

To help you establish a baseline for your password security, you need to understand your security score. The score should take into account factors such as weak, reused, and compromised passwords. Look for a solution that provides scores across the organization for admins as well as individual scores for users, both for personal and business accounts. Since many people reuse passwords for personal and work access, you need insights into both for a comprehensive view of risk. Additionally, if the solution reports historic password scores, you will gain an understanding of how your security measures and policies influence user behavior over time, as well as an understanding of how your company's password security has changed.

In addition to evaluating these features, look for a password management solution that:

- You can deploy easily, from one single point, across your organization
- Is simple to use both for admins and employees
- Comes with enhanced security such as two-factor authentication

SECTION 4:

FIVE PRACTICAL STEPS FOR EFFECTIVE IMPLEMENTATION

THE FIVE STEPS WILL HELP YOU SUCCESSFULLY LAUNCH A PASSWORD MANAGER IN YOUR COMPANY.

1. UNDERSTAND THE DEPLOYMENT OPTIONS FOR USERS.
Password managers typically offers several ways to add users:

SSO: Single sign-on (SSO) is an identification and authentication system that allows users to log in to different systems, websites, and applications with one enterprise identity. After enabling SSO for the password manager, you can invite employees via email to join the company account. The emailed link takes them to your organization's SSO login to complete a simple setup process.

ACTIVE DIRECTORY: For automated provisioning to users and groups, you can sync your password manager to a supported active directory, such as Microsoft AD. Synced email addresses that are not enrolled in the plan automatically receive an email invitation.

MANUAL INVITES: Admins can invite specific users through the admin console, either by typing in an email address or importing a .cvs or .txt file.

2. SET YOUR NEW PASSWORD POLICIES.
Before you roll out the solution to employees, create a policy that will help them understand the new procedures, requirements, and expectations.

The policy document can be very simple — shorter than a page — but should cover aspects such as:

- The approved password management solutions
- The acceptable security score for users' credentials
- Basic best practices, including for sharing and storing passwords, and disabling browser password storage solutions (like Chrome and Firefox)

3. KICKSTART CONVERSATIONS ABOUT SECURITY

Your security tools are ineffective without a strong security culture. If your employees don't understand their role in protecting your organization, they're less likely to follow security protocols.

Start conversations across the organization prior to the launch to improve employee participation. These conversations should focus on why data privacy and security are important to your business, why employees play an active role in safeguarding data, and how they can help improve the company's cybersecurity.

5. CONDUCT EMPLOYEE TRAINING

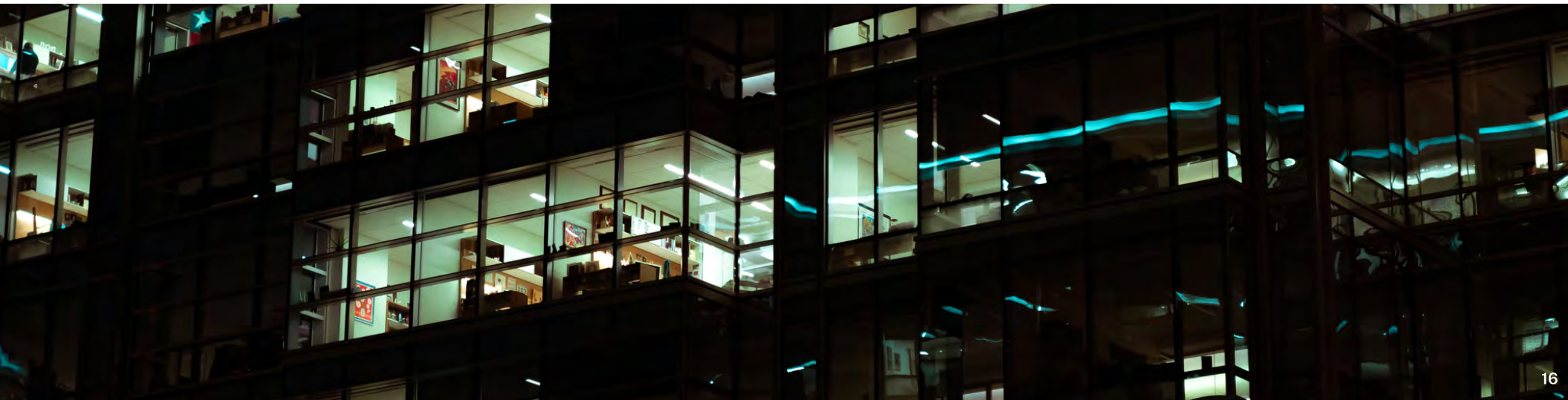
Ask your vendor for training videos and other materials that you can share with your employees. Consider offering additional options such as a live or on-demand webinar, as well as other internal resources that employees can access for help.

4. COMMUNICATE YOUR POLICY CHANGES

Communicating the changes to your users is a crucial step before you mass-deploy the password manager. Announce the upcoming adoption of the new security procedures and share the new password policy with your employees.

Consider a communication campaign that includes several phases, such as:

- General announcement
- New policy document
- User FAQ and information about training
- Post-deployment reminders and follow-ups



SECTION 5:

SEVEN KEY TAKEAWAYS ON INFORMATION SECURITY AND PASSWORD MANAGEMENT

1.

GROWING RISKS

The number of data breaches due to weak, stolen, or default passwords is on the rise. In 2019, passwords were responsible for more than 80% of hacking-related breaches,[10] compared to 63% in 2015.[11]

2.

STEEP COSTS

$4.77M is the average cost of a data breach caused by compromised or stolen passwords; that's 25% more expensive than data breaches of all causes ($3.9M)[12] In addition to the cost of mitigation, consequences can include loss of customers, adverse brand reputation, litigation, and regulatory fines.

3.

DARK WEB AND BREACHES

Cybercriminals can easily find stolen corporate passwords on the dark web — for lease, sale, and even free.[13] Because many employees reuse passwords,[14] a single data breach of an online provider can expose all your corporate accounts.

4.

WEAK PASSWORDS

Your employees can contribute to theft of credentials, whether they're acting maliciously or inadvertently. The frequency of incidents involving credential theft due to insiders has tripled per organization since 2016.[15] Insider risks include employees leaving your business with passwords.

5.

PASSWORD MANAGERS

Secure and easy to use, password managers protect access to your organization's critical data and assets without compromising user productivity. But if your password security solution is too complex, it will result in poor user adoption or user avoidance.

6.

PASSWORD MANAGER MUST-HAVES

Password managers should have a password generator, group sharing capabilities, options to see password score over time, a flexible admin dashboard, and dark web monitoring.

7.

ADOPTION STRATEGY

Select a solution that offers flexible deployment options like SSO, active directory syncing features, and the ability to send manual invites.

10 2020 Data Breach Investigations Report, Verizon, 2020
11 2016 Data Breach Investigations Report, Verizon, 2016
12 Cost of Insider Threats Global Report, IBM Security, 2020
13 "From Exposure to Takeover: The 15 billion credentials allowing account takeover," Digital Shadows, July 2020
14 Online Security Survey, Google/Harris Poll, February 2019
15 Cost of Insider Threats Global Report, IBM Security, 2020

DASH FORWARD

Many organizations rush to implement a password manager after they've been breached. Think proactively instead. Incorporate a password management solution into your risk-management strategy. By approaching deployment strategically, you'll not only avoid negative impacts to workflows but also improve your overall security posture.

WHAT'S NEXT

Find out how you can make the case to secure the digital life of your business with a password manager in this white paper.

READ NOW

For more information on Dashlane plans for business, sign up for a trial or visit dashlane.com/business.

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 their employees with the assurance that company data is safe. And employees can enjoy a way to manage their work and personal accounts that's already loved by millions. Our team in Paris, New York, and Lisbon is united by our passion for improving the digital experience and the belief that with the right tools, we can help everyone realize the promise of the internet. Dashlane has empowered over 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

DASHLANE