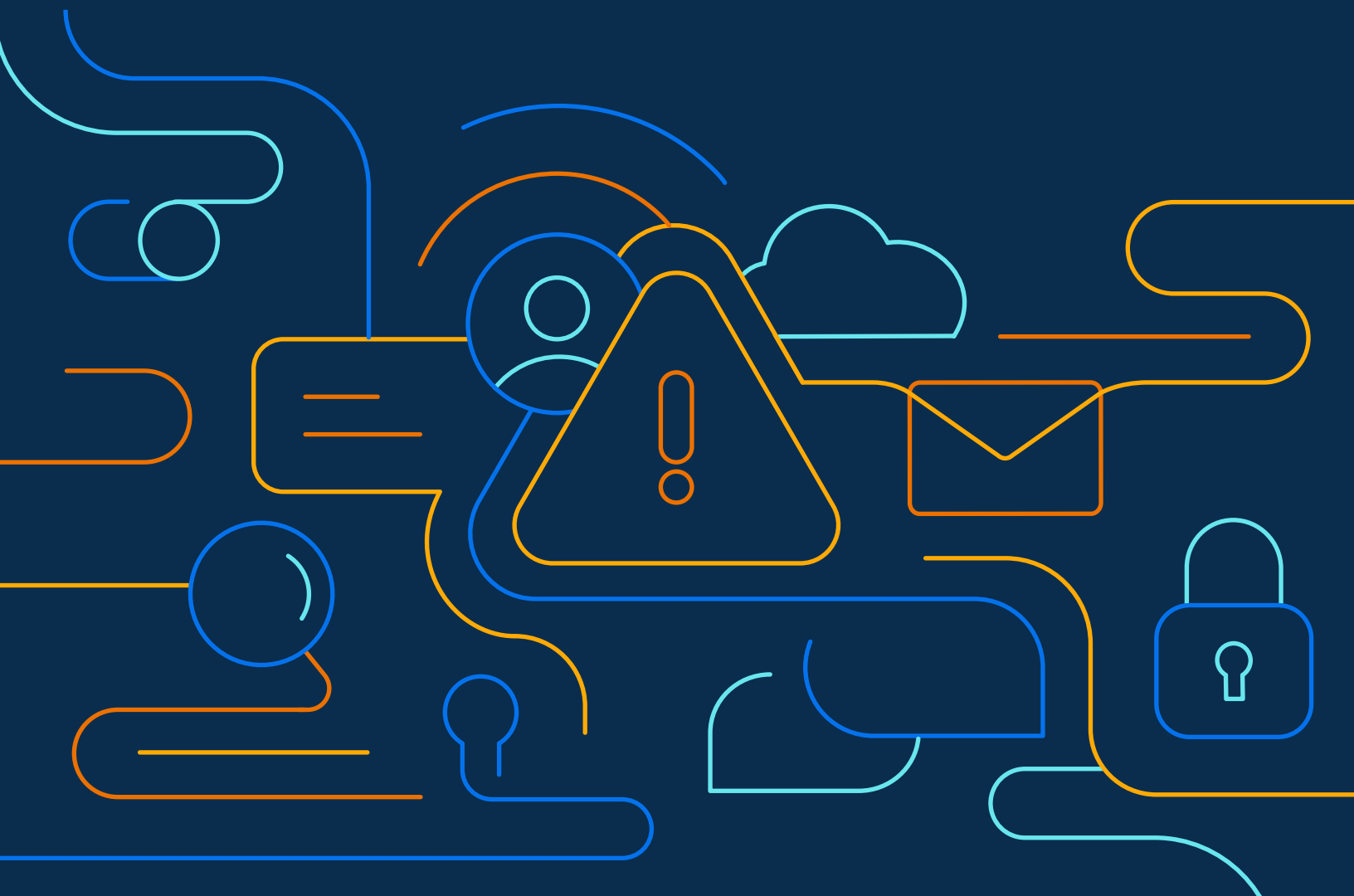
1Password

The 1 for Business

How to avoid a data breach



A data breach can happen to any business; even tech giants like Facebook and IT firms like SolarWinds aren't immune. But you can reduce the risk and mitigate the impact of a data breach by closing the security gaps created by your biggest vulnerability: passwords and secrets.

The fast-paced development cycle, expanding IT ecosystem, and shift to remote work mean countless new vulnerabilities and less oversight, while online threats continue to evolve by the day. Preparing for the possibility of a data breach starts with one simple thing – stronger and better-managed company secrets, created and secured with a password manager like 1Password.

$3.9 mil the average cost of an enterprise data breach.

80 % **of IT leaders** feel their company is unprepared for an attack.

36 **billion** records were compromised in 2020.

Losses from cybercrime rose **six-fold** in 2020 alone.

- Even the smallest company has something to lose from a breach, the most precious being its reputation as a trusted place to do business.
- Compromised passwords and secrets are your single largest vulnerability.
- The right tools can help build a culture of security that will minimize your chances of an attack and recover quickly if the worst happens.

You're only as strong as your weakest link

Effective security risk management takes a conscious and consistent effort from everyone, not just IT. A secure environment begins with better password and secrets management: 81% of data breaches are caused by weak, reused, or mismanaged passwords, and 85% of exposed secrets are found on developers' personal repositories.

- An enterprise password manager (EPM), along with tighter password and secrets management behaviors across the company, are your strongest preventative measures.
- You can't control every part of your IT infrastructure; employees will use tools outside the approved stack whether you want them to or not. But you can empower them to do it securely and give IT visibility.
- SSO and MFA only do so much. Strong passwords and securely managed dev secrets can close the gap.

P@s5word Pr0bl3m$

64% **of IT/DevOps** admit to reusing enterprise secrets between projects.

45% **of U.S. adults** use weak passwords (8 characters or fewer).

59% **of IT/DevOps** have used email to share enterprise secrets with colleagues.

A third of workers use only **2-3 unique passwords** for all their accounts.

Building a culture of security

A single compromised account can expose your most sensitive information, including customer data. Set your employees up for success with the right policies and tools in place. Start by adding an enterprise password manager to your security stack – one that helps them create, store, and share their passwords and secrets. Then, teach them how to use it and reinforce safe habits through well-defined best practices and ongoing education.

Learn more about building and maintaining a culture of security in 1Password's infographic on the topic.

Learn more

- The right tools provide the foundation for your culture of security, because they empower employees to behave securely.
- Involve the entire organization in a holistic approach to security risk management, starting from the top, down. (Make security a policy, not a suggestion.)
- Strengthen security guidelines and get buy-in from company leaders, HR, IT, and team managers.
- Make policies easily accessible for employees, and provide regular training and security updates.
- Create a non-judgemental, blame-free environment with open communication. Empower and support employees in their role of keeping the company and customers safe.

Security risk management tips every employee should know:

- Update systems, routers, and apps regularly (if not done routinely by IT).
- Avoid suspicious links, emails, and online forms.
- Don't share passwords, secrets, or other data if not necessary – and use secure sharing if you do.
- Report issues, missteps, and suspicious activity immediately to IT

1Password for business helps close your security gaps

A password manager only works if your team adopts it. 1Password is easy to use and manage, and can be deployed quickly and effortlessly to 50 or 5,000 employees. It's the world's most-trusted enterprise password manager for many reasons:

- Generate and store long, random passwords for every account, so even if credentials are compromised they won't open doors to valuable information.
- Notify employees if their company credentials are affected by a breach, so they can take action immediately.
- Run IT reports that show if any company email address or credentials have been compromised in a breach, so potential threats can be prevented.
- Integrate with your existing security infrastructure and DevOps workflow.
- Get up and running in a matter of seconds and see immediate results.
- Get free family accounts for every employee so they can practice good security habits at home and at work, while making sure personal and business data stay separate.

WIRED Best Password Manager

G2 CROWD Highest Rated Password Manager

Trustpilot Best Rated Password Manager

IBM slack PagerDuty GitLab

1Password The 1 for Business