Password decisions survey 2023
### Demographics

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>C-level Executive</td>
<td>43%</td>
</tr>
<tr>
<td>Director</td>
<td>34%</td>
</tr>
<tr>
<td>Sole decision maker</td>
<td>85%</td>
</tr>
<tr>
<td>Age 35-44</td>
<td>46%</td>
</tr>
<tr>
<td>Full-time employee</td>
<td>99%</td>
</tr>
<tr>
<td>Bachelors or masters degree</td>
<td>73%</td>
</tr>
<tr>
<td>Information Technology</td>
<td>36%</td>
</tr>
<tr>
<td>Manufacturing and Construction</td>
<td>15%</td>
</tr>
<tr>
<td>Finance/Accounting</td>
<td>9%</td>
</tr>
<tr>
<td>Science/Programming/Software</td>
<td>8%</td>
</tr>
<tr>
<td>Health Care</td>
<td>5%</td>
</tr>
</tbody>
</table>

2023 Password Decisions Survey
About the survey

In Fall 2022, Bitwarden partnered with Propeller Insights to poll 800 independent IT decision makers across a wide range of industries who play a key role in enterprise purchasing decisions for the third iteration of this survey.

This year’s findings show that passwordless technology has made inroads with businesses enthusiastic about its perceived security benefits and improved user experience (UX).

The survey also demonstrates a continued desire for C-suite-driven security leadership and underscores how security concerns are influencing business decisions.
Password habits at work
Strategies for managing passwords at work

Password management software remains popular - but so do risky practices such as writing down passwords or saving them on spreadsheets.

<table>
<thead>
<tr>
<th>Method</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password management software</td>
<td>84%</td>
</tr>
<tr>
<td>Document on my computer</td>
<td>54%</td>
</tr>
<tr>
<td>My memory</td>
<td>45%</td>
</tr>
<tr>
<td>Pen and paper</td>
<td>29%</td>
</tr>
</tbody>
</table>

2023 Password Decisions Survey
Most (66%) of IT decision makers share passwords through a password manager but a sizable number also share via email and online documents.

Password sharing methods:

- Password manager: 66%
- Email: 41%
- Shared online document: 38%
- Messaging & chat: 30%
- Spoken: 27%
- Paper: 22%
- I never share passwords: 14%
Most important attributes for a good password manager

- 60% Security
- 56% The password manager integrates 2FA
- 40% Easy to use
- 36% Operates across a wide range of devices and platforms
- 30% Supports biometric logins
- 24% User interface (UI)
- 23% Allows self-hosting and complete environmental control
- 18% Is built on open source technology
- 13% Offers free option

2023 Password Decisions Survey
Enterprise-wide password manager

A large majority (79%) want their employer to require employees to use the same password manager across the organization.

Would you like your employer to require employees to use the same enterprise-wide password manager across the organization?

- 79% Yes
- 16% No
- 5% Doesn’t matter

2023 Password Decisions Survey
If your company used a password manager and provided a complementary family account for personal use, how likely would you be to use it at home with your family?

- 71% Very likely
- 24% Somewhat likely
- 5% Not likely

If offered, 71% said they’d also be very likely to use a password manager at home.
### Password reuse

Almost all (90%) reuse passwords

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>11%</td>
<td>More than 15 sites</td>
</tr>
<tr>
<td>24%</td>
<td>10-15 sites</td>
</tr>
<tr>
<td>36%</td>
<td>5-10 sites</td>
</tr>
<tr>
<td>19%</td>
<td>1-5 sites</td>
</tr>
<tr>
<td>10%</td>
<td>Never reuse</td>
</tr>
</tbody>
</table>
2FA is wildly popular

92% use it in the workplace, up from 88% last year

Do you use two-factor authentication in the workplace?

- Yes: 92%
- No: 7%
- Not sure: 1%
Why do you think people may be reluctant to utilize two-factor authentication technology at work or for personal use?

- People are not aware of the benefits of 2FA (48%)
- Think 2FA is not necessary because their password is strong enough (47%)
- Think it’s very unlikely they’ll get hacked (41%)
- It slows down workflow (41%)
- Lack of motivation/time to implement (36%)

Almost half (48%) believe people who are reluctant to use 2FA are not aware of the benefits.
Does your organization have cyber insurance?

Almost three-fourths (75%) say their organization has cyber insurance.

- **Yes**: 75%
- **No**: 21%
- **Not sure**: 4%
Show your work: 65% were required to demonstrate they offered cyber awareness training to employees when they applied for cyber insurance. 64% had to show use of MFA. 61% had to demonstrate use of a password manager.
Security risks & cyber attacks
Close to half (41%) of phishing attacks come from fake financial institutions. Among the options, phishing attacks most often pretend to be:

- **My financial institution**: 41%
- **My boss or exec**: 22%
- **Government entity**: 21%
- **Family member or friend**: 8%
- **Healthcare organization**: 6%
Ransomware migration strategy

Up from 75% last year, 80% report having a ransomware mitigation strategy in place.
Cyberattack experiences

The percentage reporting cyberattacks is up: 60% this year, compared to 54% last year.
Shadow IT Engagement

Almost one-third (32%) of IT decision makers and 49% of employees engage in ‘shadow IT’

Have you ever used unauthorized devices or software without IT’s approval?

- Yes: 32%
- No: 67%
- Not sure: 1%
Has your organization struggled with employees using unauthorized devices or software without IT’s approval?

Almost half (49%) report employees engage in ‘shadow IT’.
Why do you think employees within your organization use unauthorized devices or software without IT’s approval?

Most believe employees do it because they think it makes them more efficient.

- 73% believe it helps make their day-to-day ‘on the job’ activities faster and more efficient.
- 52% report a lack of authorization for certain applications or software they want to use.
- 50% cite slow response times to IT-related issues involving company-issued devices and software.
The persistence of remote work continues to drive cybersecurity concerns

Have you become more concerned about cybersecurity in the past year?

- Yes, because more employees are working remotely and may be more lax with their overall security posture (60%)
- Yes, because several high-profile cyberattacks have been the result of password breaches (43%)
- Yes, because turnover is higher than usual and I'm not sure what happens to passwords when people leave the organization (35%)
- Yes, for other reasons not listed here (13%)
- No, I'm not more concerned about cybersecurity this year (9%)

2023 Password Decisions Survey
Passwordless revolution
Why has your organization not deployed passwordless?

Of the IT decision makers that have not gone passwordless, half cite the inability of applications in use to make the transition.

- 49%: The applications we're using are not designed to go passwordless
- 39%: End users prefer passwords/reluctant to switch to passwordless
- 28%: Limited budget
- 23%: Leadership resistance
- 21%: Limited talent and skills

2023 Password Decisions Survey
Deploying passwordless

Around half (49%) are deploying or have plans to deploy passwordless tech.

Do you currently deploy, or have future plans to deploy, passwordless?

- 49% Yes
- 37% No
- 15% Not sure
Deploying passwordless

Two-thirds (66%) have 1-2 users groups or multiple teams going passwordless.
A majority (51%) are relying on the ‘something you are’ form of passwordless authentication.
The primary reason to deploy passwordless?

Better security, say 41%

- 41% Better security
- 24% Better user experience
- 19% Increase workplace productivity
- 17% Minimize burden of IT help desk
FIDO2 Gaining

47% say FIDO2 is an ‘important aspect’ of their passwordless adoption