In November 2021, Bitwarden partnered with Propeller Insights to poll over 400 independent IT decision makers across a wide range of industries who play a key role in enterprise purchasing decisions.

The findings show an uptick in password manager usage, indicating its increasingly mainstream appeal.

Concurrently, IT decision makers continue to struggle with adhering to security best practices and express security-related unease about remote work.
Demographics

26% C-level Executive
54% Director
83% Sole Decision Maker
48% Age 35-44

26% Information Technology
14% Manufacturing and Production
12% Science/Programming/Software
8% Health Care
7% Finance/Accounting
Password Practices at Work
Password managers are on the rise, but risky security practices remain pervasive - such as relying on computer documents and paper.

### Strategies for managing passwords

- **Password management software**: 86%
- **Document on my computer**: 53%
- **My memory**: 42%
- **Pen and paper**: 29%

© Bitwarden 2022 Password Decisions Survey
Password sharing methods

Compared to last year, the number of IT decision makers sharing passwords via email skyrocketed from 39% to 53% due in part to the sudden adjustment to remote work and increased rate of employee turnover.

- Email: 53%
- Shared online document: 43%
- Messaging/chat: 41%
- Spoken: 31%
- I never share passwords: 24%
- Paper: 21%
Most respondents want their employers to require employees to use the same enterprise-wide password manager.

- Yes: 84%
- No: 9%
Security Risks and Cyberattacks
<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>My financial institution</td>
<td>35%</td>
</tr>
<tr>
<td>A government entity</td>
<td>22%</td>
</tr>
<tr>
<td>My boss or another executive within my org.</td>
<td>21%</td>
</tr>
<tr>
<td>A healthcare organization</td>
<td>11%</td>
</tr>
<tr>
<td>A family member or friend</td>
<td>8%</td>
</tr>
</tbody>
</table>

Phishing attacks remain a scourge as criminals hone more sophisticated social engineering tactics.
Password reuse

Despite a year of high-profile cyberattacks and increasing vulnerabilities posed by remote work, almost all respondents reuse passwords across multiple sites.
More than half of respondents confirmed their organization has experienced a cyber attack.
Do you have a ransomware mitigation strategy?

In spite of recent high-profile breaches, 25% of organizations either don't have or aren’t sure if they have a ransomware mitigation strategy in place.
Both employees AND IT decision makers still resort to using Shadow IT

30% of decision makers find themselves resorting to shadow IT as a workaround
Why employees resort to shadow IT practices

While some may believe shadow IT helps make their work faster and more efficient, the long-term security impact is potentially ruinous.
Employer-led cybersecurity continuing education

- **54%** Offered a formal, intensive cybersecurity education training program
- **53%** Shared ongoing updates about phishing attacks or other threats to be aware of
- **51%** Provided a tutorial about password best practices
- **47%** Offered assistance with setting up a password manager
- **9%** My employer has not offered any of these programs, benefits, or information

© Bitwarden 2022 Password Decisions Survey
Remote work and the Great Resignation
Rise of remote work has heightened cybersecurity concerns

- Because remote work may lead to weaker security posture: 61%
- Because password breaches have led to high-profile cyberattacks: 55%
- Because turnover is making password management more difficult: 23%
- No, not more concerned: 9%

© Bitwarden 2022 Password Decisions Survey
The Great Resignation hasn’t spared the world of IT decision makers with 48% working more hours than last year.
58% of IT decision makers are working more hours due to turnover and difficulty hiring

- 29% More because of turnover
- 29% More because of trouble hiring
- 27% More because remote team requires more time
- 26% More because work-life balance elusive while WFH
- 25% Less for various reasons
- 16% Not sure/don’t know

© Bitwarden 2022 Password Decisions Survey
Technologies in Use
<table>
<thead>
<tr>
<th>Perceived barriers to implementing password managers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost</td>
</tr>
<tr>
<td>Lack of motivation/time</td>
</tr>
<tr>
<td>They're not always easy to use</td>
</tr>
<tr>
<td>No need; password managers built into web browsers</td>
</tr>
<tr>
<td>I don’t trust them</td>
</tr>
<tr>
<td>I don’t think they are necessary</td>
</tr>
</tbody>
</table>

© Bitwarden 2022 Password Decisions Survey
Top attributes of a good password manager

- **63%** Strong encryption subject to third-party audit
- **49%** Easy to use
- **48%** Wide range of devices and platforms
- **36%** Supports biometric logins
- **34%** User interface
- **30%** Allows self-hosting and complete environmental control
- **24%** Relies on open source technology
- **16%** Offers a free option

© Bitwarden 2022 Password Decisions Survey
While 2FA popularity is encouraging, perceptions that it “slows down workflow” and “takes time to implement” drive employees away from embracing it.

- 45% It slows down workflow
- 44% Lack of motivation/time to implement
- 28% Think being hacked is unlikely
- 23% People aren’t aware of the benefits of 2FA
- 21% Perception that a password is strong enough
2FA has become mainstream

88%

of respondents use two-factor authentication in the workplace