Authentication Attitudes, Usage & FIDO Brand Research Report

May 27, 2020
Research Findings
Consumers want stronger security for financial apps & storage of sensitive data

Consumers prefer to use methods stronger than username/password for:

- **81%** Online banking and personal finance
- **78%** P2P payments
- **67%** Online cloud services (Google Drive, Dropbox, OneDrive, etc)
- **64%** e-Commerce
Consumers are comfortable with online shopping and banking, yet worry about financial or identity theft

- 85% are comfortable online shopping
- 80% are comfortable banking online
- 75% worry about identity theft or fraudulent use of their payment or banking information
- 73% worry about criminals gaining access to their personal/sensitive information
Most consumers aren’t using best practices for passwords

52% are using 5 or few passwords across all their online accounts

ONLY 5% said they use a unique password for every site
Primary means for keeping track of passwords?
Top 3 answers

45% Keep track in their head
37% Write them down
32% let the browser store the password

... which makes sense since the majority use 1-5 passwords
They are resetting passwords often

76% reset a password at least once every six months

51% More than half reset at least once every 3 months
They have familiar tactics for assigning passwords

“I usually assign one password to my accounts unless the website requires something more secure and then I use a slight variation of my usual password. If the website is one I don’t use often and requires a really strange password, I request a new password every time I want to login.”

Typically use one that is familiar to me for some reason. DOB for family member, motivational word with year, some combination word with meaning solely to me and numbers & characters.”

“I use somewhat the same password just changing uppercase lower case numbers and symbols.”

“No, older accounts like social medias have older, easier passwords while newer financial and email accounts have longer and more difficult passwords.”

“Yes, I have a rotation of base words and change numbers and special characters/capitalized letters on a schematic basis.”

Yes, I usually assign one password to my accounts unless the website requires something more secure and then I use a slight variation of my usual password. If the website is one I don’t use often and requires a really strange password, I request a new password every time I want to login.”

Typically use one that is familiar to me for some reason. DOB for family member, motivational word with year, some combination word with meaning solely to me and numbers & characters.”

“I use somewhat the same password just changing uppercase lower case numbers and symbols.”

“No, older accounts like social medias have older, easier passwords while newer financial and email accounts have longer and more difficult passwords.”

“Yes, I have a rotation of base words and change numbers and special characters/capitalized letters on a schematic basis.”

Q26. Do you have a strategy for assigning different types of passwords to different types of web sites and apps?
They are less familiar with biometric capabilities on their desktops than on mobile devices, security keys

<table>
<thead>
<tr>
<th>Feature</th>
<th>Use it now</th>
<th>Heard of it and am familiar with it</th>
<th>Heard of it but not familiar with it</th>
<th>Have never heard of it</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text message authentication</td>
<td>65%</td>
<td>21%</td>
<td>9%</td>
<td>6%</td>
</tr>
<tr>
<td>Biometric fingerprint on smartphone</td>
<td>42%</td>
<td>34%</td>
<td>18%</td>
<td>6%</td>
</tr>
<tr>
<td>Biometric facial scan on smartphone</td>
<td>22%</td>
<td>37%</td>
<td>31%</td>
<td>10%</td>
</tr>
<tr>
<td>Biometric fingerprint on desktop</td>
<td>16%</td>
<td>38%</td>
<td>29%</td>
<td>17%</td>
</tr>
<tr>
<td>Security keys that are plugged into or communicate wirelessly with your computer</td>
<td>16%</td>
<td>27%</td>
<td>28%</td>
<td>29%</td>
</tr>
<tr>
<td>Wearable computing device (e.g., smart watch) that enables your smartphone or computer</td>
<td>16%</td>
<td>34%</td>
<td>31%</td>
<td>20%</td>
</tr>
<tr>
<td>Biometric eye scan on smartphone</td>
<td>13%</td>
<td>33%</td>
<td>35%</td>
<td>19%</td>
</tr>
<tr>
<td>Biometric facial scan on desktop</td>
<td>11%</td>
<td>32%</td>
<td>37%</td>
<td>20%</td>
</tr>
<tr>
<td>Biometric eye scan on desktop</td>
<td>8%</td>
<td>32%</td>
<td>36%</td>
<td>24%</td>
</tr>
</tbody>
</table>
But want to use them

Interest in Using These Ways to Securely Access Mobile Apps/Websites

- **69%** Biometric fingerprint on smartphone
- **58%** Biometric facial scan on smartphone
- **60%** Biometric fingerprint on desktop
- **56%** Biometric eye scan on smartphone
- **52%** Biometric facial scan on desktop
- **50%** Biometric eye scan on desktop
- **53%** Security keys that are plugged into or communicate wirelessly with your computer
- **49%** Wearable computing device (e.g., smart watch) that enables your smartphone or computer

Base: Total (n=1,032)
Q22. How interested would you be to use each of the following ways to securely access websites or apps that have your sensitive information?
Next, we educated them about FIDO

76% of respondents find the FIDO approach appealing
They value security benefits slightly over usability

Importance of Benefits

- **92%** Is secure
- **90%** Protects you from having your account taken over
- **89%** None of your personal information or login info is sent over the internet
- **86%** Works on any device people use every day

- **84%** Works on any browser type
- **83%** Is convenient
- **73%** Reduces use of passwords
They find FIDO more appealing than usernames/passwords and SMS OTP

83% said FIDO is better
They would trust mobile apps and websites using FIDO more

71% said they would trust a website more if it used FIDO
They want to use FIDO

77% are extremely or very interested in using FIDO for login
So what do consumers think about the FIDO brand?

We showed them 3 logos

And this button
Few have seen the logos before, but would want to learn more about it if they saw it on a login screen.

50-55% would click a mouseover symbol to learn more.

39-48% would do a search to find out more about the logo.
Consumers like the FIDO login button

72% said they would be more willing to learn about the FIDO approach if they saw it

80% said they found the button appealing
FIDO logos would create perceptions that a company is innovative and customer centric.

## Agreement Statements About Company Using the FIDO Logos

- **Is up-to-date on current industry security standards**: 75%
- **Is an innovative company**: 77%
- **Does everything it can to protect customer data**: 73%
- **It is a company that cares about me as a customer**: 67%
- **Is a trustworthy company**: 69%
- **Improves my overall impression of the company**: 69%
- **Is at the forefront of anticipating and addressing customer needs**: 69%

## Impact of FIDO Logos on Willingness to Purchase from...

- **Mobile retailers**: 70%
- **Online retailers**: 70%

---

**Base**: Total (n=1,032)

Q13. How much do you agree or disagree with each of the following statements about the company using the logos below? | Q14. What impact, if any, would seeing one of these logos have on your willingness to purchase from each of the following?
Consumers want to see FIDO branding at the point of login, particularly for more sensitive apps

They said it’s very important to see FIDO logo for these apps:

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Very Important</th>
<th>Maybe</th>
<th>Not Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online banking and personal finance</td>
<td>75%</td>
<td>18%</td>
<td>7%</td>
</tr>
<tr>
<td>Person-to-person payments (e.g. PayPal, Venmo, etc.)</td>
<td>73%</td>
<td>21%</td>
<td>6%</td>
</tr>
<tr>
<td>Online retailing / e-commerce</td>
<td>71%</td>
<td>22%</td>
<td>6%</td>
</tr>
<tr>
<td>Travel websites (airlines, hotels, etc.)</td>
<td>59%</td>
<td>31%</td>
<td>9%</td>
</tr>
<tr>
<td>Online cloud service (e.g. Dropbox, OneDrive, Google Drive, iCloud, etc.)</td>
<td>59%</td>
<td>32%</td>
<td>9%</td>
</tr>
<tr>
<td>Email services (e.g. Gmail.com, YahooMail.com, etc.)</td>
<td>57%</td>
<td>32%</td>
<td>11%</td>
</tr>
<tr>
<td>Log on to social media accounts (like Instagram, Facebook, Twitter, etc.)</td>
<td>54%</td>
<td>35%</td>
<td>11%</td>
</tr>
<tr>
<td>Car share services (e.g. Uber, Lyft, etc.)</td>
<td>50%</td>
<td>37%</td>
<td>13%</td>
</tr>
<tr>
<td>Online food delivery services (e.g. Domino's, GrubHub, DoorDash, etc.)</td>
<td>50%</td>
<td>38%</td>
<td>12%</td>
</tr>
<tr>
<td>Search engines (e.g. Google, Yahoo, Bing, etc.)</td>
<td>44%</td>
<td>39%</td>
<td>17%</td>
</tr>
<tr>
<td>Online video/ music streaming apps (e.g. Netflix, Spotify, Hulu, etc.)</td>
<td>43%</td>
<td>43%</td>
<td>13%</td>
</tr>
</tbody>
</table>
Learn more:

LoginWithFIDO.com