
Individuals vs. IT professionals: security beliefs and behaviors

<table>
<thead>
<tr>
<th>Behavior</th>
<th>Individuals</th>
<th>IT Professionals</th>
</tr>
</thead>
<tbody>
<tr>
<td>2FA adoption</td>
<td>23%</td>
<td>37%</td>
</tr>
<tr>
<td>Biometrics usage</td>
<td>37%</td>
<td>60%</td>
</tr>
<tr>
<td>Password complexity</td>
<td>39%</td>
<td>50%</td>
</tr>
<tr>
<td>Password strength</td>
<td>51%</td>
<td>49%</td>
</tr>
</tbody>
</table>

Protecting the workforce

84% of IT professionals said their organization experienced a phishing attack, while 12% experienced credential theft, and 8% experienced a man-in-the-middle attack.

53% of individual users believe that eliminating usernames and passwords would offer better security.

42% of these respondents feel that it is irritating to copy and paste one-time codes.

5% of IT professionals believe that 2FA disrupts their workflow.

Managing passwords & preventing account takeovers

29% of individuals believe SMS or mobile authentication app 2FA is easy to use and significantly improve account security.

46% of IT professionals believe that 2FA is an important area for improving account security.

55% of IT professionals believe SMS or mobile authentication app 2FA is easy to use.

Securing mobile users

56% of individuals believe mobile devices are a source of account theft.

31% of IT professionals believe their organization makes mobile devices a priority for security.

Protecting customer accounts

Customer information and personally identifiable information (PII) are at the top of the list for IT professionals to protect, yet 59% of IT professionals report that customer accounts have been compromised.

52% of IT professionals believe a hardware security key would offer better security.

47% of IT professionals believe 2FA is very important.

40% of these respondents believe that 2FA will prevent account takeovers.

When it comes to accessing information online, individual users ranked security (59%), affordability (57%) and ease of use (35%) as the most important factors.

56% of IT professionals and individuals prefer a method of protecting accounts that doesn’t involve passwords.

55% of IT professionals and individuals prefer 2FA authentication, while 44% prefer biometrics.

44% of IT professionals believe that biometrics could improve the security of their organization.

50% of IT professionals believe that 2FA makes using passwords much more difficult for the user.

52% of IT professionals believe that 2FA would offer better security.

60% of these respondents believe that 2FA should be mandatory for corporate accounts.

Reaching a safer future

56% of IT professionals will only adopt new technologies that are easy to use and significantly improve account security.

46% of IT professionals report that their organization relies on copy and paste one-time codes.

56% of IT professionals believe biometrics make passwords more important.

44% of IT professionals believe 2FA is an important area for improving account security.

40% of these respondents believe that 2FA will prevent account takeovers.

52% of IT professionals believe a hardware security key would offer better security.

60% of these respondents believe that 2FA should be mandatory for corporate accounts.


© 2020 Yubico

Yubico was founded in 2006 with the mission to make internet login simpler, and for two decades we have developed secure access management solutions for the world’s leading enterprises, including 85% of Fortune 500 companies. Yubico is the pioneer and leader of the hardware security key, behind the majority of the hardware keys in use today. Our solutions are used by more than 500 million people across 250,000 organizations worldwide. Find more information at www.yubico.com.