The 2020 State of Password and Authentication Security Behaviors Report

Do individual users and IT professionals see eye-to-eye on security?

A recent study from Ponemon Institute shows that both IT professionals and individual users are engaging in risky security practices despite increasing privacy and security concerns. However, expectation and reality are often misaligned between the two groups when it comes to the implementation of usable and desirable security solutions.

Individuals *vs.* IT professionals: security beliefs and behaviors

Individuals		IT Professionals
25%	Have become **highly alarmed** about the privacy and security of their personal data in the past two years.	37%
76%	Of the individuals and IT professionals who experienced an **account takeover**, some changed how they managed passwords or protected their accounts.	65%
64%	**Do not** use 2FA as a form of account protection for personal accounts.	60%
39%	**Reuse passwords** across workplace accounts.	50%
51%	Sometimes or frequently **share passwords** with colleagues.	49%

Protecting the workforce

51% of IT professionals said their organization experienced a **phishing attack**, another **12%** experienced **credential theft**, and **8%** experienced a **man-in-the-middle attack**.

31% of IT professionals say that their organization uses a **password manager**, which are effective tools to securely create, manage and store passwords.

42% of IT professionals report that their organization relies on **sticky notes** to manage passwords.

59% of IT professionals report that their organization **relies on human memory** to manage passwords.

Managing passwords & preventing account takeovers

46% of IT professionals **require the use of 2FA to gain access** to corporate accounts

37% of organizations that implement 2FA to secure business accounts **rely on mobile authentication apps** and **28% rely on SMS codes.**

23% of individuals believe SMS or mobile authentication app 2FA methods are **very inconvenient.**

54% of these respondents feel that SMS or mobile authenticator apps **disrupt their workflow.**

47% of these respondents feel that it is **irritating** to copy and paste one-time codes.

Securing mobile users

55% of organizations **allow the use of personal mobile devices.**

62% of organizations don't believe that they take the necessary steps to **protect information on mobile devices.**

56% of individuals that use a personal device to access work related items **don't use 2FA.**

Protecting customer accounts

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

60% of these respondents say they believe usernames and passwords offer **sufficient security.**

25% of IT professionals **have no plans** to provide 2FA to customers.

47% of these respondents say they believe it would be **inconvenient** for customers.

When it comes to accessing information online, individual users rated security (56%), affordability (57%) and ease of use (35%) as very important.

Reaching a safer future

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

55% of IT professionals and individuals prefer a method of protecting accounts that doesn't involve passwords.

56% of IT professionals believe that eliminating passwords would **improve the security of their organization.**

54% of IT professionals believe that eliminating passwords would **improve user convenience.**

65% of IT professionals believe the **use of biometrics** would increase the security of their organization.

53% of individual users believe the use of biometrics would **offer better security** for their accounts.

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

60% of individuals would be **willing to pay $50-$60** to have the highest form of security across all of their online accounts.

For full details on the Ponemon Institute survey, read
The 2020 State of Password and Authentication Security Behaviors Report

Visit yubico.com/authentication-report-2020

yubico
www.yubico.com

Yubico was founded in 2007 with the mission to make secure login easy and available for everyone. In close collaboration with leading internet companies and thought leaders, Yubico co-created the FIDO U2F and FIDO2/WebAuthn open authentication standards, which have been adopted in major online platforms and browsers, enabling two-factor, multi-factor, and passwordless login and a safer internet for billions of people.