NOVEMBER 2023

MFA CONSUMER SENTIMENT REPORT

A multi-year study of consumer perspectives regarding multi-factor authentication

Cybercrime Support Network | COMCAST | CLEAR MISSION CONSULTING

EXECUTIVE SUMMARY

These are the major conclusions of a multi-year study performed by the Cybercrime Support Network (CSN) with support from Comcast. Over 1,200 adults in the United States were surveyed between Spring 2022 and Fall 2023 about their experiences and preferences regarding MFA.

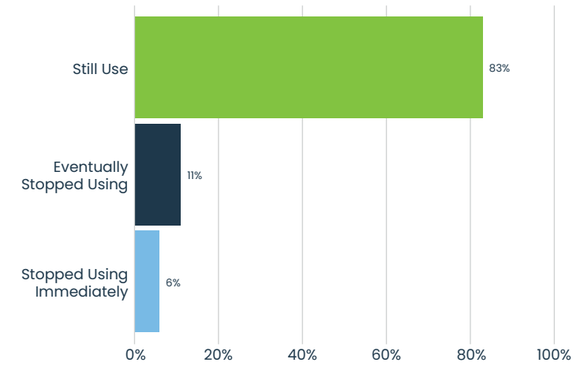
Consumers Embrace Accounts that Require MFA

Consumers overwhelmingly continue to use accounts even when required to employ MFA. Moreover, our results suggest consumers are more willing to adopt MFA as they gain exposure to it—those who regularly encounter MFA are **27% more willing to use MFA** than users who are knowledgeable about MFA but have never used it.

89%
use an account that already requires MFA.

77%
say they are willing to use MFA for account access.

What did you do when an account required MFA?



MFA Increases Consumer Protection and Trust

We asked consumers about MFA in connection with their digital accounts.

- **76% say it is in the best interest** of their personal information and its security when companies require MFA for their accounts.
- **77% feel MFA protects** their personal information from being easily compromised.
- **66% say they trust a company more** if it requires them to use MFA.

Reducing Friction for Consumers

While resistance to MFA is low, businesses can further reduce friction through consumer education and by improving ease-of-use.

Consumers who rate the importance of securing online accounts highly are **56% more willing to use MFA** than consumers who don't, suggesting that businesses can increase MFA adoption by educating their users about how MFA improves security.

Convenience and ease of use are concerns for consumers. Businesses can lower barriers to MFA adoption by addressing top complaints—that MFA is time-consuming, requires extra steps to access accounts, or requires additional devices or software in order to access accounts.

> **"The security game has changed. It's not just tech, it's how we talk about it. Let's debunk the myth that MFA is a hassle."**
>
> —Kristin Judge, CSN Founder

TABLE OF CONTENTS

KEY FINDING #1

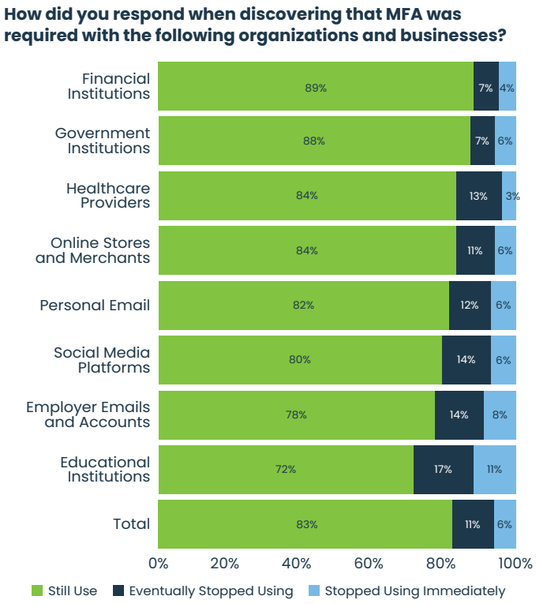
CONSUMERS CONTINUE TO USE MFA-ENABLED ACCOUNTS

Account Types Impact on MFA Adoption

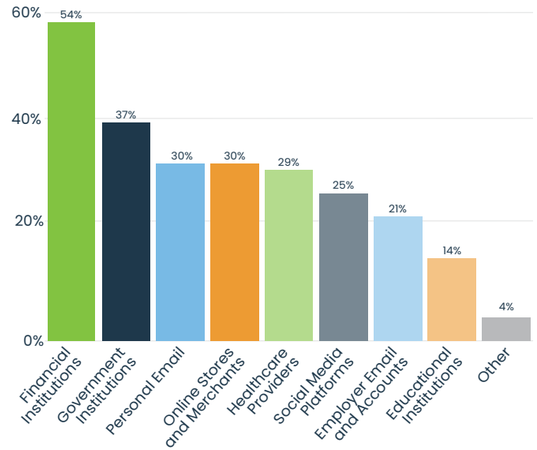
We asked consumers how they responded when different types of accounts required them to use multi-factor authentication (MFA).[1] Consumers still use the vast majority (83%) of these accounts.

According to the survey, school and employer accounts—which may not be essential for some respondents—are the two types of accounts consumers are least likely to continue using. Though this conclusion cannot be drawn definitively from this study, the inconvenience of maintaining multiple accounts—in addition to, say, a personal email account—may be a factor in consumers' decision to stop using them, and not just the requirement to employ MFA.

How did you respond when discovering that MFA was required with the following organizations and businesses?



Which of the following organizations and businesses have required you to use MFA?



Mandatory MFA Across Various Digital Accounts

How many consumers have had to make a decision about whether to continue using an online service or account that required MFA? Most of them—89% of consumers say at least one digital account has required them to use MFA. The most common type of account to require MFA is a consumer's bank or other financial institution. Most consumers (54%) have a bank or other financial account that has enforced mandatory MFA.

[1] Due to rounding, numbers throughout this report may not add up to 100%.

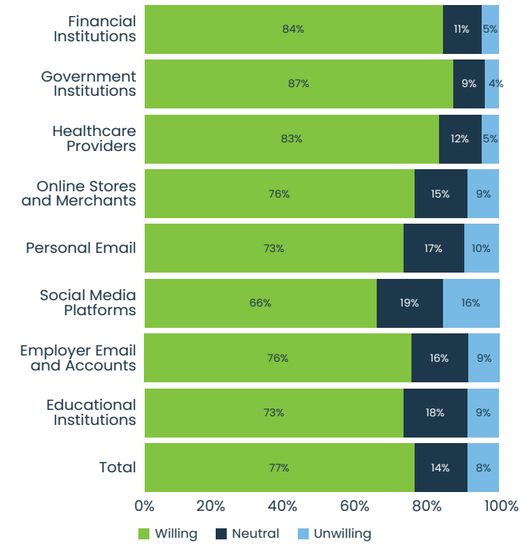
Willingness to Use MFA

We also asked consumers how willing they are to use MFA[2] across all account types, 77% of consumers say they are willing to use MFA, with only 8% unwilling. Willingness varies by account type, with more users willing to use MFA, for example, to interact with government institutions than for accessing social media platforms.

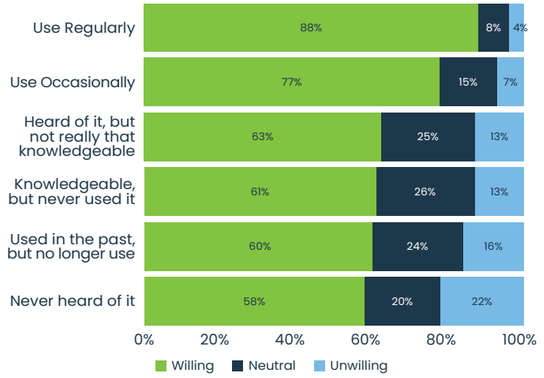
77%

of consumers say they are willing to use MFA for account access.

Willingness to Engage MFA by Account Type



Willingness to Use MFA vs. Knowledge of MFA



MFA Adoption Linked to Frequent Usage

Consumer willingness to use accounts that require MFA increases with more frequent usage.[3] Consumers who say they regularly use MFA are 27% more willing to use MFA than consumers who say they are knowledgeable about MFA but have never used it, and 30% more willing than consumers who are completely unfamiliar with the term.

TAKEAWAY #1

Consumers overwhelmingly say they are willing to engage with businesses and institutions that require them to use MFA to access their accounts. In practice, even more continue to use MFA-required accounts than than those who say they are willing to do so. **This suggests that businesses are unlikely to lose customers by requiring them to use MFA.**

[2] We asked survey respondents to rate their "willingness to engage with two-factor authentication measures when dealing with different types of online accounts" on a scale from 1 ("not at all willing") to 10 ("extremely willing"). Ratings of 7 or higher were considered "willing" responses, 4 and lower were considered "unwilling," and scores of 5 or 6 deemed "neutral." Unless otherwise shown, percentages are based on the total of all responses, regardless of account type, and exclude responses of "I do not use this platform."

[3] We asked survey respondents to "indicate your awareness and knowledge of" various cybersecurity measures. The results here are for awareness and knowledge of two-factor authentication.

KEY FINDING #2

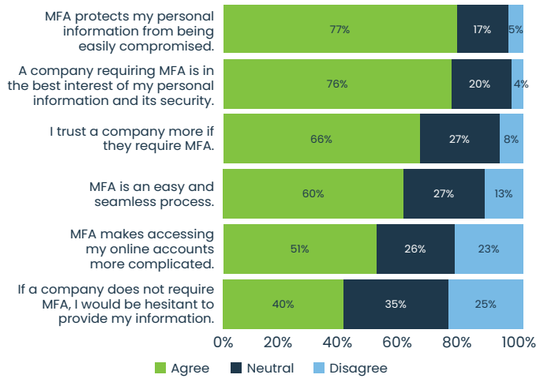
MFA BUILDS CONSUMER TRUST

Trust, Protection, and Security

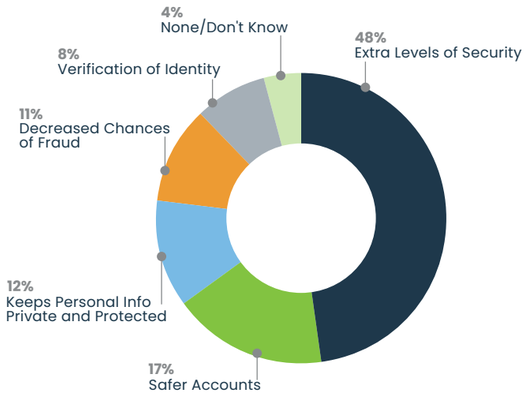
We polled consumer sentiments about MFA.[4] More than three-quarters of consumers feel that MFA protects their personal information, and that it is in the best interest of their personal information and its security for a company to require MFA. Nearly two-thirds also say they trust a company more if it requires MFA.

While not a majority, another 40% of consumers would be hesitant to provide their information to a company that does not require MFA.

How much do you agree or disagree with the following statements?



What is the single largest benefit of an online site requiring MFA?



Consumer Perceptions of MFA Benefits

When asked to pinpoint the primary advantage of MFA,[5] nearly half of consumers highlight the added layers of security it provides for their information. Only 4% of consumers are unable to identify at least one benefit of MFA, demonstrating its widespread recognition among the general population.

TAKEAWAY #2

Rather than *losing* customers through mandatory MFA, businesses may lose some by not securing consumer accounts. **Most consumers value MFA's protection and are likelier to trust entities offering this added security**. Many would hesitate to share personal information with entities lacking MFA protection.

[4] We asked survey respondents to rate how much they agreed or disagreed with six statements about MFA (the questions used "two-factor authentication" instead of MFA) on a scale from 1 ("Strongly disagree") to 5 ("Strongly agree"). Scores of 1 or 2 were labeled "disagree," 3 was labeled "neutral," and 4 or 5 were labeled "agree."

[5] In Spring 2022, we asked survey respondents, "What are the biggest benefits of an online site requiring two-factor authentication?" as an open-ended question. Analysts categorized each response by theme. We presented the resultant themes as options to survey respondents in Fall 2023 for the question, "What is the single largest benefit of an online site requiring two-factor authentication?"

KEY FINDING #3

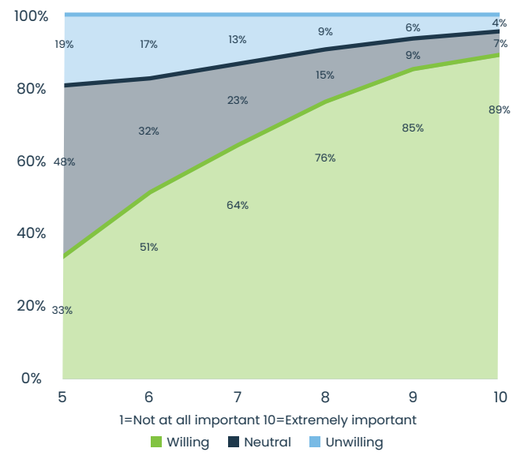
SECURITY AWARENESS DRIVES ACCEPTANCE

MFA Acceptance Revolves Around Awareness

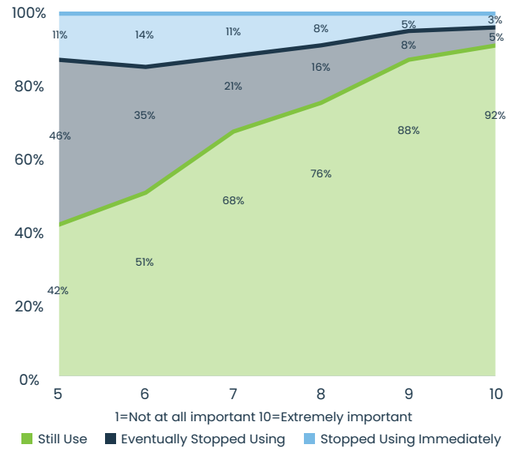
The key factors distinguishing consumers who accept MFA from those who do not largely revolve around digital security awareness and behavior. This suggests that individuals with a heightened appreciation for cybersecurity and an understanding of data protection are more likely to embrace MFA.

We asked consumers to rate the importance of strong digital security measures for different types of accounts.[6] As consumer feelings about the importance of securing accounts rise from moderate (5 out of 10) to very high (10 out of 10), willingness to use MFA also increases—by 56%.

Willingness to use MFA by Average Rating of the Importance of Strong Digital Security Measures for Online Accounts



How did you respond when discovering that MFA was required? vs. Average Importance of Strong Digital Security Measures

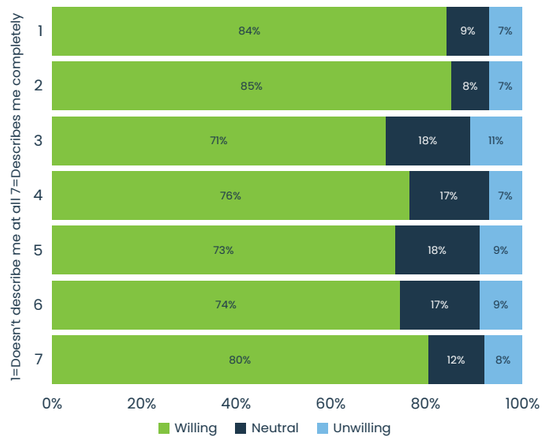


Security Importance and MFA Acceptance

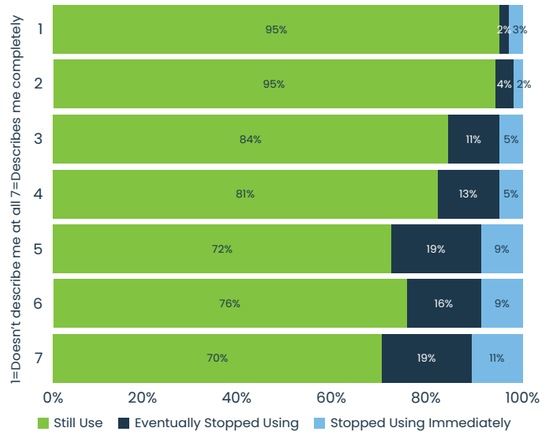
How consumers respond when required to use MFA for an account mirrors their willingness to use MFA. Consumers that rate highly the importance of strong digital security continue using MFA-required accounts 50% more often than those who give it the lowest importance.

[6] We asked survey respondents to rate the importance of strong digital security measures, on a scale from 1 (not at all important) to 10 (extremely important), for eight account types: financial institutions, healthcare providers, online merchants/stores, personal email, social media, school/educational institutions, employer accounts, and government institutions. The results are based on the average rating per respondent, rounded to the nearest whole number. The total number of respondents whose ratings averaged 4 or less made up less than one percent of all responses, so those values are excluded from the results.

Willingness to Use MFA vs. Agreement with "Computer security/cybersecurity is too complicated or hard to understand."



How did you respond when discovering that MFA was required? vs. Agreement with "Computer security/cybersecurity is too complicated or hard to understand."



Understanding of Cybersecurity and MFA Usage

We also asked consumers to rate their own understanding of cybersecurity.[7] There is no clear pattern connecting consumer willingness to use MFA with their understanding of cybersecurity. However, there is a clear trend to how consumer understanding of cybersecurity impacts their actions in practice—those who feel cybersecurity isn't too hard to understand continue using MFA-required accounts 25% more often than consumers who feel cybersecurity is too complicated.

Interestingly, this data suggest that consumers who express limited understanding of cybersecurity are likely less accepting of MFA in practice than they claim and consumers who express confidence in understanding cybersecurity are likely more accepting in practice than they claim—both by about 10%.

TAKEAWAY #3

Consumers who value cybersecurity and understand its importance are more accepting of MFA than those who find cybersecurity complicated or believe their information is not important to protect. While there is little resistance to using MFA, these findings suggest that **businesses and institutions can overcome any remaining resistance by educating consumers** about the importance of protecting their information with cybersecurity practices.

[7] We asked survey respondents how well the statement, "Computer security/cybersecurity is too complicated or hard to understand," describes them on a scale from 1 ("doesn't describe me at all") to 7 ("describes me completely").

KEY FINDING #4

CONSUMERS PREFER METHODS THEY KNOW

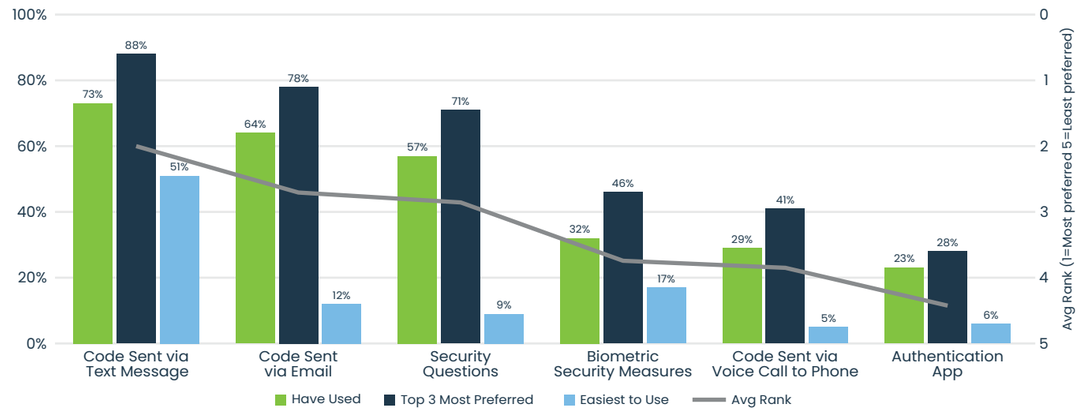
Preferences and Familiarity with MFA Methods

We polled consumers a few different ways to gauge their preferred MFA methods. For the most part, preferences track closely with familiarity. That is, consumers prefer to use methods they have previous experience using.

Familiarity even trumps ease of use. More consumers (17%) chose biometrics as the easiest method to use than having a code sent by email (12%) or answering security questions (9%). However, the latter two methods rank ahead of biometrics in both consumer experience and consumer preference.

The chart below compares consumers' experience using MFA methods with their stated preferences[8] and the methods they find easiest to use.[9]

MFA Method Preferences



[8] We asked survey respondents, "If two-factor authentication is required when engaging in online business, which authentication method would you prefer?" They ranked each of six MFA methods from most preferred to least preferred. The chart reflects two values calculated from these rankings: the percentage of respondents who listed each method among their top three most preferred choices, and the average rank (between 1 and 6, 1 being most preferred) respondents assigned to each method.

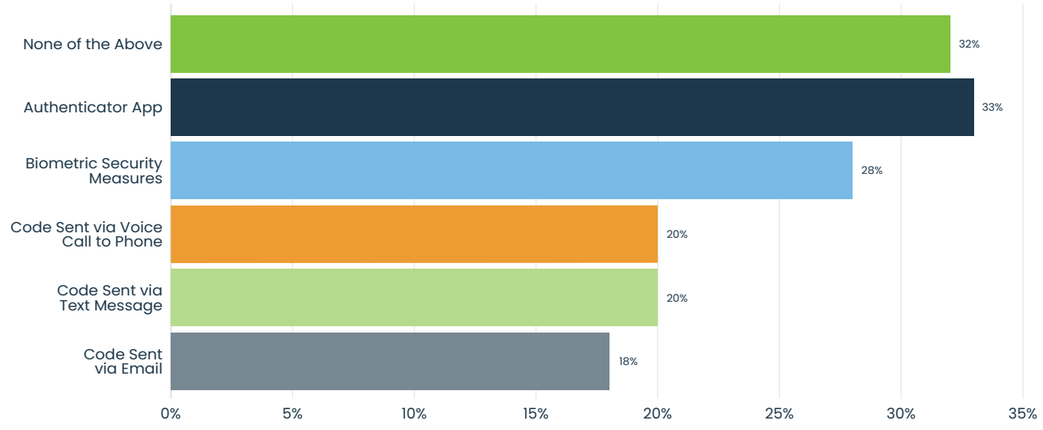
[9] We asked survey respondents which MFA method was easiest to use. They could choose one option.

Impact of MFA Methods on Consumer Engagement

When asked which MFA methods—if required to engage a business online—would stop them from engaging with that business, roughly one third (32%) indicate no method would stop them from engaging, and no more than one third of consumers say any one method would be a deal-breaker.[10]

These numbers appear to inflate consumers' preparedness to stop using services that require MFA. At best, 18% of consumers say one method (having a code sent by email) would cause them to stop engaging a business. That proportion is three times higher than the number (6%) who have immediately stopped using an account that required any type of MFA.

Which required MFA methods would cause you to stop engaging in online business with that platform?



TAKEAWAY #4

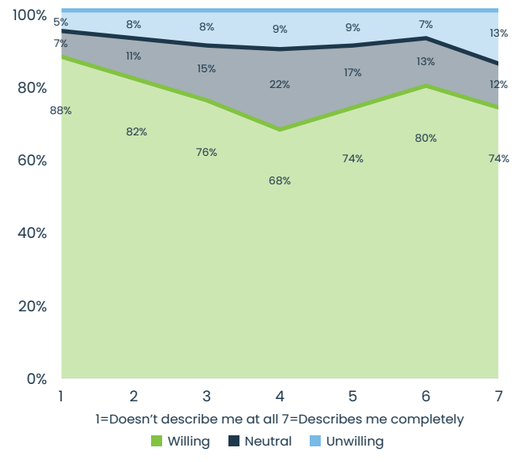
While it is important for businesses and institutions to be responsive to consumer preferences regarding MFA methods, these findings suggest that **consumer familiarity is an important factor in consumer acceptance.** That is, as market penetration of newer MFA methods (like biometrics and authentication apps) increases, so too may consumer acceptance of those methods when required for account access.

[10] We asked survey respondents, "Which required two-factor authentication methods would cause you to stop engaging in online business with that platform?" Options included five MFA methods and "None of the above would cause me to stop engaging in online business should they be required." Other than "none of the above," respondents could select multiple options, so values will total greater than 100%.

KEY FINDING #5

CONVENIENCE REDUCES MFA FRICTION

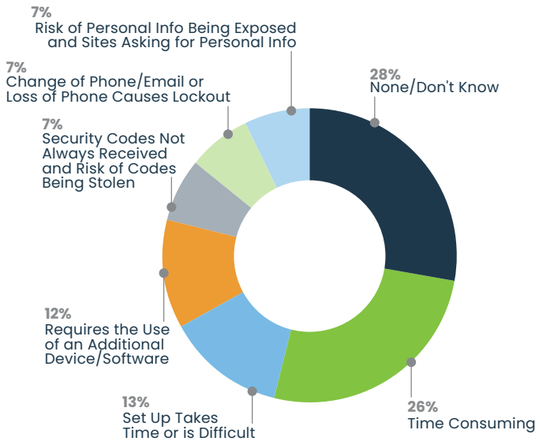
Willingness to Use MFA vs. Agreement with "I think that many websites make transactions too difficult by asking security questions or requiring access codes."



Concerns about MFA Difficulty

We polled consumers on their agreement with the statement, "I think that many websites/apps make transactions too difficult by asking security questions or requiring access codes."[11] 54% of consumers agree with that statement, while only 24% disagree. Consumers who most strongly agree that these MFA methods make transactions too difficult are 14% less willing to use MFA than consumers who most strongly disagree with the same statement.

What is the single largest challenge of an online site requiring MFA?



Challenges with MFA Adoption

We also asked consumers what the largest challenge is of using a site that required MFA. While a small plurality say there is "none" or don't know, the biggest complaints consumers have is that MFA is time consuming, that setup takes time or is difficult, or that it requires the use of an additional device or additional software.[12] These three concerns, related to convenience and ease of use, take precedence over consumer apprehensions regarding MFA issues—such as malfunctioning, account lockouts, or the need for personal information.

[11] We asked survey respondents how well the statement described their lifestyle and technology usage on a scale from 1 ("doesn't describe me at all") to 7 ("describes me completely"). For analysis purposes, agreement was considered any score 5 or higher and disagreement was any score 3 or lower.

[12] In Spring 2022, we asked survey respondents, "What are the biggest challenges of an online site requiring two-factor authentication?" as an open-ended question. Analysts categorized each response by theme. We presented the resultant themes as options to survey respondents in Fall 2023 for the question, "What is the single largest challenge of an online site requiring two-factor authentication?"

TAKEAWAY #5

Ease of use and convenience are top concerns for consumers who are more reluctant to use MFA. As businesses and institutions roll out MFA, they may want to consider emerging techniques—like passkeys, in-app notifications, and remembered devices—that simplify MFA for consumers.

FINAL THOUGHTS

We began this study with the question, "What would happen if more users were required to employ MFA to prevent unauthorized account access?" Our research shows that an overwhelming majority of consumers accept MFA and are willing to use accounts that require it. Contrary to potential fears that requiring MFA might cause consumers to turn away from engaging with businesses or institutions online, consumers appreciate the added protection of MFA and are more likely to trust businesses and institutions that demonstrate their committment to safeguarding their personal information.

Consumer resistance to using MFA is minimal. Our research suggests that increasing consumer awareness of the risks of account compromise and the importance of securing their accounts may overcome that resistance. Consumers express greater willingness to use MFA when they use it regularly and prefer methods they have used in the past, suggesting that consumers become more accepting of MFA with more exposure and familiarity. Businesses and institutions can also reduce friction to consumer acceptance by prioritizing convenience and ease-of-use when implementing MFA.

Methodology

Respondents were sourced from an online panel company and screened on the following criteria:

- Reside in the United States with geographical dispersion consistent with the population
- Ages 18-75
- Regularly use the internet to conduct personal business such as banking, booking travel, purchasing consumer goods and services, monitoring health services, social media, etc.
- No minimum income requirement for the survey, but had quotas for income groups under $25k, $25k-$49k, $50k-$75k, $76k-$100k, over $100k, as determined by the U.S. Census figures.
- Mix of gender, race, and ethnicity consistent with screening criteria above.

> **The security field recognizes MFA's significance in protecting accounts. It's time to shift from encouraging consumers to voluntarily adopt MFA to assisting them when it's mandated. I believe consumers are prepared for this transition.**
>
> —Kristin Judge, CSN Founder

WHAT TO EXPLORE NEXT

Good research presents new questions that should be asked in order to learn more about idea execution and educational messaging. The following questions could be asked as a follow-up to this survey:

Conclusion #1: Willingness varies by account type, with more users willing to use MFA, for example, to interact with government institutions than for accessing social media platforms.

Future survey question #1: What do social media platforms have for educational messaging on the importance of using MFA? Do consumers know about social media hacks and the consequences?

Conclusion #2: There is a clear trend to how consumer understanding of cybersecurity impacts their actions in practice—those who feel cybersecurity isn't too hard to understand continue using MFA-required accounts 25% more often than consumers who feel cybersecurity is too complicated.

Future survey question #2: Of people who don't want to use MFA, would they use it if someone they trusted showed them how? Would they use it if they knew it took less time than expected?

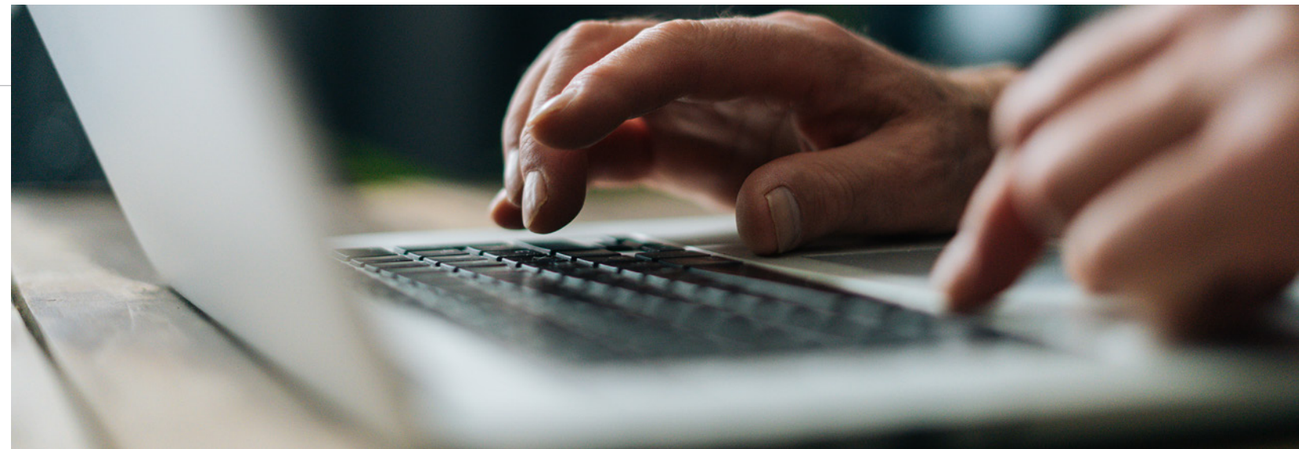
Conclusion #3: More than three-quarters of consumers feel that MFA protects their personal information and that it is in the best interest of their personal information and its security for a company to require MFA. Nearly two-thirds also say they trust a company more if it requires MFA.

Future survey question #3: Ask consumers that have stopped using online accounts what their reasons were for ceasing engagement - such as technical issues, inconvenience, or difficulties related to MFA, or something else.

Educational Messaging

Since the biggest complaints consumers have is that MFA is time consuming, setup takes time or is difficult, or it requires the use of an additional device or software, educational messaging should change.

The security community should test educational campaigns that address how little time MFA takes, emphasize the ability to remember a browser or stay signed in, and teach how to use MFA in existing infrastructure they already use.



Cybercrime Support Network (CSN) is a 501(c)(3) nonprofit organization whose mission is to serve individuals and small businesses impacted by cybercrime.

Clear Mission Consulting partners with nonprofits to amplify their mission impact with smarter strategies by integrating effective strategic planning with inclusive leadership practices.

Supported by

COMCAST

Study Design

Integrated Insight and Cybercrime Support Network

Analysis and Report Author

David Wagner, Clear Mission Consulting

Report Design

Karissa Brumley, Cybercrime Support Network

FightCybercrime.org