HAVE YOU HEARD ABOUT MULTI-FACTOR AUTHENTICATION (MFA)?

Multi-factor authentication (MFA), or two-factor authentication (2FA), is a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify a user's identity for login. MFA increases security because even if one credential becomes compromised, unauthorized users will be unable to meet the second authentication requirement and will not be able to access the targeted physical space, computing device, network, or database.

SOURCE: https://www.cisa.gov/publication/multi-factor-authentication-mfa

HOW DOES IT WORK?
These additional layers lead to the term of 'multi-factor authentication' or MFA and can include three elements:

- **Things you know**—such as a password or other personally-known information such as the answers to security questions
- **Things you have**—such as an ID badge with an embedded chip, or a digitial code generator
- **Things you are**—such as physical traits like your fingerprints or voice

SOURCE: https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication

BY THE NUMBERS

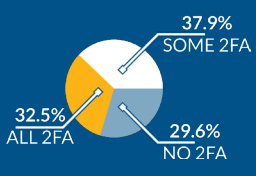
2FA USE

79% IN 2021

28% IN 2017

79% of respondents reported using 2FA in 2021, a significant increase compared to the **28%** of respondents who used 2FA in 2017.

Around one-third of respondents reported using 2FA for all applications, while **37.9%** only used it for some. The remaining **29.6%** reported no use of 2FA.



Respondents ranked financial accounts as the account category of highest concern should an unauthorized person gain access. Health accounts ranked fourth behind social media and email.

53% of respondents preferred SMS for the second factor they would choose for a new account and **20%** chose email as their preference.

SOURCE: 2021 Duo Labs Report: State of the Auth Experiences and Perceptions of Multi-Factor Authentication

LOOKING FOR MORE INFORMATION?

Check out the resources below!

HHS 405(d)—Aligning Health Care Industry Security Approaches

The HHS 405(d) Program aims to enhance cybersecurity and align industry/sector approaches by developing best practices and mitigation strategies to attack the most common cyber threats facing the healthcare and public health sector. The *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)* publication includes practices related to access management and multi-factor authentication. MFA for email system configuration is discussed in practice 1.S.A of Technical Volume 1. Remote access with MFA is discussed in practice 2.S.A of Technical Volume 1 and practices 1.M.B, and 3.M.D of Technical Volume 2.

RESOURCES

HICP Main Document

HICP Technical Volume 1

HICP Technical Volume 2

Health Sector Cybsersecurity Coodination Center (HC3)

HC3 provides recommendations and mitigation strategies, like multi-factor authentication, for protecting the sector against cyber threats, especially threats that impact patient safety, security, and privacy. For more information, please email HC3@hhs.gov.

RESOURCES

HC3 Intelligence Briefing Multifactor Authentication

Utilizing Two Factor Authorization

Department of Homeland Security (DHS)—Cybersecurity & Infrastructure Security Agency (CISA)

In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an important homeland security mission. CISA leads the Nation's strategic and unified work to strengthen the security, resilience, and workforce of the cyber ecosystem to protect critical services and American way of life. Check out this fact sheet from CISA on MFA and the rest of the resources and support they provide to prevent and recover from cyber attacks.

RESOURCES

CISA Multi-factor Authentication Fact Sheet

National Institute of Standards and Technology (NIST)

NIST was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories. Today, NIST measurements support the smallest of technologies to the largest and most complex of human-made creations — from nanoscale devices so tiny that tens of thousands can fit on the end of a single human hair up to earthquake-resistant skyscrapers and global communication networks. The practices found in HICP, like enabling multi-factor authentication, are largely based on NIST frameworks.

RESOURCES

Back to Basics: What's multi-factor authentication—and why should I care?

Small Business Cybersecurity Corner: Multi-Factor Authentication

U.S. Federal Executive Branch—The White House

In 2021, the White House published the "Executive Order on Improving the Nation's Cybersecurity" calling for the federal government to take action toward protecting our Nation from malicious cyber actors and partner with the private sector to foster a more secure cyberspace. This executive order included the implementation of multi-factor authentication.

RESOURCES

Executive Order on Improving the Nation's Cybersecurity

Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technologies Anne Neuberger, September 2, 2021