What is MFA and Why It’s a Good Thing?

What is MFA:

Multi-factor Authentication (MFA) is a multi-step account login process that requires the user to provide two or more verification factors to gain access to a resource such as an application, website, or a VPN. One verification factor is typically your username and password (something you know). The other could be something you have (e.g., a cellphone or key card) or something you are (e.g., fingerprints or some other biometric data to prove who you are). MFA is a core component of a strong identity and access management policy.

Why MFA is Good to Have:

We all use passwords to gain entry into our email systems, work databases, and bank accounts. We are usually forced to change our combinations periodically in the hopes that we'll stay just a bit safer. But the truth is that passwords aren’t secure enough anymore, regardless of how complex they are. Hackers have developed countless methods of stealing credentials to gain unauthorized access to private accounts and data.

MFA provides an additional layer of defense to a user’s account and makes it more difficult for unauthorized parties or hackers to access. By requiring people to confirm identity in more than one-way, multi-factor authentication provides a greater assurance that they really are who they claim to be—which reduces the risk of unauthorized access to sensitive data.

Given the realities of today’s security landscape and the addition of government regulations that protect individuals’ data, many organizations have already adopted MFA. As compliance standards continue to change, MFA’s presence will become even more common. Given its ease of use and the protection it provides, cancer registries should use MFA to access any sensitive data.

How does it work?

A typical MFA process uses an authenticator (or authentication) app, and the process looks like this:

- Registration: A person creates an account with the authenticator app that is also linked to a secure system and establishes a username and password. They then link an item, such as a cellphone, to the account and asserts that this item is theirs.
- Login: a person enters a username and password, as they typically would, to access a secure system.
- Verification: They system connects with the registered item. Phones might ping with verification codes, or key fobs might display the current individualized code.
- Reaction: The person completes the MFA process with the verified item. Entering verification codes or accepting a verification “push” on a phone are common next steps.

Other resources describing MFA can be found here: https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication

Primary author: Don Green, Information Management Services, Inc.
Editors: NAACCR Data Security and Confidentiality Workgroup

Date updated: 2023-01-26