Cloud Destinations

Embrace Cloud Multiverse

Multi-Factor Authentication Awareness

OVERVIEW

Multi-factor authentication (MFA) is a layered approach to securing physical and logical access where a system requiresa user to present a combination of two or more different authenticators to verify a user's identity for login. MFA increases security because even if one authenticator becomes compromised, unauthorized users will be unable to meetthe second authentication requirement and will not be able to access the targeted physical space or computer system.

WHY IS MFA IMPORTANT?

Implementing MFA makes it more difficult for a threat actor to gain access to business premises and information systems, such as remote access technology, email, and billing systems, even if passwords or PINs are compromisedthrough phishing attacks or other means.

Adversaries are increasingly capable of guessing or harvesting passwords to gain illicit access. Password cracking techniques are becoming more sophisticated and high-powered computing is increasingly affordable. In addition, adversaries harvest credentials through phishing emails or by identifying passwords reused from other systems. MFAadds a strong protection against account takeover by greatly increasing the level of difficulty for adversaries.

HOW DOES MFA WORK?

MFA requires users to present two or more authentication factors at login to verify their identity before they are grantedaccess. Each additional authentication factor added to the login process increases security. A typical MFA login would require the user to present some combination of the following:

- Something you know: like a password or Personal Identification Number (PIN);
- Something you have: like a smart card, mobile token, or hardware token; and,
- Some form of biometric factor (e.g., fingerprint, palm print, or voice recognition).

For example, MFA could require users to insert a smart card or a bank card into a card reader (first factor) and then entera password or a PIN (second factor). An unauthorized user in possession of the card would not be able to log in without also knowing the password; likewise, the password is useless without physical access to the card.

Consider enforcing MFA on Internet-facing systems, such as email, remote desktop, and Virtual Private Network (VPNs). Implementation schedules, costs, adoption willingness, and the degree of protection provided vary depending on the solutions selected and the platforms to be protected, so match the capability to the need.