kyndryl

Additional layers of security are necessary to protect your data

Multifactor Authentication (MFA) is an additional layer of authentication that requires two or more pieces of identity evidence.[1]

MFA is like an additional "locked door" to your account, a cyber-attacker would need to break through, which helps with:

- Slowing down or even preventing account attacks.
- Avoiding having your identity stolen. Protecting yourself in case your password is weak or stolen.[2]

Did you know?

Over 80% of cyber breaches happen due to weak or stolen passwords.

Alternative MFA methods can block 90% of targeted attacks, 99% of bulk phishing attacks and 100% of automated bot attacks.[3]

You could be the biggest defender with an MFA, but also the biggest risk to your account without one.

Is "SMS code" strong enough as an MFA factor?

You try to log into your account, but you must enter a special one-time code sent via SMS, along with your password to complete the authentication process. You are thinking this should be secure enough.

Unfortunately, there have been many cases where an attacker was able to bypass SMS as an MFA factor, obtain the SIM information from cell phones and convince the carriers to move the cell phone number to the attacker's cell phone. That's how they get your number, text messages and more. They use this information as MFA to reset your passwords and get control over your account.

There are multiple ways you can prove you are who you are:[4]

1 **Push Notifications** are sent to user's mobile device or app. After receiving the notification, the user approves or denies the login attempt, typically by tapping a button or entering a PIN.

2 **Mobile Apps** like Google Authenticator, Microsoft Authenticator, provide users with auto-generated, time-based one-time passwords (OTPs) that change periodically.

3 **Biometric Authentication:** Fingerprints, facial recognition, or iris scans can be used as authentication on devices equipped with biometric sensors.

4 **Security Questions:** Alongside a password, users answer predefined security questions during login. These questions are typically personal and known only to the user.

5 **Voice Recognition** systems analyze the user's voice patterns to verify their identity. Users speak a passphrase or specific phrases, and the system matches their voice against enrolled voiceprints.

6 **SMS/text or email codes**: a one-time verification code, which should be avoided as single-factor password only type of mechanism.

Recommendation: not to have SMS as a sole MFA. If you are using one, add another type of MFA, if possible.

For more information, explore more references and visit the following pages:

1. Video: Multi-factor authentication.
   https://www.getcybersafe.gc.ca/en/resources/video-multi-factor-authentication
2. Turn on multi-factor authentication.
   https://twitter.com/Kyndryl/status/1714657818870006185
3. 84 Must-Know Data Breach Statistics [2023].
   https://www.varonis.com/blog/data-breach-statistics#:~:text=81%20percent%20of%20confirmed%20breaches,following%20two%20years%20(IBM)
4. Multi-Factor Authentication: Who Has It and How to Set It Up.
   https://www.pcmag.com/how-to/multi-factor-authentication-2fa-who-has-it-and-how-to-set-it-up

This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice. Not all offerings are available in every country in which Kyndryl operates. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.