MFA – What is MFA and Why Use It?

More than a Password - Protect Yourself from Malicious Hackers with Multifactor Authentication

Ever worry about getting hacked?

Your password isn't protecting you the way you think it is. Especially if someone can guess your password from looking at your social media. But let's say you have a complex password – or a password manager even – unfortunately malicious cyber actors still have ways to get past your password. And once they're in your accounts… you can wave bye-bye to your money, and possibly your identity.

So, what do you need? More than a Password! A second method to verify your identity.

Multifactor authentication (MFA) can make you much more secure. Taking the extra step beyond just a password can protect your business, online purchases, bank accounts, and even your identity from potential hackers.

Different ways to say MFA:

- Multifactor Authentication
- Two Step Authentication
- 2-Step Verification
- Two Factor Authentication
- 2FA

What is Multifactor Authentication?

Prove it's you with two! … Two step authentication, that is.

MFA is a layered approach to securing your online accounts and the data they contain. When you enable MFA in your online services (like email), you must provide a combination of two or more authenticators to verify your identity before the service grants you access. Using MFA protects your account more than just using a username and password.

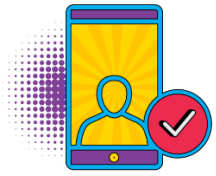
Users who enable MFA are significantly less likely to get hacked. Why? Because even if a malicious cyber actor compromises one factor (like your password), they will be unable to meet the second authentication requirement, which ultimately stops them from gaining access to your accounts.

June 2024

Online services want to make sure you are who you say you are, and—more importantly—they want to prevent unauthorized individuals from accessing your account and data. So, they are taking a step to double check. Instead of asking you just for something you know (e.g., a password)—which can be reused, more easily cracked, or stolen—they can verify it's you by asking for another piece of information:

They'll ask for …

Something You Know *(Like a PIN number or a password)*



Something You Have *(Like an authentication application or a confirmation text on your phone)*

Something You Are *(Like a fingerprint or face scan)*

How Do I Enable MFA?

Now that you know what it is, you'll see prompts for multifactor authentication all over. So whenever available, be sure to opt in.

Start by looking at the security settings on your most-used accounts. You may see options to enable MFA listed as "Two Factor Authentication," "Multifactor Authentication," or "Two Step Factor Authentication." There are many ways you may be asked to provide a second form of authentication.

Popular forms of MFA include:

- Text message (SMS) or voice message
- Application-based MFA
- Phishing-resistant MFA
- Fingerprint authentication or face scan

Where to implement MFA:

- Email accounts
- Financial services
- Social media accounts
- Online stores
- Gaming and streaming entertainment services

If you don't see a prompt for multifactor authentication on one of these accounts, send a note to each company asking them to enable the feature. After all, it's your security at stake!

Why Should My Organization Enable MFA?

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

Malicious cyber actors are increasingly capable of phishing or harvesting passwords to gain unauthorized access. They take advantage of passwords you reused on other systems. MFA adds a strong protection against account takeover by greatly increasing the level of difficulty for bad actors.

If your organization does not already have MFA implemented on your accounts (including Microsoft 365), reach out to your IT Support group and recommend that they help deploy the technology.

Summary

Strong authentication via MFA is critical and should be implemented across all networks, systems, applications, and resources to adequately protect the organization.

June 2024