Cybersecurity: Multifactor authentication

Add extra protection to your accounts.

What is it?

Multifactor authentication (MFA) is a way to add an extra layer of protection to your accounts, including your email or online banking.

MFA requires that you provide at least two pieces of evidence, also known as factors, before you can log into an online account. This might include a combination of different factors, such as:

- **Something you know:** This is the password or PIN you created for the account.
- **Something you have:** Usually, this is a single-use code or password that is temporarily assigned to your account and expires immediately after use. You may receive these codes through a soft token, like a text or an app notification, or a hard token, like a USB key assigned to you.
- **Something you are:** This is your personal biometric information, like a scan of your fingerprint, iris, or retina.

How does it work?

When logging into an MFA-enabled account, you will first enter your username and password. If correct, you will be asked to provide a second factor.

Some organizations will require a second factor every time you log in. Others may only ask if you access the services from a new device or application, including browser.

Why should I use MFA?

MFA reduces the likelihood that an attacker will gain access to your account by requiring two pieces of evidence when logging in.

When a website is breached in a cyberattack, compromised but otherwise valid username and password combinations are often bought and sold online.

Cybercriminals know that most people reuse the same password on more than one account, and they try to use that to their advantage. In a tactic known as brute force attack, they may try to enter a compromised username and password combination on other popular websites to gain access to the information.

For example, a cybercriminal may use a username and password combination stolen from an online retailer to try gaining access to the main email account. If successful, they can change the password, lock you out of your account, request services in your name, and potentially access your personal or credit information.

How do I enable MFA?

Log into an account and go to the settings to see if MFA is available.

In most cases, you will have to enable MFA manually, but some applications or websites may send you a push notification inviting you to enable FMA to protect your account and information further.

MFA is not available on every service or account. Organizations may also use another name, such as two-step verification or two-factor verification.

Where should I use MFA?

Consider applying MFA to as many accounts as you can. At minimum, you should enable it on your email account(s) because, often, they are connected to personal services you may access, including government benefits.