Multi-Factor Authentication

In This Module

- What is Multi-Factor Authentication?
- Why is it useful?
- How can you start using it?

What Is Multi-Factor Authentication?

Multi-Factor Authentication (MFA) is an authentication method that keeps your data safe by requiring two or more pieces of information about you:

- Something you know (a password or passphrase)
- Something you have (a fingerprint, your face, your phone, etc.)

It is a important component of digital security because it can make it harder for people to gain unauthorized access to your account

How to Start Using MFA

Look for options to set up MFA on different sites that you use. Many sites now have options to enable MFA and encourage users to do so.

Consider MFA for places where you have particularly sensitive data, such as your email account or financial services and banking sites.

Common Forms of MFA

After entering your password, you can use these methods for an extra layer of security:

- SMS Token
- Email Token
- Software Token
- Phone Authentication
- Biometric Authentication

More information about each of these methods can be found on your handout.

Activity

Use the handout provided to think through the sites and apps you currently use. Is MFA available to you? Is it set up on your accounts? Would you like it to be?

Takeaways

- Multi-Factor Authentication is a great way to add a layer of security to your online accounts
- Consider setting up MFA for accounts where you have particularly sensitive or valuable information stored
- Think about what method works best for you as well. For example, if you don’t always have your phone with you, you might want to avoid MFA methods that rely on you having access to your cell phone

Questions?

NYC Digital Safety

Privacy & Security