Enable Two-Factor Authentication

Introduction

Two-factor authentication is an identity confirmation method that necessitates users to provide two forms of authentication, like a password and a one-time passcode (OTP), to verify their identity and access an online account or other vulnerable resources.

You can use one of your personal devices or accounts to enable two-factor authentication. This activity can be accomplished using a Windows machine, a Google account, or a Mac.

Learning objectives

After completing this activity, you will be able to:

- Enable two-factor authentication for a Microsoft account
- Activate two-factor authentication for a Google account
- Set up two-factor authentication on a Mac

Instructions

Complete one or more of the following exercises based on your devices and accounts.

Enable two-factor authentication for a Microsoft account

1. Visit https://account.microsoft.com/
2. Log in with your username and password.
3. From the top menu, select the **Security** tab.
4. In the **Security** tab, select **Advanced Security Options**.
5. Click **Add a new way to sign in or verify**.
6. You will see various methods to verify your identity. Select one of these options and follow the prompts to enable two-factor authentication for your Microsoft devices.

Activate two-factor authentication for a Google account

1. Visit myaccount.google.com
2. From the navigation panel on the left, select **Security**.
3. Under **How do you sign into Google,** select **2-Step Verification**.
4. Select **Get started**.
5. Follow the prompts to enable two-factor authentication for your Google accounts.

Set up two-factor authentication on a Mac

1. On your Mac, select the Apple menu.
2. Select **System Settings**.
3. From the top of the sidebar, select your name. If your name is not visible, select **Sign in with your Apple ID**. Then, enter your Apple ID and password.
4. Click **Sign-In & Security**.
5. Next to **Two-Factor Authentication,** select **Turn on**.
6. If prompted, enter your Apple ID and password again.
7. Provide answers to your security questions, and then click **Continue**.
8. Follow the prompts to enable two-factor authentication on your Apple devices.

For this activity, I reviewed the process of enabling two-factor authentication (2FA) on personal accounts and verified that 2FA was already active across the platforms listed in the lab.

My Google account has had 2-Step Verification enabled for several years. It uses a combination of password + mobile app (Google Authenticator) to generate one-time passcodes when signing in from unrecognized devices. I also receive security alerts and activity confirmations via backup email and text, which reinforces account integrity.

On the Microsoft side, I previously configured 2FA through the Microsoft Authenticator app. This includes push notifications and backup verification via trusted device prompts. The security dashboard under "Advanced Security Options" confirms that multiple secure sign-in methods are already in place and active.

As for Apple — I don't use it. Their 2FA system has a history of being overly controlling while still managing to have security flaws. Between locked-out users and random trust device bugs, I've learned to keep my distance. Google and Microsoft have handled identity verification far more reliably in my experience.

Since I had already completed all the required configurations, I used this activity as a quick audit to confirm that recovery options, trusted devices, and verification methods were still accurate and up to date.