Securing your Google Account

Purpose
This article contains a few suggestions on how to secure your Google Account.

Make use of the Google Account Security Check
When you access your Google Account, on the left hand side there is a link to Security.

If you see a message like Security issues found, click on Secure Account link...
From here, you can review any potential issues, such as apps accessing your Google Account, devices that are accessing it and verifying 2-Step Verification.

It is always good to review this once in a while to make sure everything looks to be in order.

Set Recovery Information

It is helpful to set a Mobile Phone Number and a secondary email address to help notify you when the account has been accessed by another machine.

One thing to be careful of when you do set this up, is to pay strict attention to the message you are receiving.

The message will identify a general location and device name that is making the attempt.

If this is not something you allowed, you should access your Google Account manually (IE: Don’t click the link, go to a browser and go to https://www.gmail.com and log in there and verify the situation.

Set up 2-Step Verification

You can setup 2-Step Verification which will help in verifying an actual attempt to connect.

In this example, a user has it set to send a Google Prompt on their Phone to ask for verification.

They also set up the Google Authenticator App as an alternative.

For more on this, please refer to Two-Factor, Two-Step or Multi-Factor Authentication.
Alternative Second Step methods

Google also provides alternative methods for 2-Step Verification such as **Backup Codes**, which is a printable set of numbers that can be used.

**Security Key** is another alternative, using systems like YubiKey, which is basically a hardware key that can be plugged into a computer or mobile device to act as a second verification.

Related articles

- How to use Zoom
- Working From Home
- Connecting to a Network/Samba Share
- UFW - Basics
- Digital Piracy