2-Factor Authentication

https://www.weymouth.ma.us/technology-services/pages/technology-class-materials

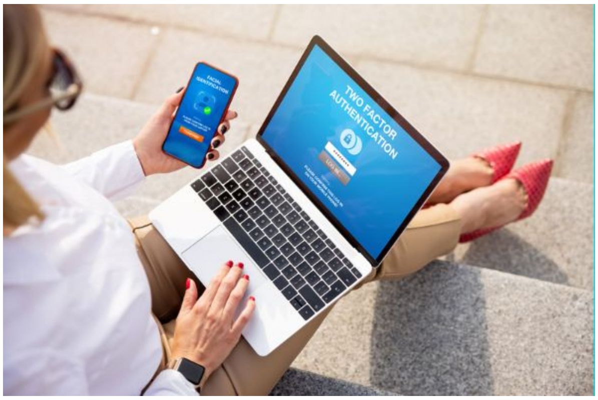
WEYMOUTH
PUBLIC LIBRARIES

2-factor authentication is a security feature for online accounts (such as email) that require a password.

If your account only had a password, someone who knows your password could access your account.

With 2-factor authentication, you have to provide an additional piece of information to access your account.

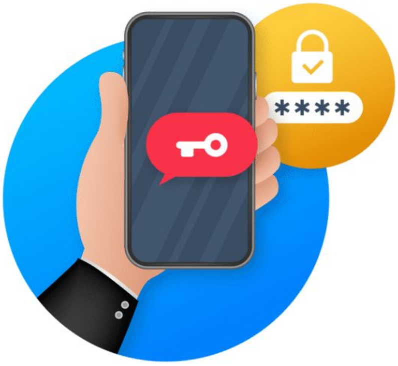
Typically this other piece of login information is sent to your phone.



Unlike your account password, a 2-step verification code is *temporary* and *one-time use*.

It is also *time-sensitive* and will *expire*.

A new code is sent to you every time you need to sign in.



What kinds of website accounts require 2-factor authentication?

- Email
- Accounts with personal information
- Accounts with financial information

Typical 2-Factor Authentication Code Sign In Process

- Go to your email provider in a web browser (gmail.com, yahoo.com, etc.)
- On the sign in screen, type in your email address.
- Then type in your password.
- At this point, you will usually get a prompt to send a 2-factor authentication code to your phone.
    - Remember: A 2-step authentication code is *temporary* and *one-time use*. It is also *time-sensitive* (i.e. it will *expire*).

https://edu.gcfglobal.org/en/thenow/what-is-twofactor-authentication/1/

When will I need to enter a 2-factor authentication code?

- Everytime you sign in to your account (if you’ve set it up that way or the website requires it).

- When you haven’t signed in to your account for a while.

- When you’re signing in to your account on a new device or a device that you don’t normally use.

- When you’re signing in to your account on an internet connection you don’t normally use.

What if I find 2-factor authentication really annoying?

- 2-factor authentication is optional for *some* websites.
- For many websites (such as email), it’s required.

Making 2-factor Authentication More Manageable

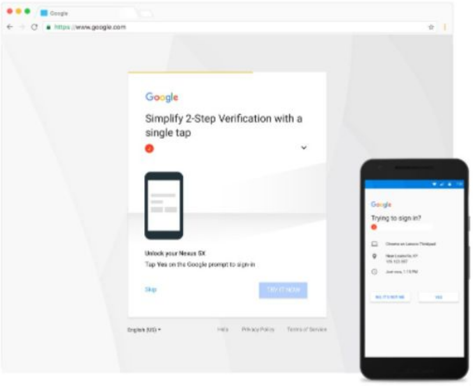
Strategy 1
Level: Elementary
Make sure that you have your phone with you.

- You don't have to have a smartphone! A flip phone that can receive text messages will also work.
- If you don't have a smartphone or a flip phone, sometimes you can use a landline.
    - You would need to have the service call you with the code, since it won't be able to receive text messages. Also, this option isn't portable, of course.

Strategy 1
Level: Basic
Understand the different methods of 2-factor authentication

- Push notifications
- Text messages
- Phone call

Push Notifications



Google

Simplify 2-Step Verification with a single tap

Unlock your Nexus 5X

Tap Yes on the Google prompt to sign-in

Google

Trying to sign in?

Chrome on Lenovo Thinkpad

Strategy 2
Level: Intermediate
Print out backup codes (only for Gmail and ProtonMail)

- Print out a group of one-time use codes that you can enter instead of a code sent to your device. Just be sure to keep it in a safe location!
  - Sign in with backup codes - Computer - Google Account Help
  - Two-factor authentication (2FA) - ProtonMail Support
- This is an excellent and important step to take because if anything ever happens to your phone, you can use these codes.

Strategy 3
Level: Advanced
Use an email service provider that doesn't require 2-factor authentication

- ProtonMail
  - Bonus! ProtonMail is an excellent option for people who want to create email addresses but don't have cell phones or otherwise don't want to provide a phone number.