# Online Privacy: Passwords and Two-Factor Authentication (2FA)

THE KANSAS CITY PUBLIC LIBRARY TECHACCESS

| Term | Definition |
|---|---|
| **Password** | A secret combination of letters, numbers, and symbols that only you know, which allows you to access an account, change settings, and update details on an account |
| **Two-factor authentication (2FA)** | A way to access an account that requires two separate forms of identification. The first is a password. The other can be a code sent to your smartphone or a security question that you set up |
| **Username** | A combination of letters, numbers, and symbols that uniquely identifies you on an account; if this is an account online, others will be able to see the username |

## Online Privacy: Passwords




When you create an account, you must create both a **username** and **password** so that you can set up the account to your specifications. It also means your settings will be the same, whether you access your account from your smartphone, a personal device like a computer or tablet, or a public device, like a library computer.

Because every account you create needs a username and password, you might feel it will make it easiest for you to make your password the same for all your online accounts.

**But this can be very dangerous and make it easy for someone to hack into your account.** If you use the same username and password combination for numerous accounts, you are compromising your online safety. If someone were to figure out your password, they can try to hack into other accounts using the same username and password combination.

**Online Privacy: Passwords and Two-Factor Authentication (2FA)**

THE KANSAS CITY PUBLIC LIBRARY TECHACCESS

## What makes a strong password?

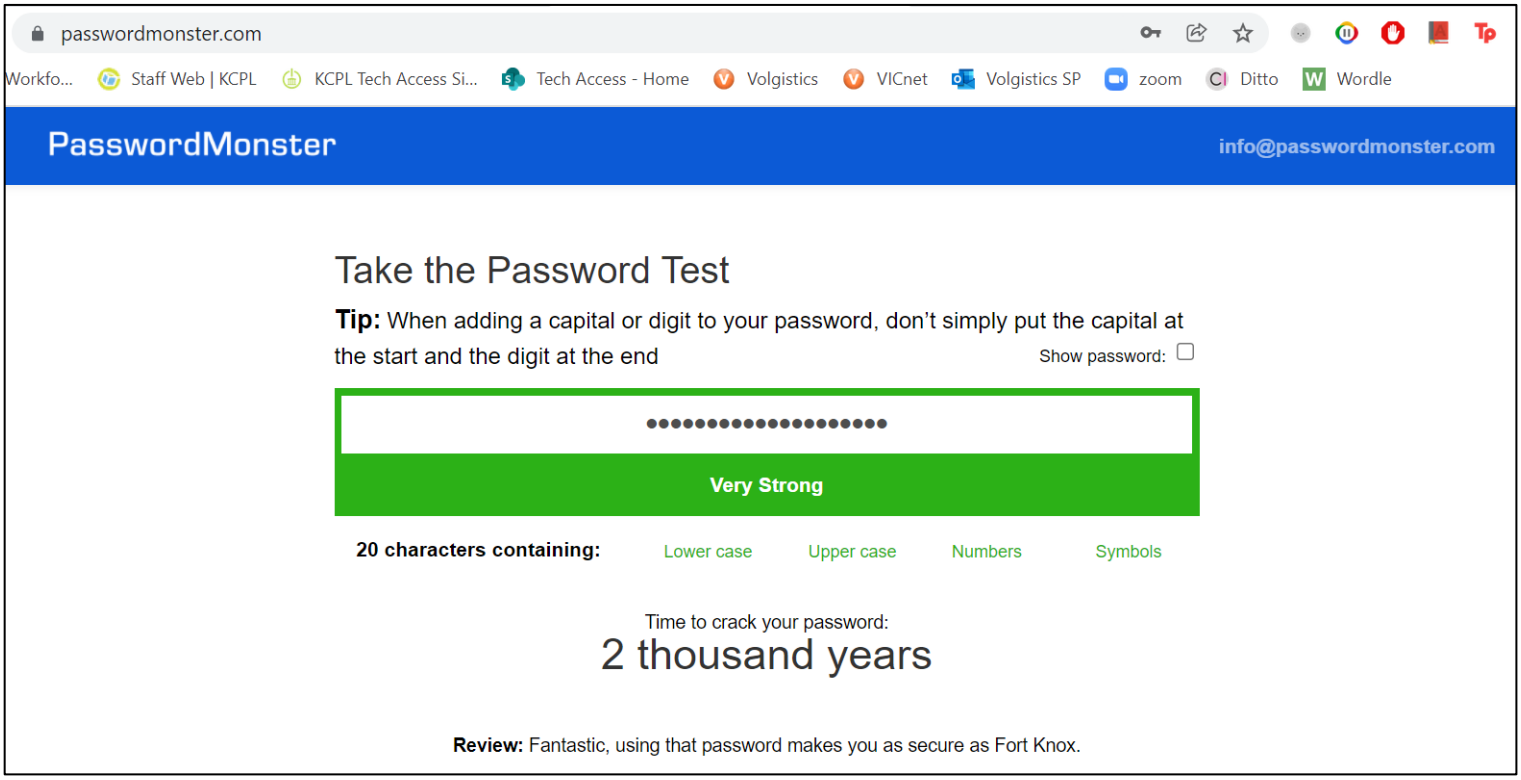
Using the list below from **Privacy Rights Clearinghouse**, consider how you can use these characteristics to create your own strong passwords to protect your online privacy.

- Avoid using dictionary words.
  - **Example:** phoenix, orlando
  - **Why:** Easy for hackers to figure out using an electronic dictionary, which can substitute numbers and symbols for similar letters.
- Don't use personal information.
  - **Example:** w3st4thblvd, anniemay89
  - **Why:** Personal information can be easily found, including any part of your name, birthday, Social Security number, or address.
- Avoid common sequences of numbers or letters.
  - **Example:** qwerty, 123456, abc987789cba
  - **Why:** Sequential combinations are very easy to guess.
- Use symbols when possible.
  - **Example:** t#ym31of0urF@ve$pice$
  - **Why:** Creates more permutations of possible words, making it harder to guess.
- Make it longer.
  - **Example:** S1ngusa$ongy0uret3ep1anomaN
  - **Why:** Passwords become harder to crack the longer they are.
- Consider using the first letter from each word in a sentence, a phrase, a poem, or a song title as a password.
  - **Example:** 0u@mdw1pw&w
  - **Why:** This creates a password that looks random but has an actual meaning you can remember.
- Create different passwords for different accounts and applications.
  - **Why:** If one password is breached, your other accounts won't be put at risk too.
- Write down your passwords and keep them in a securely locked place.
  - **Why:** If you create numerous accounts and will not remember all your usernames and passwords, it's important to have it somewhere only you can find.
- Consider using a secure password manager.
  - **Why:** An online password manager can store and create strong passwords for you.
- If you have already established a password that is not strong, change it!
  - **Why:** To protect your account now that you have more tips on creating strong passwords. Look for a link on the site's homepage that directs you to password and account management.

# Online Privacy: Passwords and Two-Factor Authentication (2FA)

THE KANSAS CITY PUBLIC LIBRARY TECH ACCESS

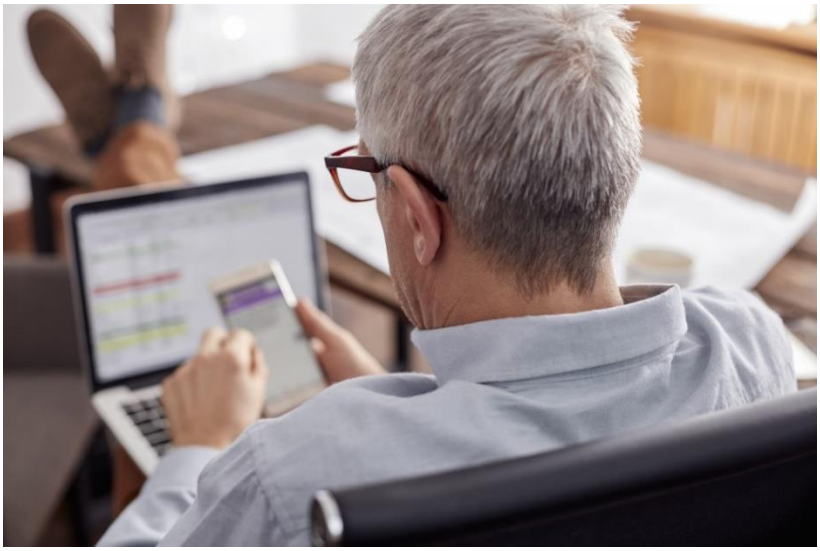
When in doubt, use a website like https://www.passwordmonster.com/ to determine the strength of your passwords and make sure you're including all the characters that make up a strong password.



**Online Privacy: Passwords and Two-Factor Authentication (2FA)**

THE KANSAS CITY PUBLIC LIBRARY TECHACCESS

## Online Privacy: Two-factor Authentication



When we think about online safety and security, strong passwords are the first thing that come to mind. But in the last decade or so, another method has become popular to protect your information online: **two-factor authentication** (**2FA**). 2FA is about confirming you are who you say you are when you log into an account. Most sites require 2FA as the minimum standard for security.

A **factor of authentication** is a piece of evidence that a user must present to prove they are who they claim to be.

There are three types of factors:

- The *knowledge factor* is something you know – a password.
  - These are the easiest to hack, because there are only so many possible combinations of numbers, letters, and symbols in a password.
- The *possession factor* is something you have – like a cellphone.
  - While it may be easy to crack someone's password, it's much harder to hack into the account if you also have a code sent to your phone to confirm that it's really you trying to get into your account.
- The *inherence factor* is something that represents who you are – like a fingerprint.
  - Unless you are the owner of the account, it's almost impossible to fake those, making this the strongest security option of the three.

By combining at least two of these factors, you are setting up two protective layers between yourself and anyone who would try to hack into your account for malicious reasons. A very common combination is using a password then getting a notification on your phone which you confirm – telling your account that it is you trying to access it.

Though it may seem intimidating to set up two-factor authentication, you are creating a stronger security system for yourself and protecting your information when you do. With an application like *Authy* or *Google Authenticator*, you can easily set up 2FA and ensure you are protecting your information and accounts to the best of your ability.

References:
Creating strong passwords: https://edu.gcfglobal.org/en/internetsafety/creating-strong-passwords/1/
Password strength test: https://www.passwordmonster.com/
10 Rules for Creating a Hacker-Resistant Password: https://privacyrights.org/resources/10-rules-creating-hacker-resistant-password
How to Set Up 2 Factor Authentication: https://seniorplanet.org/how-to-set-up-2-factor-authentication/
Multi-factor Authentication for Seniors: https://www.gwadvisors.net/multi-factor-authentication/