Staying Safe Online

JEFFERSON COUNTY
LIBRARY
DISTRICT

Topics

- Passwords
- Password managers
- Multi-factor authentication
- Phishing
- Updating

Course Schedule

Dates and Titles

April 26 - Settings

Times

Fridays,
2:00 – 3:30 pm

Intro to Excel

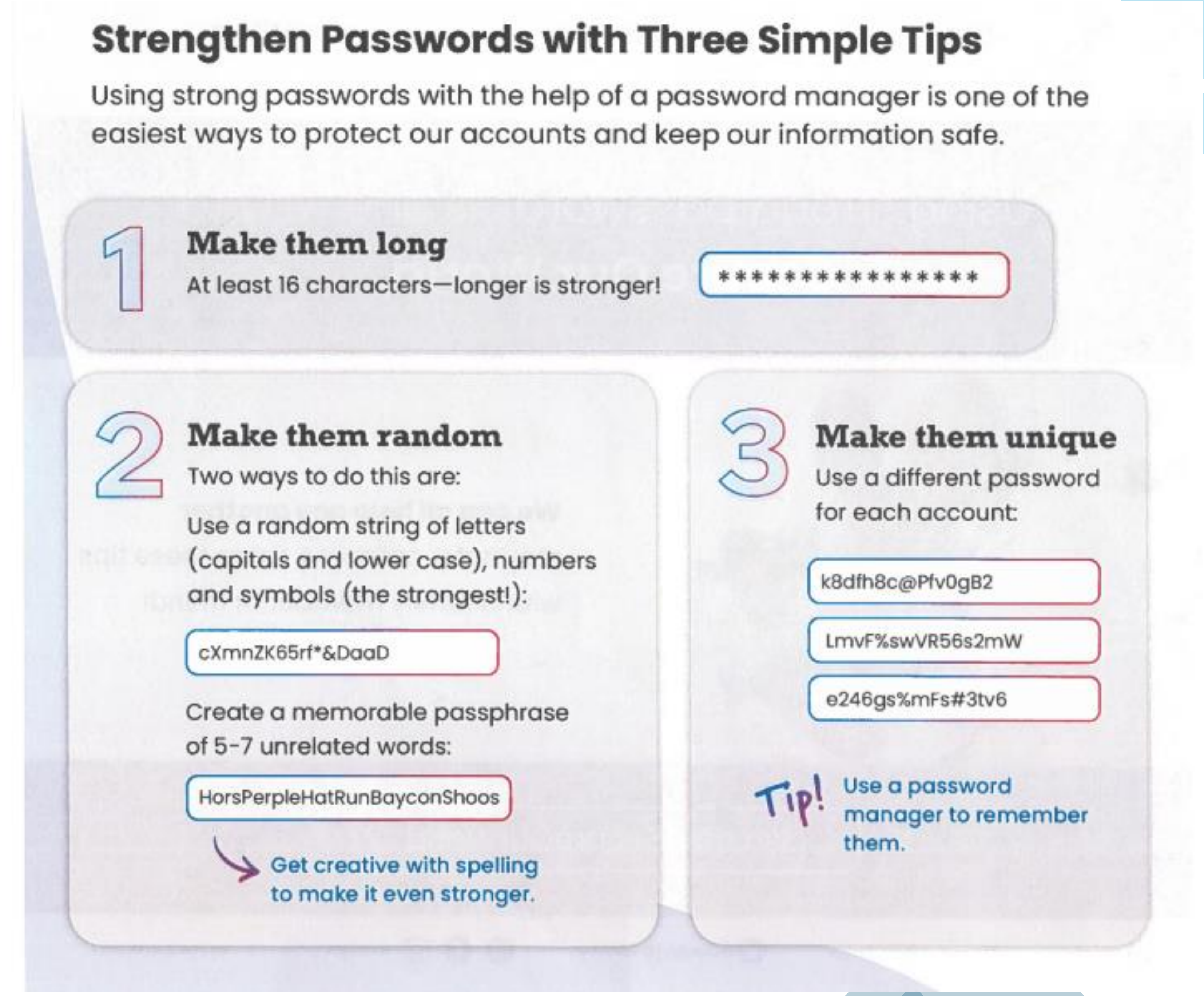
- **Date:** April 25
- **Location:** Port Townsend Public Library
- **Time:** 4:00 – 5:30 pm
- **Description:** Learn how to create a basic budget spreadsheet in this introduction to Microsoft Excel class. Laptops available.

Tech Tuesdays

- **Title:** How to Use MyChart, presented by Jefferson Healthcare
- **Date:** May 7
- **Time:** 3:00 – 4:30 pm
- **Description:** Learn how to use MyChart to access your medical information online.

Tech Tuesdays

- **Title:** eBooks, eAudiobooks, and eMagazines from Your Library
- **Date:** May 14
- **Time:** 3:00 – 4:30 pm
- **Description:** Access thousands of eBooks, eAudiobooks, and eMagazines free with your library card.



Strengthen Passwords with Three Simple Tips

Using strong passwords with the help of a password manager is one of the easiest ways to protect our accounts and keep our information safe.

1 Make them long

At least 16 characters—longer is stronger!

****

2 Make them random

Two ways to do this are:

Use a random string of letters (capitals and lower case), numbers and symbols (the strongest!):

cXmnZK65rf*&DaaD

Create a memorable passphrase of 5-7 unrelated words:

HorsPerpleHatRunBayconShoos

Get creative with spelling to make it even stronger.

3 Make them unique

Use a different password for each account:

k8dfh8c@Pfv0gB2

LmvF%swVR56s2mW

e246gs%mFs#3tv6

Tip! Use a password manager to remember them.

Passwords

- Use unique passwords for each account.
- Use long passwords – 16 characters or more.
- Use passphrases – a series of random words.
- Use a password manager.

Tips for making strong passwords

JEFFERSON COUNTY LIBRARY DISTRICT

Don’t create passwords using public information such as:

- Pet’s or people’s names
- Addresses or postal codes
- Key dates like a birthday or an anniversary

Don’t Reuse Passwords

- Longer Passwords are Stronger
- The absolute minimum length is eight characters, but 16 or 20 characters are even more secure!
- One of the main ways cybercriminals access your accounts is by trying passwords you have used elsewhere.

Keep It Unique

- Use numbers and special characters to alter regular dictionary words, and don’t use simple patterns like “password1, password2, password3” for different sites.

Use a Passphrase

- Passphrases are a sentence-like string of words that are easy to remember but difficult to crack. For example, “jellyfish-apple-1600-pirate” or a few nonsense words like “Betty was eating tires and playing tuna fish.”

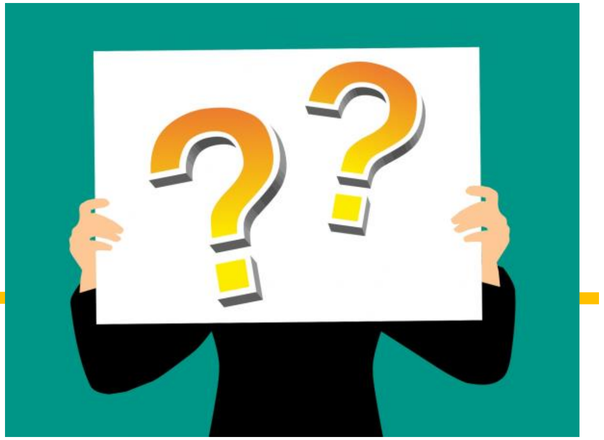
Review

Which of the following tips help to create strong passwords?

1. Don’t create passwords using public information.
2. Don’t reuse passwords.
3. Keep passwords unique.
4. Use a passphrase.
5. All of the above.

JEFFERSON COUNTY LIBRARY DISTRICT

Review



Which of these is the strongest password?

1. jclibrary
2. PortHadlock98339
3. password1234
4. Matador3Gr0omTackling!

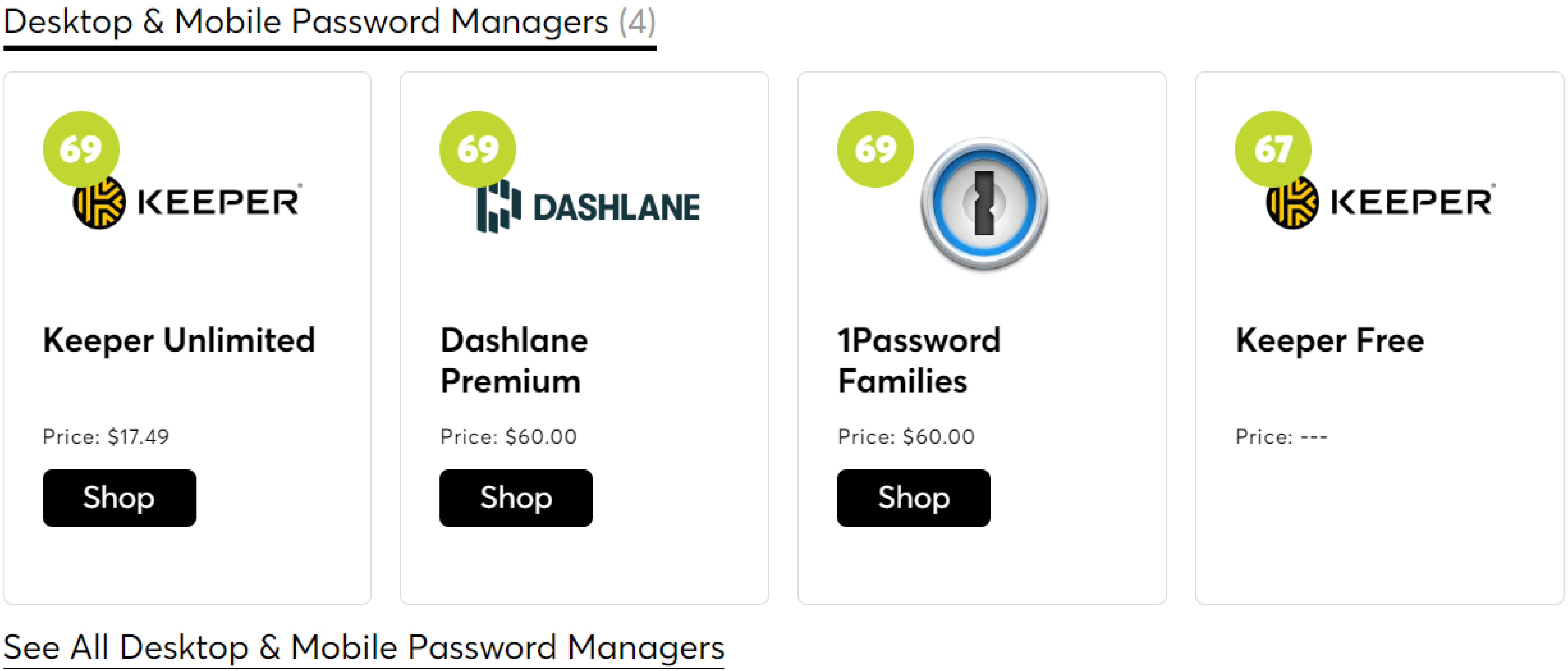
Why?

JEFFERSON COUNTY LIBRARY DISTRICT

Password Managers

- Requires users to remember only one master password.
- Credentials are stored in an encrypted vault.
- Password generator tools for creating strong passwords.

Consumer Reports - Recommended



Desktop & Mobile Password Managers (4)

69

Keeper Unlimited

Price: $17.49

69

Dashlane Premium

Price: $60.00

69

1Password Families

Price: $60.00

67

Keeper Free

Price: ---

See All Desktop & Mobile Password Managers

Quiz

What are some of the features of a password manager?

A. It stores and generates strong, unique passwords.
B. Information in kept in an encrypted vault that only you can access.
C. It requires you to remember only a single master password.
D. All of the above.

Password Managers

For additional information about password managers, please schedule a One-on-One Tech Help meeting.

Multifactor Authentication

Multi-factor authentication is also known as two-factor authentication or two-step verification, and often is abbreviated as MFA or 2FA.

Generally, you will enter your username and password.

You will then prove your identity with an additional factor such as a fingerprint, face identification, or one-time code.

Multifactor Authentication

Multifactor authentication increases your cybersecurity by requiring a second form of authentication.

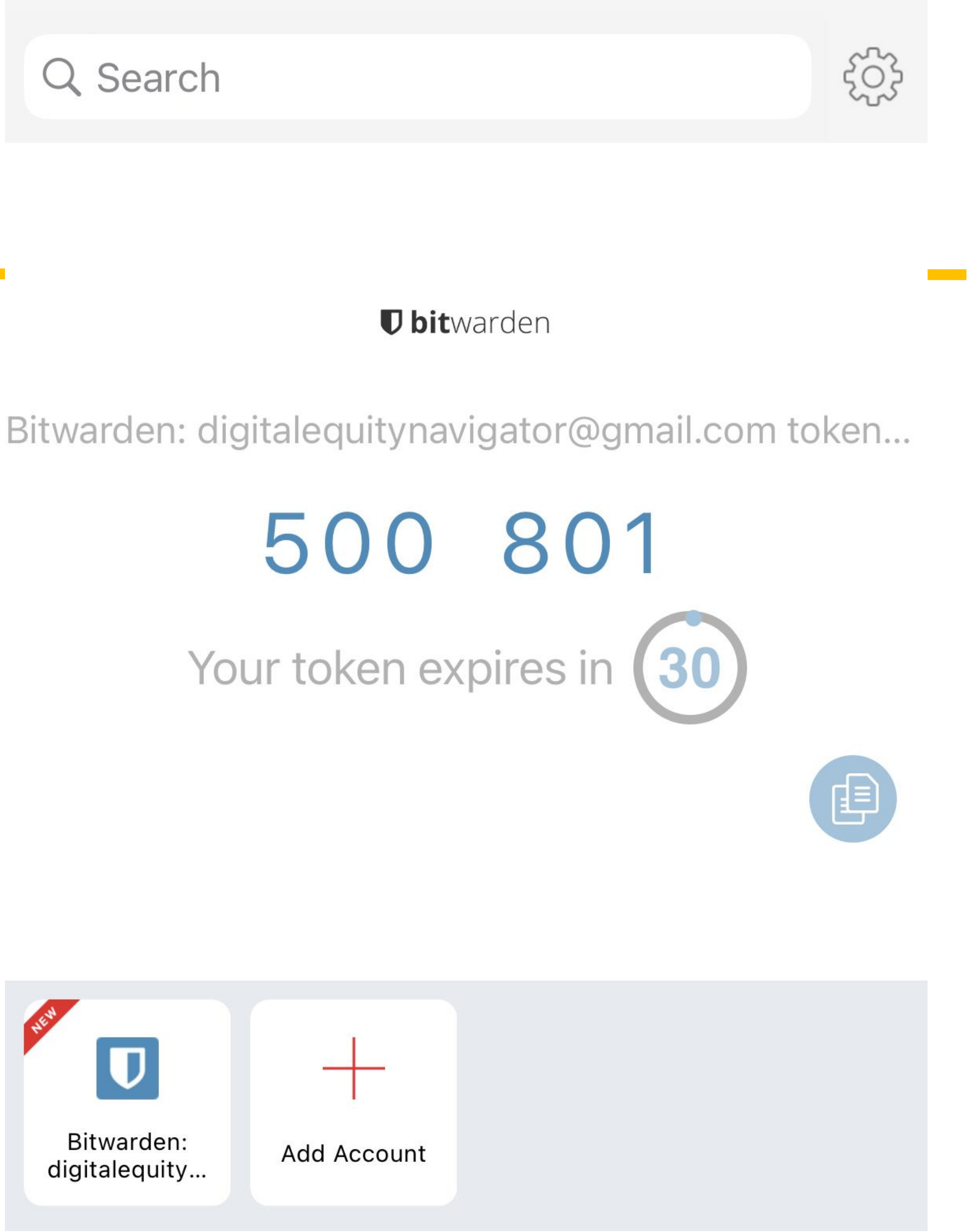
If a user’s credentials were to be involved in a data breach, the second factor would still be needed to gain access to an account.

One-time codes

One-time codes can be received the following ways:

- **Email**
- **Text message (SMS)**
- **Authenticator apps**

Which method do you think is the least secure?



Bitwarden: digitalequitynavigator@gmail.com token...

500 801

Your token expires in 30

Authentication apps

A mobile app that generates a one-time code linked to specific online accounts. Below are a few, free authentication apps, though there are many to choose from.

- Authy
- 2FA
- Duo Mobile
- Google Authenticator

Recommendation

It is recommended that you implement multi-factor authentication for any account that permits it, especially any account associated with work, school, email, banking, and social media.

Review

When should you enable multi-factor authentication?

1. Whenever you feel like it.
2. Only during full moons and solar eclipses.
3. Wherever offered, especially for accounts related to email, social media, finances, medical, work, or school.

JEFFERSON COUNTY LIBRARY DISTRICT

Review

How does multi-factor authentication increase security?

1. It requires a one-time code, fingerprint, or face identification in addition to a username and password.
2. It changes my password for me.
3. It saves my username and password.

JEFFERSON COUNTY LIBRARY DISTRICT

Review

Why does enabling multifactor authentication increase your cybersecurity?

Think Before you Click!

What is a phishing scam?

When a cybercriminal sends you a fake email, direct message, text, or a pop-up ad to trick you into taking an action such as clicking a link, providing personal information, or making a payment.

A phishing message may be cleverly disguised to look like a real message from a familiar company such as your bank.

EASY TIPS TO AVOID

PHISHING SCAMS

Indicators of a malicious email

Email addresses and websites do not look genuine.

There is a suspicious attachment.

There is a call to action button (possibly a panic button)

The email is poorly written.

The email asks you to confirm personal information.

Are you expecting the email

3 Parts of a valid email address

dheaton@jclibrary.info

Username

@

Domain Name

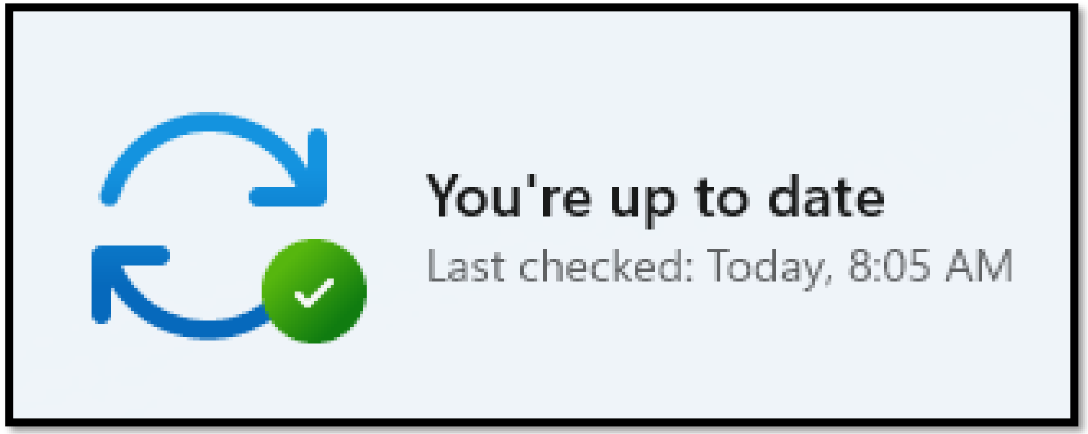
Phishing Quiz

https://phishingquiz.withgoogle.com/

Software Updates

It is also recommended that you update your software to protect against phishing and other types of malware.

Keeping software up-to-date improves your cybersecurity by ‘patching’ known vulnerabilities in software.

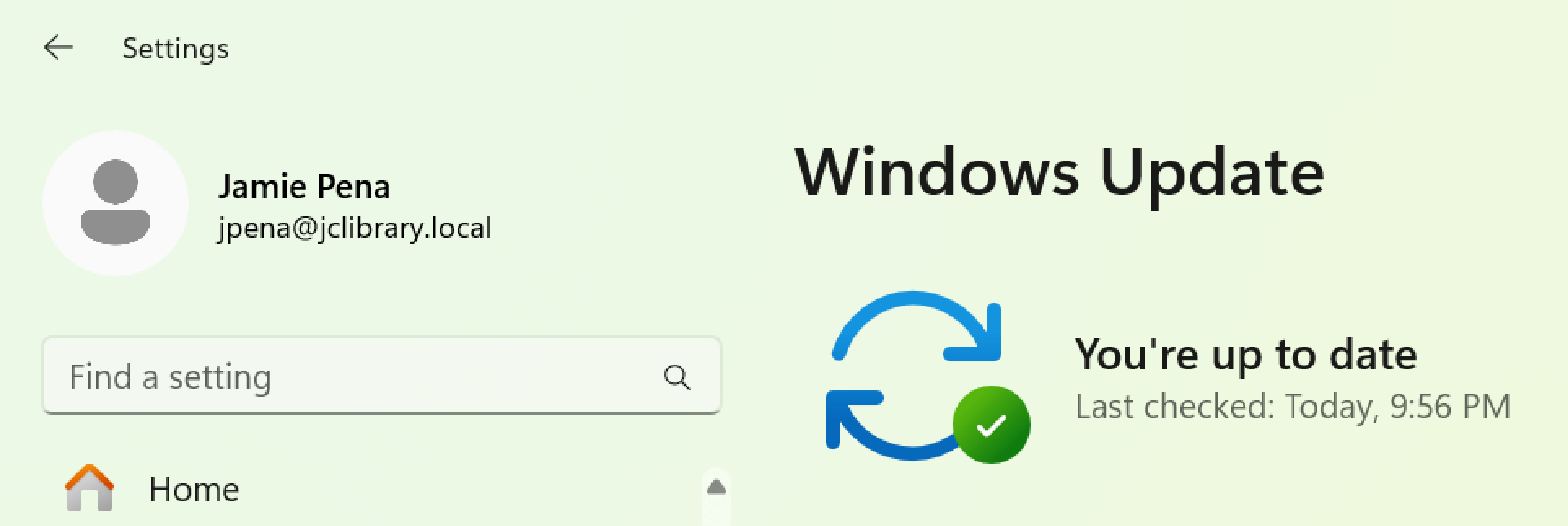


You're up to date

Last checked: Today, 8:05 AM

Software Updates

Updates can generally be found under **Settings**.



Windows Update

You're up to date

Last checked: Today, 9:56 PM

Updating Recommendations

- Enable automatic updates whenever offered.
- Only download software from verified sources or your system’s official app store.
- Don’t fall for phishing update pop-up windows.
- If automatic updates aren’t an option, update when prompted, and check regularly.

Resources

Passwords - https://staysafeonline.org/online-safety-privacy-basics/passwords-securing-accounts/

Password Managers - https://staysafeonline.org/online-safety-privacy-basics/password-managers/

Resources

Phishing - https://www.cisa.gov/secure-our-world/recognize-and-report-phishing

Updates - https://staysafeonline.org/resources/software-updates/

Last Class

Basic Computer Skills: Settings
Date: Friday, April, 26
Time: 2:00 – 3:00 pm

- Changing backgrounds
- Managing notifications
- Uninstalling apps
- Accessibility features

JEFFERSON COUNTY
LIBRARY
DISTRICT

Questions?

If you have questions about the topics covered in this presentation, contact the Jefferson County Library District to schedule a One-on-One tech help appointment.

360-385-6544

information@jclibrary.info

JEFFERSON COUNTY
LIBRARY
DISTRICT