TVCC Cybersecurity Training

Interesting Facts

- Cybercrime is up 600% due to the pandemic
- 98% of cyber-attacks rely on social engineering
- 81% of organizations were affected by cybercrime last year
- Third-party app stores hosts 99% of discoverable mobile malware
- A malicious hacking occurs every 39 seconds
- 80% of all targeted attacks started with phishing scams
- Higher education particularly vulnerable (transparency, legacy systems)
- 30% education industry users fell for phishing scams
- 94% of malware is delivered via email
- $17,700 is lost every minute due to phishing attacks
- 60% of breaches involved vulnerabilities for which a patch was available but not applied

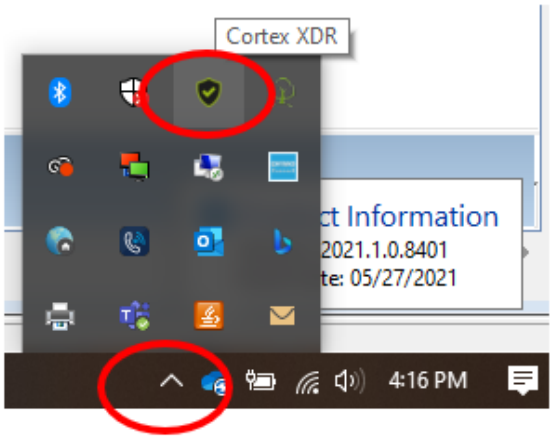
TVCC Best Practices Reminders

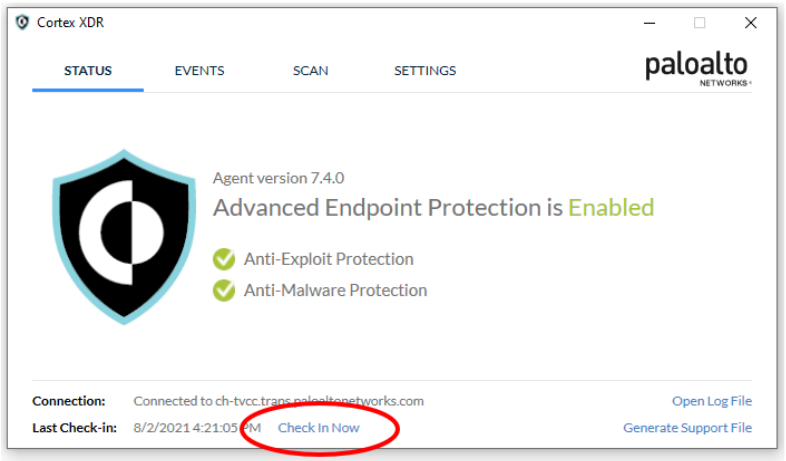
- DO NOT share your username & passwords with anyone
- Lock your computer when you step away from it ( + L), virtually and physically
- Do not save your passwords in the browser (use a password vault with a completely different password than anything else)
- Keep your system up to date
- Make backups
- Use multi-factor authentication (MFA)
- Encrypt your data and protect personal information
- Use Virtual Private Network (VPN) or View for remote access
- Limit activities on public WiFi
- Slow down and evaluation emails carefully

Cortex / Anti-Virus Software

“Check-in” with Cortex XDR

- Bottom right corner of your screen, click on the up arrow then on the Cortex shield
- Then click on the “Check In Now” words in the next window





Why “check-in”?

- Cortex Block something from running.
- Keep your computer secure
- Verify your computer is connected to the console

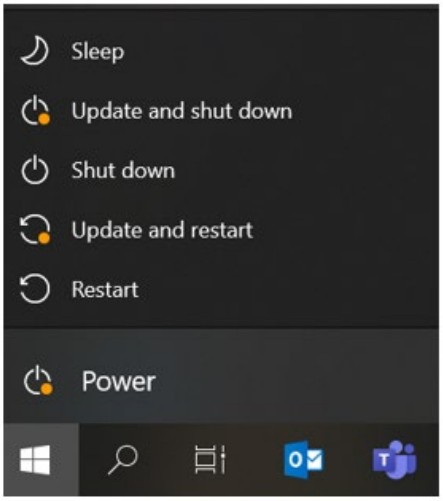
Keep your computer up to Date!

Updates help patch security flaws

Hackers love security flaws, also known as software vulnerabilities. A software vulnerability is a security hole or weakness found in a software program or operating system. Hackers can take advantage of the weakness by writing code to target the vulnerability.

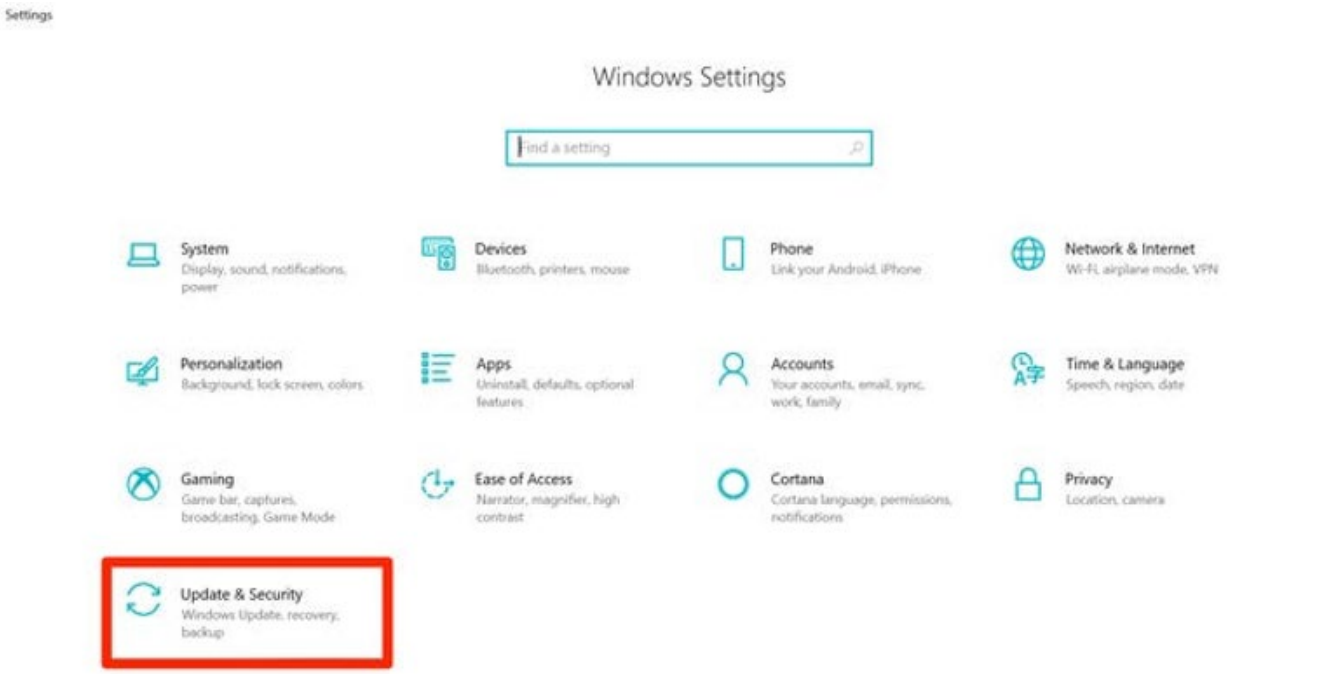
Software updates often include software patches. They cover the security holes to keep hackers out.

Look for updates when you shutdown or restart (orange dot)



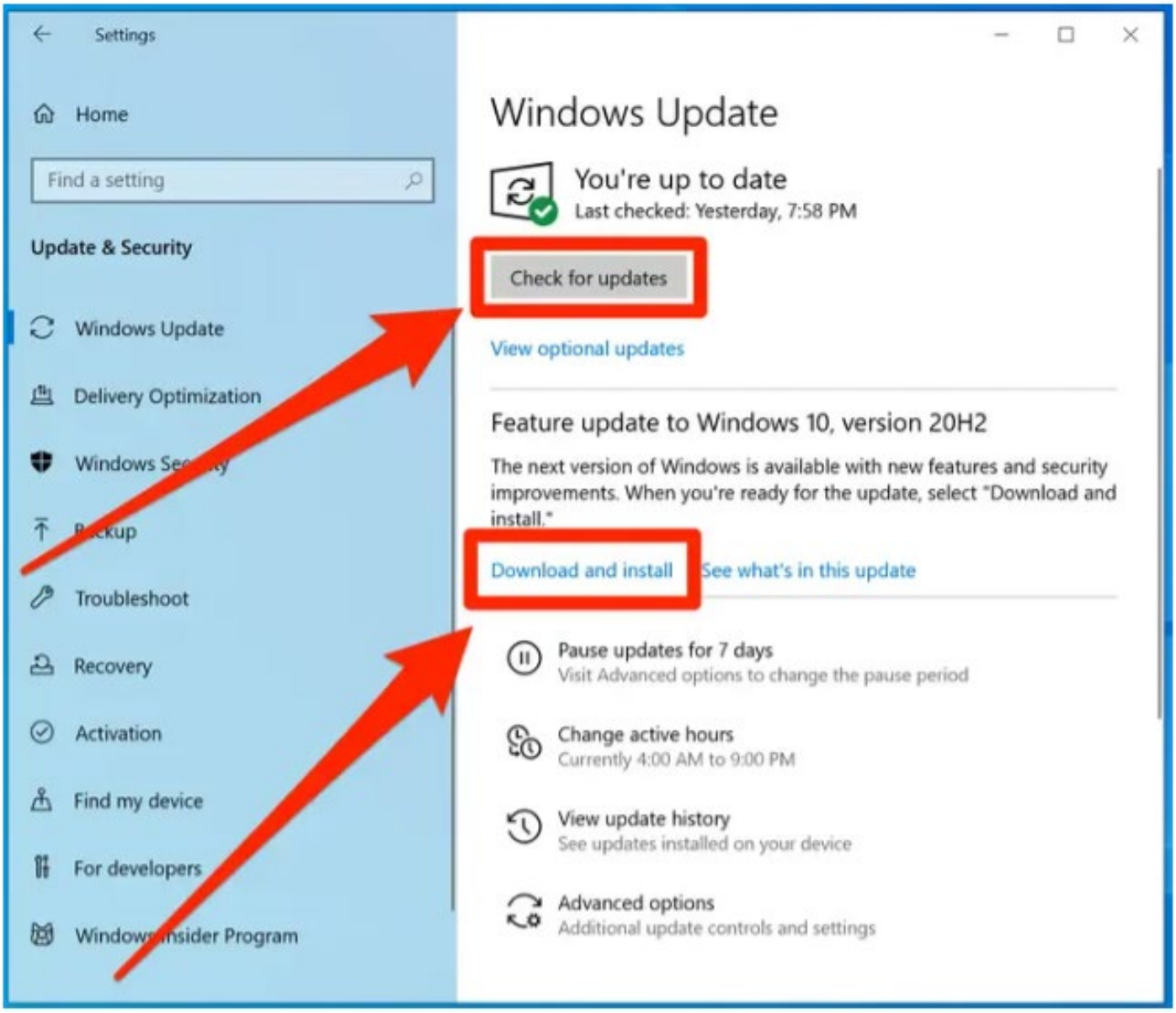
In Windows 10, you decide when and how to get the latest updates to keep your device running smoothly and securely. To manage your options and see available updates, select Check for Windows updates.

Or select the **Start** button, then go to **Settings** **> Update & Security** **> Windows Update**



To check for an update, click "Check for updates."

If there's an update ready to install, it should appear under the "Check for updates" button. Click "Download and install."



Password Managers

What's a password manager?
Password managers generate unique, complex passwords for every site, store them securely and enter them on different browsers and computing devices. You can use them as browser extensions or mobile apps that fill out login pages with your username and password for you.

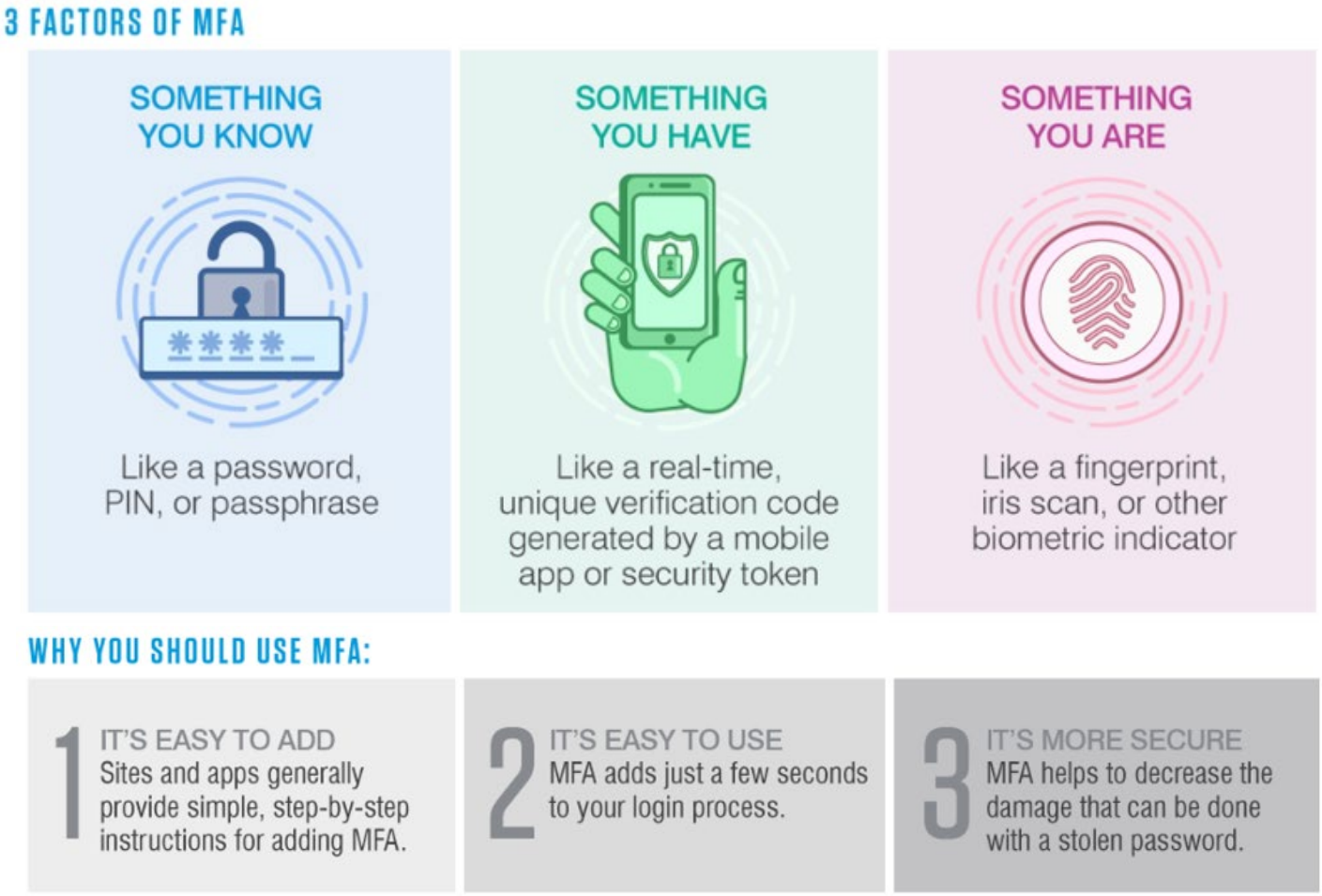
Don’t Reuse Passwords!
Password reuse is a serious problem because of the many password leaks that occur each year, even on large websites. When your password leaks, malicious individuals have an email address, username, and password combination they can try on other websites. If you use the same login information everywhere, a leak at one website could give people access to all your accounts. If someone gains access to your email account in this way, they could use password-reset links to access other websites, like your online banking or PayPal account.

Why Browser-Based Password Managers Aren’t Ideal
Web browsers — Chrome, Firefox, Internet Explorer, and others — all have integrated password managers. Each browser’s built-in password manager can’t compete with dedicated password managers. For one thing, Chrome and Internet Explorer store your passwords on your computer in an unencrypted form.

Some examples of password vaults:

What is multifactor authentication (MFA)?

Multifactor authentication (MFA) adds a layer of protection to the sign-in process. When accessing accounts or apps, users provide additional identity verification, such as scanning a fingerprint or entering a code received by phone.

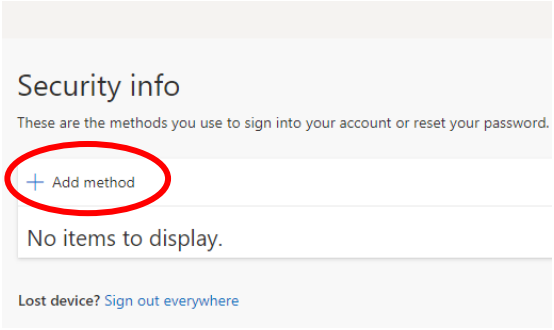


Turn Verification On and Off

1. Visit www.office.com

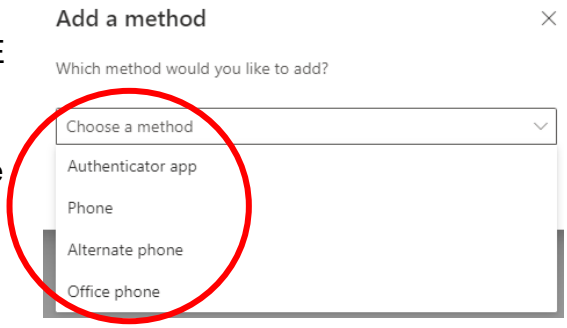
2. Click “Sign in” in the top right corner and sign into Microsoft with your TVCC email & password.

3. Once signed in, click your name in the top right corner and select “View account”

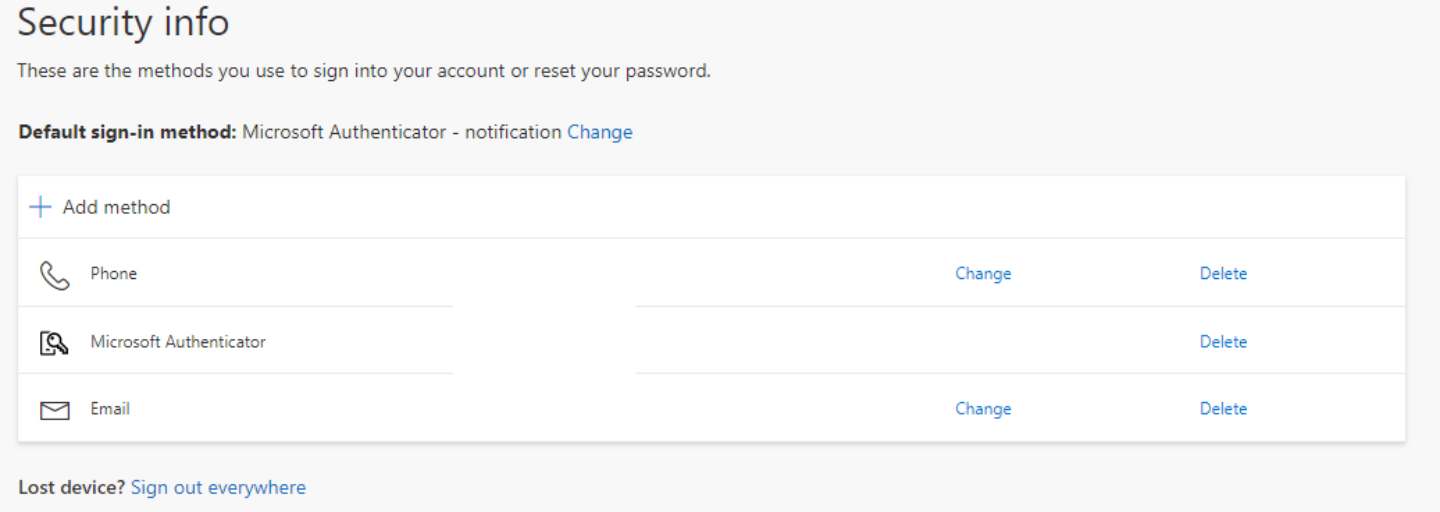


4. Click “Security info” on the next page and then “UPDATE INFO”.

5. You will need to choose a method of verification from the drop-down list.



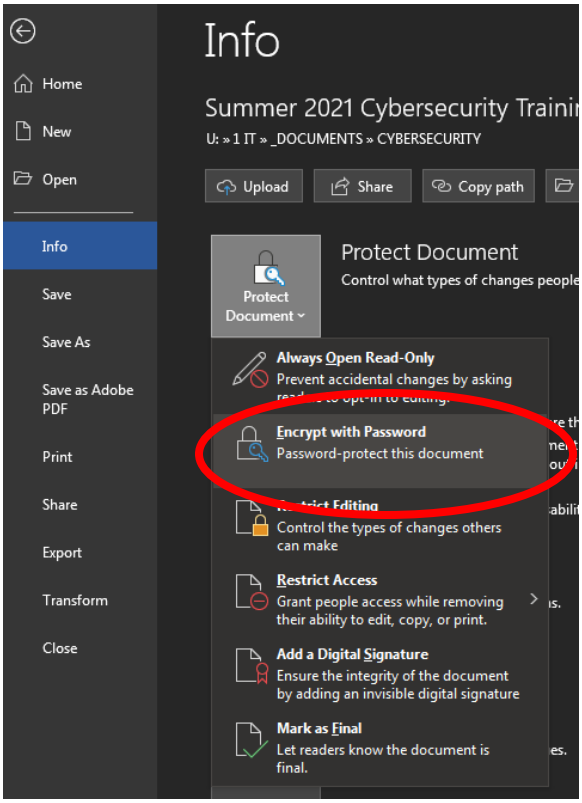
6. Whatever method you choose, you will be prompted via that method to verify you have access to that method. If you choose the “Authenticator app”, you will need to download the “Microsoft Authenticator” onto your smart phone.



Password Protect Documents

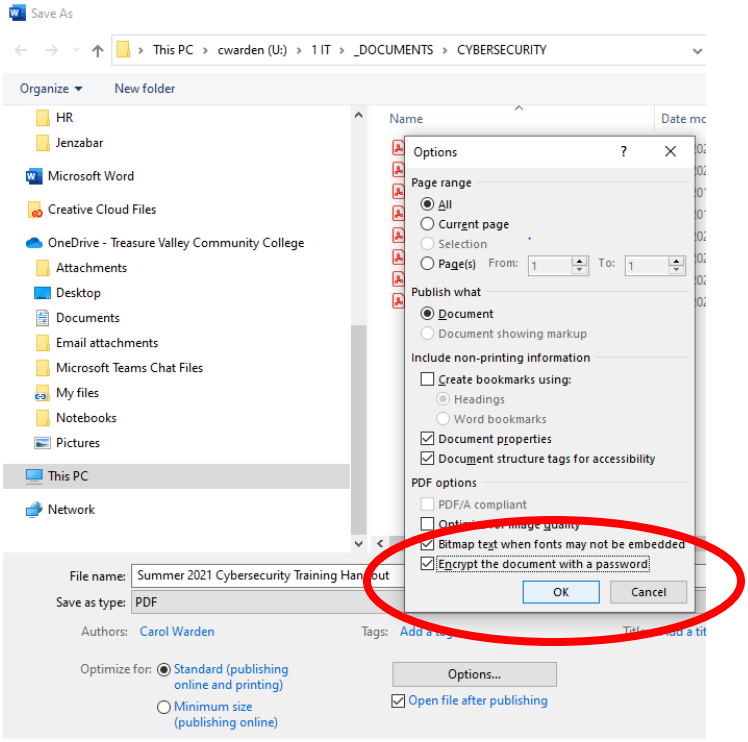
Word Documents

- Go to **File** > **Info** > **Protect Document** > **Encrypt with Password**
- Type a password, then type it again to confirm it
- Save the file to make sure the password takes effect



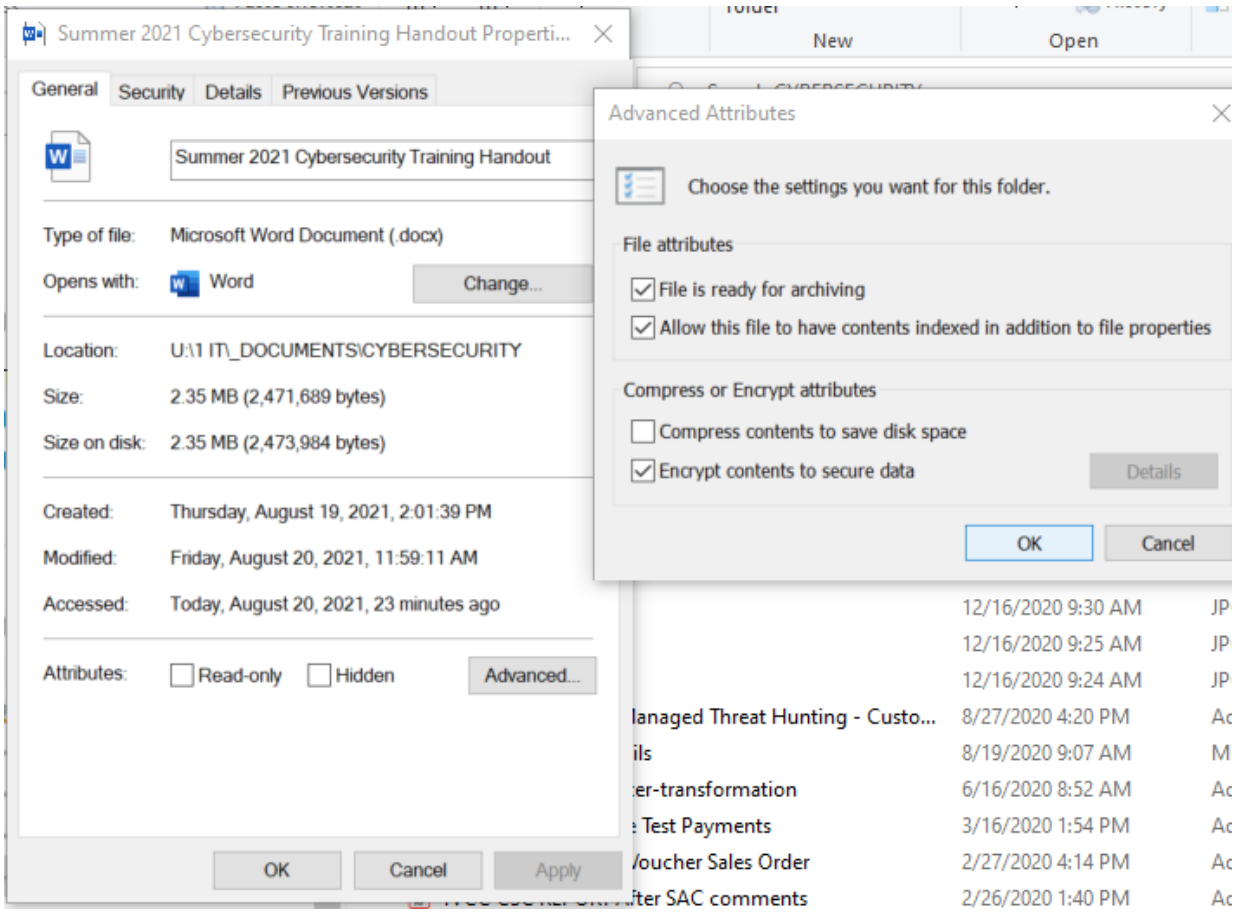
PDF Documents

- Open your Word document
- Click **File** > **Save As**
- In the "**Save As Type**" box select PDF
- Click the "**Options**" button & check the "**Encrypt the document with a password**" box
- Enter your password & confirm it by entering it again
- When you open the document, you will be prompted to enter a password



Encrypt a File or Folder

- Right-click a file or folder & select **“Properties”**
- Select the “**Advanced**” button
- Click the “Encrypt contents to secure data” box
- Click the “Options” button & check the “Encrypt the document with a password” box
- Enter your password & confirm it by entering it again
- When you open the document, you will be prompted to enter a password



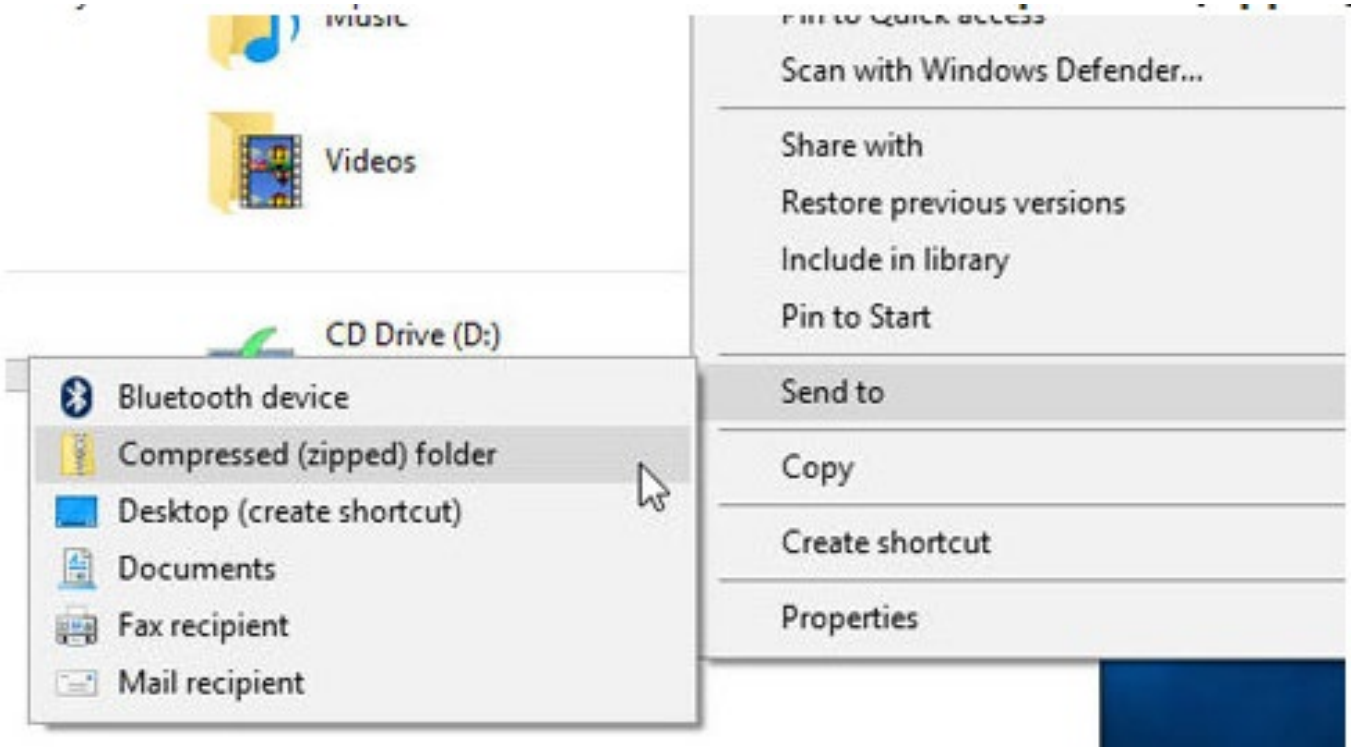
How to Zip a File or Folder

To Zip Files

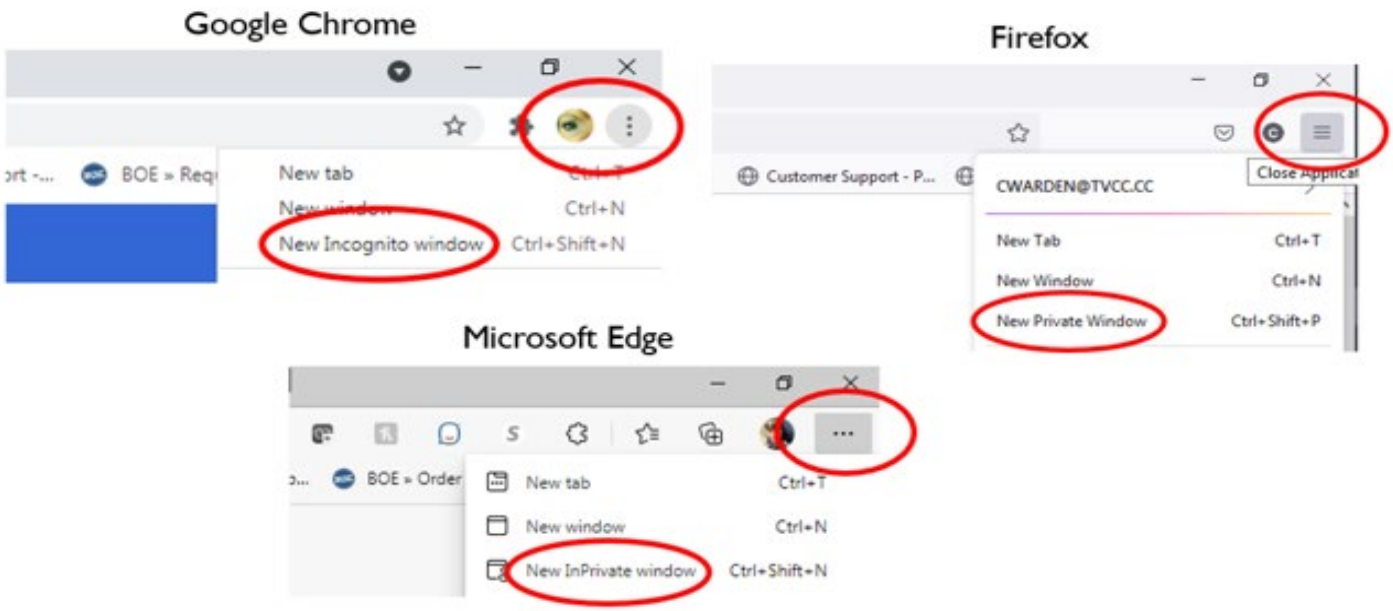
- Open File Explorer
- Select the file or folder & right-click on it
- Select “Send to > Compressed (zipped) folder”

Unzip Files

- Entire Folder - right-click & select “Extract All” & follow the instructions
- Single file or folder, double-click the zipped folder to open it, then drag or copy the item from the zipped folder to a new location



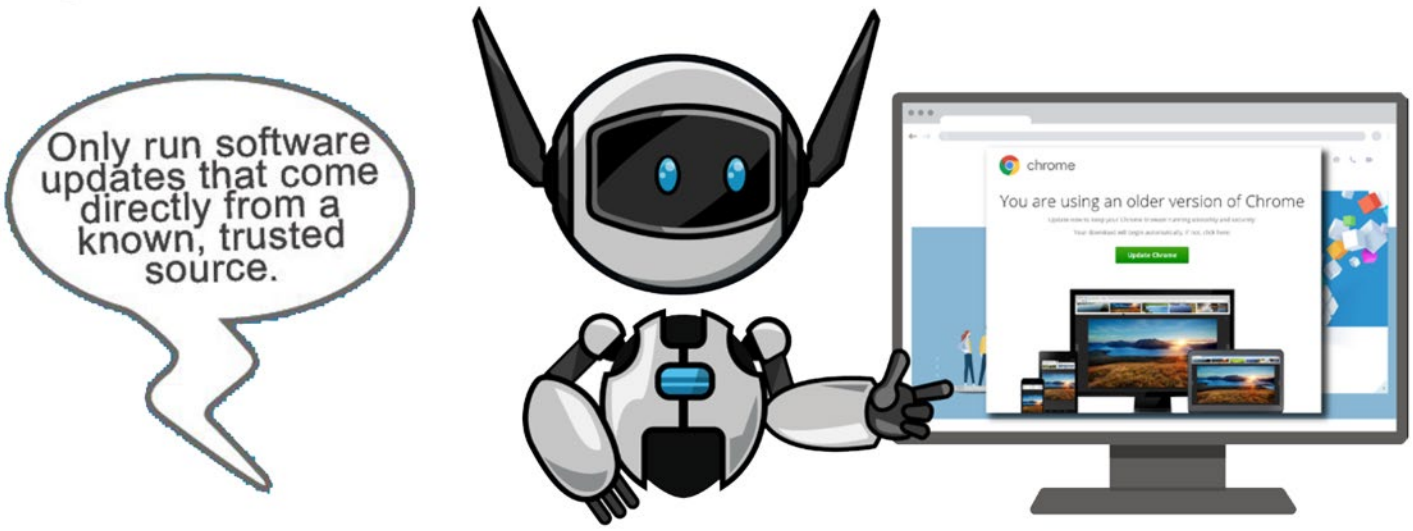
Use “Incognito” Browser Mode



What is incognito mode?

Incognito mode. Alternatively referred to as **private browsing, InPrivate Browsing**, or a **private window**, Incognito mode is an Internet browser setting that prevents browsing history from being stored. Normally, when you visit any web page, any text, pictures, and cookies required by the page are stored locally on your computer.

Fake Browser Updates



If you see an unexpected pop-up:

Do not download any files or run updates. When in doubt, refer to your organization's software update policy, or check with your IT security team.

Use your device's system tools to stop any process that may be running in the window.
On a PC, for example, go through the Task Manager.

Cybercriminals are injecting code into trusted websites to produce malicious pop-up windows. These urge people to update their web browsers but are designed to install malware.

Interacting with a malicious pop-up could give attackers access to your device – and your organization's systems.

If you think you've accidentally downloaded malware, immediately contact your IT security team.

AVOIDING DANGEROUS EMAIL LINKS

Get an email with a link?

FOLLOW THESE FIVE TIPS TO STAY SAFE:

EXPECTING IT?

Only click links if you're expecting them.

TRUST IT?

http://

If a link is unexpected, but you trust the source, type the URL you know into a browser or use a bookmark.

VERIFY IT.

Use a search engine to verify the site.

Search

HOVER OVER IT.

https://marigoldbank.account-login.us/

https://user.account-login.us/

Hover your cursor over a link to reveal its true destination.

CHECK THE DOMAIN.

Pay close attention to the link's actual domain. Watch for common tricks like using subdomains, hyphens, or shortened URLs.

Not sure about a link? Contact your IT Security Team.

Deleting Email from Outlook

1. Open the **Outlook** desktop application.

2. Select the message(s) in your Inbox to be deleted. (If you previously deleted the message, you can find it in the Deleted Items folder.)

3. Hold down the **Shift** key on your keyboard and click **Delete** in the top control bar.

4. In the confirmation window that appears, click **Yes**. This will move the message to the Recoverable Items folder.

5. Select the **Folder** tab in the top menu.

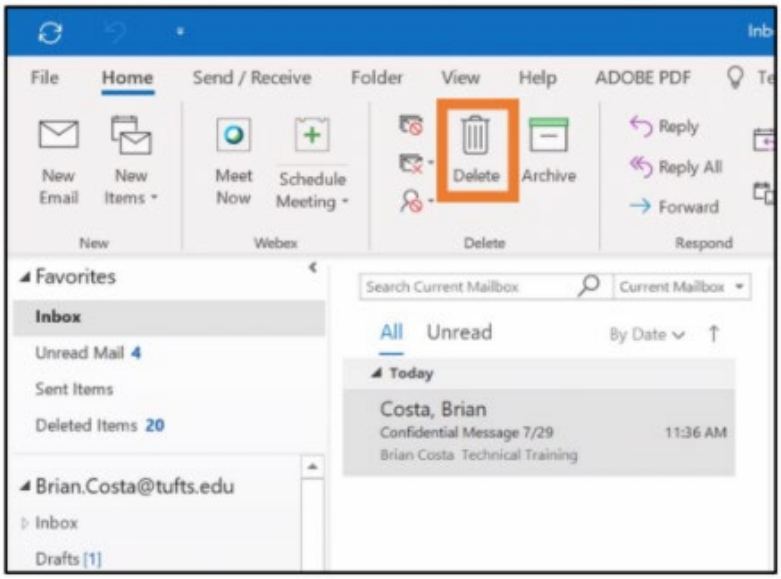
6. Click **Recover Deleted Items**.

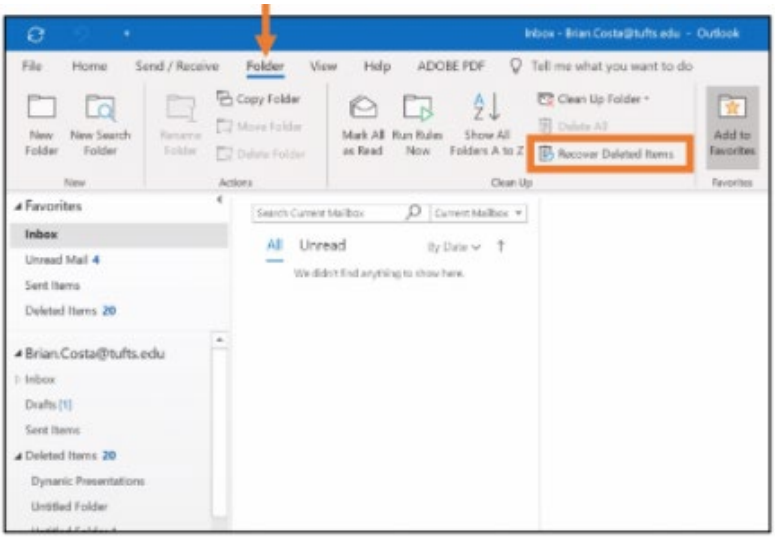
7. In the Recover Deleted Items window, select the message(s) you want to manage.

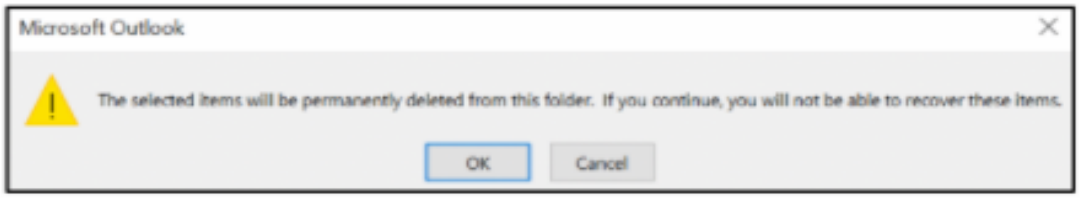
8. Select **Purge Selected Items** at the bottom of the window.

9. Click **Ok**

10. A warning will appear that you are about to permanently delete the selected messages and you will no longer be able to recover them. To proceed, click **OK**







Social Engineering Explained

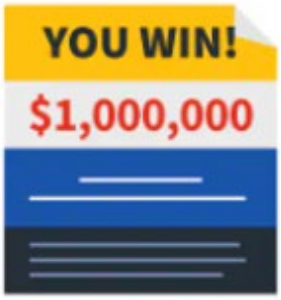
Also known as human hacking, social engineering is the manipulation of someone to divulge confidential information that can be used for fraudulent purposes.

Knowing the red flags can help you avoid becoming a victim:

Your 'friend' sends you a strange message.

Your emotions are heightened.

The request is urgent.



The offer feels too good to be true.

You're receiving help you didn't ask for.

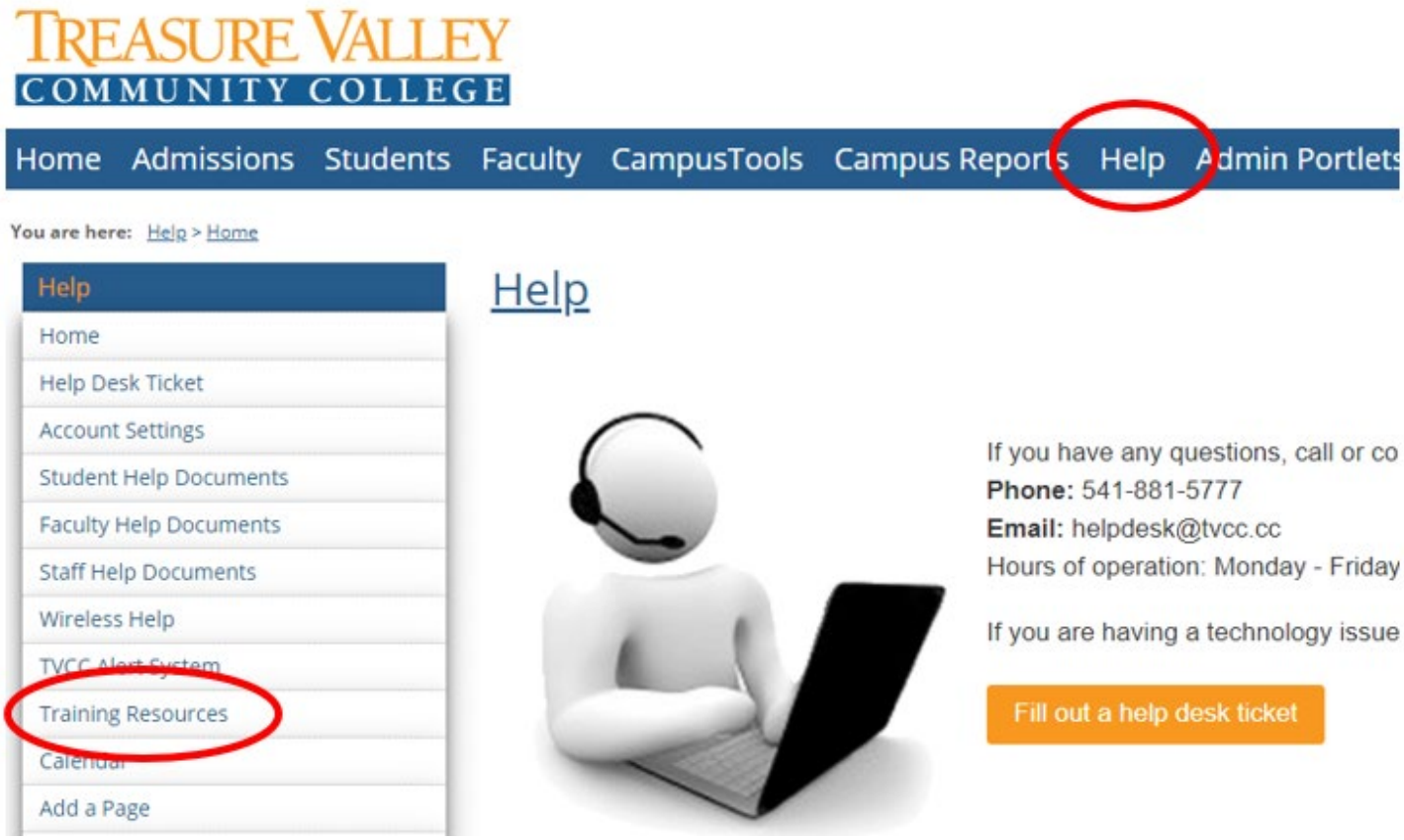
The sender can't prove their identity.

5 ways to outsmart a social engineer

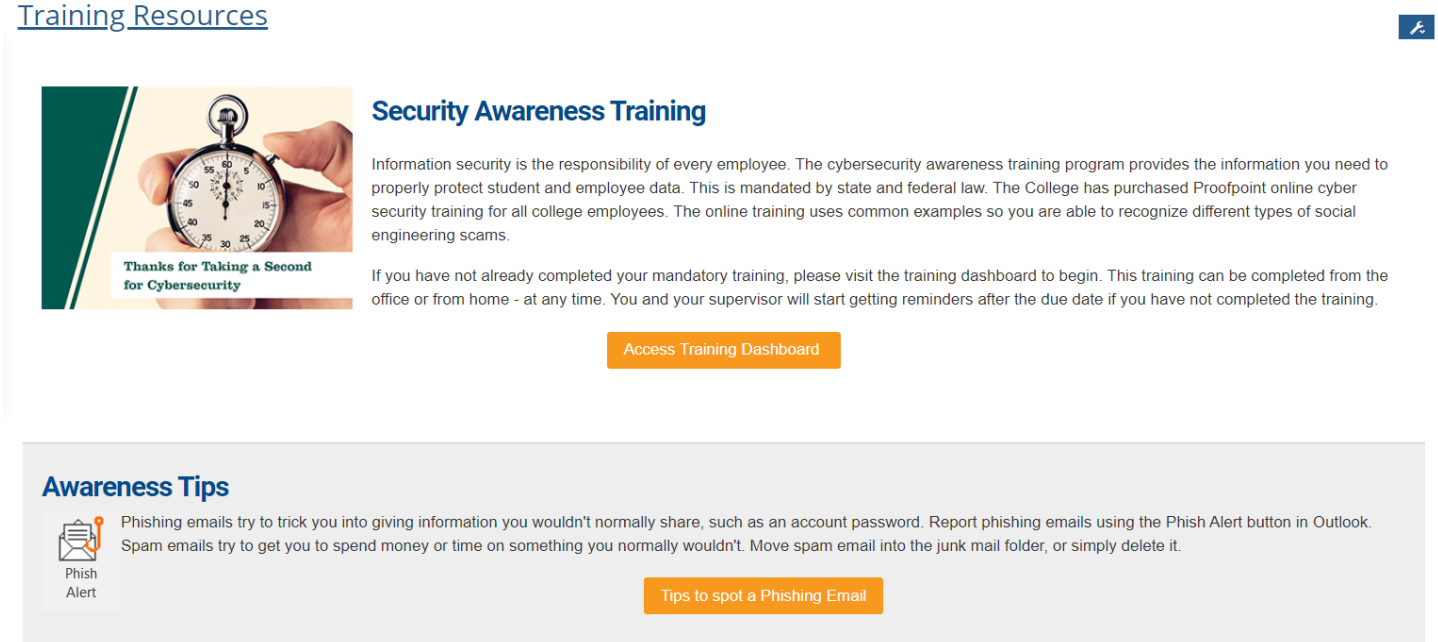
- Don't take things at Face Value
- Ask Questions
- Do your own Due Diligence
- Don't be afraid to say 'No'
- Allow yourself to be a little paranoid

How to Find Your Training?

- Log into MyTVCC
- Click “Help”
- Click “Training Resources”



Click on “Access Training Dashboard”



Two sections: “My Assignments” and “Additional Training”