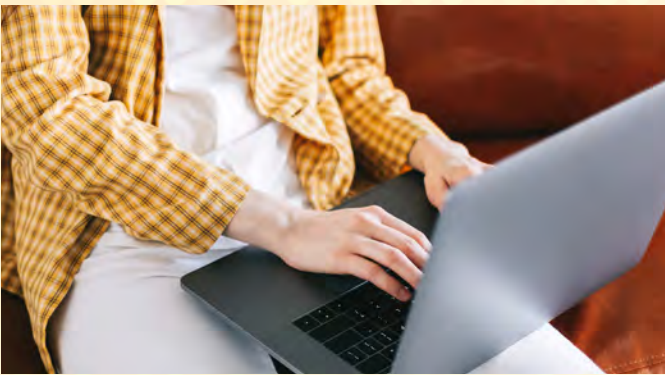




TECHNOLOGY TIPS

Brought to you by the Information Technology Department

Protect your computers and your data



When we think of cybersecurity, we tend to think of threats coming from the outside. We think of “hackers” trying to access our bank accounts and steal our identities, but we tend to forget about the physical security of our computers and our data. We can have all of the cybersecurity measures in place to prevent outside attacks, but we can’t forget about the attacks that happen because we forgot to lock our computer when we went to get a drink or lock our office when we left for the evening. All it takes is a few minutes and someone could sit down at your desk and copy down your passwords that you have saved on an unlocked computer or on a sticky note that you think is hidden.

In the next few months before the campus gets busy with welcoming all of our students back, let’s take the time to start building good physical security habits:

1 Always lock your computer when you stand up, even for just a second. On a PC this is as easy as pressing Win+L or Cmd+Ctl+Q on a Mac.

2 Always set a strong password for your machine. At Temple College, we require passwords to be at least 6 characters long and contain three of the following four categories: uppercase character, lowercase character, number or special character. Passwords must be changed every 200 days and the past four passwords cannot be reused.

3 Always use Multi-Factor Authentication if available. This adds an additional layer of security to your login. This could be a text message or phone call to your phone of choice, or an authenticator app that will generate a one-time code. This way, if your password is ever compromised, you still have an additional control to keep people out of your account.

4 Never reuse passwords! If the password you use on a game or shopping site is compromised, you don’t want the attacker to also have access to your work or personal accounts.

5 Never write down passwords! It is always best to memorize your passwords, but if you need some extra help you can use a free password manager such as LastPass or Dashlane. Make sure you use a secure password with Multi-Factor Authentication to access your password manager.

6 Never leave sensitive information on your desk! Any document that has Personally Identifiable Information (PII) of a student or staff member (including test scores) should be packed away when not in use. You never know who will be walking by your office and could see something on your desk that they shouldn’t see.

Having password problems? Need help logging in?

Stop by in person, email helpdesk@templejc.edu, or call 254-298-8450


TECHNOLOGY TIPS

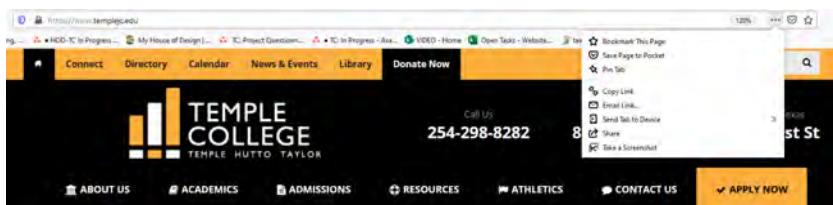
Create, change or customize a view in Microsoft Outlook

Having trouble reading your emails? Microsoft Outlook lets you customize the size of the text in your emails, as well as the font. Read this article to learn how you can customize your inbox as well as the mail you send: <https://support.microsoft.com/en-us/office/create-change-or-customize-a-view-f693f3d9-0037-4fa0-9376-3a57b6337b71>

Take a snip

Want to capture something on your screen, such as a portion of a web page? There are several ways to do this.

- **Keyboard shortcut:** Press the Windows logo key  + Shift + S to open the snipping bar, then drag the cursor over the area you want to capture. The area you snipped will be saved to your clipboard.
- **Using your browser:** Web browsers also have built-in snipping functions. In Firefox, for example, just look for the three dots on the upper right of each page. Clicking here will bring up a menu that includes "Take a Screenshot". If you click that option, it brings up a tool that lets you select the area you want to capture. Firefox gives you the option of copying the selection to your clipboard or downloading it for future use.



What's your favorite mode?

Make your apps and app tiles stand out with Light or Dark mode. Select **Start** > **Settings** > **Personalization** > **Colors**. Under **Choose your color**, select the color mode you prefer.

Choose Light or Dark mode



Don't fall for phishing emails

Be cautious about opening attachments and downloading files from emails, regardless of who sent them. These files can contain viruses or other malware that can weaken your computer's security. If you are not expecting an email with an attachment from someone, such as a fax or a PDF, please call and ask them if they indeed sent the email. If not, let them know they are sending out phishing emails and need to change their email password immediately.

Never enter private or personal information into a popup window.

If there is a link in an email, use your mouse to hover over that link to see if it is sending you to where it claims to be. This can thwart many phishing attempts.

Look for 'https://' and a **lock icon** in the address bar before entering any private information on a website.

Look for spelling and bad grammar. Cybercriminals are not known for their grammar and spelling. Professional companies or organizations usually have staff that will not allow a mass email like this to go out to its users. If you notice mistakes in an email, it might be a scam.

If an email seems suspicious, please forward it to Helpdesk@templejc.edu so our Information Security team can examine it and determine if it is legitimate.

Tips for avoiding email scams

If an email seems suspicious, here are some tips for identifying a scam. We advise to be wary of emails that:

- Ask for login credentials
- Threaten to suspend an account or service without a response
- Notify you of a virus
- Tell you to click a link to solve any of the above issues