CYBERSECURITY TRAINING FOR TEACHERS (CTT)

EXISTING THREATS AND ENFORCING DEVICE SECURITY

Objectives

At the end of this module, the learner should be able to:

- Apply physical security to computing devices.
- Secure their devices from logical threats.

Education has employed the use of technology a lot more in the recent past. Teachers are now able to use mobile devices, laptops and computers as part of instructional material. With the onset of an unprecedented global pandemic, the need for technology in education has never been clearer. Online classes, the use of the internet to share learning material and communication between instructors and learners has entirely been dependent on our physical devices.

These devices are prone to potential security threats that may lead to loss and corruption of data or physical damage to the hardware itself. Our devices are exposed to both physical and non-physical security threats.

Physical threats cause physical damage and they include fires, floods, theft, vandalism or even accidents such as spilling your morning coffee on your keyboard.

Non-physical threats, on the other hand, cause loss or corruption of data, unauthorized access to private data, illegal monitoring of activities on the system, loss of sensitive information and may disrupt operations that rely on the computer systems. Non-physical threats are caused by malware, phishing attacks or even software and applications that have not been updated for a while.

To protect devices from both physical and non-physical security threats, it is important that measures are put into place, both at the personal level and at the organizational level.

The following list shows some of the possible measures that can be taken to protect against cyber security threats and consequently secure your data and that of your students and learning institution:

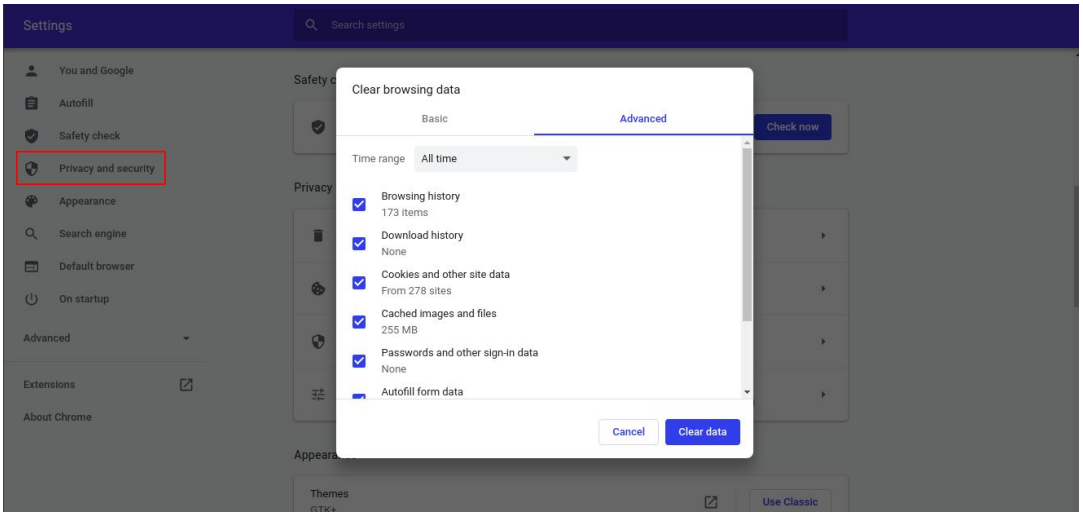
CYBERSECURITY TRAINING FOR TEACHERS (CTT)

1. **Be selective over the applications and software that you use.** There are many applications out there that are not inherently safe. Before you download, buy and use that software or application do your due diligence with regard to researching it. Look up the software/app reviews from other users and think critically about the permissions it requires. For example, a game application has no use for your call logs or camera, if it does that's a red flag.
2. **Employ use of strong, unique passwords across all your devices.** To physically access your mobile or laptop use biometric authentication such as facial recognition of fingerprint scanning, if that option is available. Use password managers for passwords that you use on websites that you need access to.
3. **Ensure you have an antivirus that's always updated.** Windows 10 operating systems come with an inbuilt antivirus software, Microsoft Defender Antivirus, that works just as equally if not better than other third party antivirus software. Always make sure it is up-to-date and running anytime you are online. If you do decide to get other antivirus software, be sure to always keep them up to date and ensure that they are always running.
4. **Clear your cache and your browser history frequently.** Your browser stores small pieces of information about you every time you visit a website. These pieces of information are called cookies. Websites use cookies to keep track of users and enable user-specific features and they are stored in the browser's cache. This cache also holds saved searches and your web history which could easily have very personal information such as your home address, students' information and other personal data. To better protect that information, be sure to delete browser cookies and clear your browser history on a regular basis.

   On Chrome:

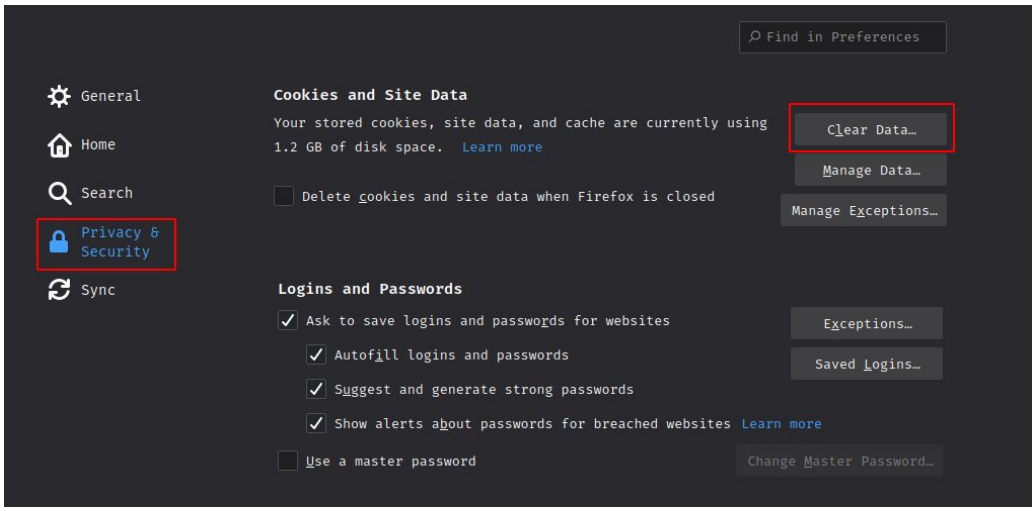
   - On your computer, open Chrome.
   - At the top right, click More .
   - Click **More tools Clear browsing data**.
   - At the top, choose a time range. To delete everything, select **All time**.
   - Next to "Cookies and other site data" and "Cached images and files," check the boxes.
   - Click **Clear data**.

CYBERSECURITY TRAINING FOR TEACHERS (CTT)



On Firefox:

- Click the menu button ☰ and select Preferences.
- Select the Privacy & Security panel.
- In the **Cookies and Site Data** section, click Clear Data



5. **Install all updates across all your devices.** Ensure that your operating system, software, mobile application and your mobile device are updated to the latest versions. Updates fix vulnerabilities that hackers can use to access your sensitive data. You can easily enforce this by automating your updates by reviewing your device settings.
6. **Always backup all your data frequently in a safe location.** Losing important data such as students' information, exam results or even personal information may be painful. Having a restoration point for your data makes it easier to protect your, your student's and your learning institutions' data.
7. **Avoid public Wi-Fi at all costs.** This is Wi-Fi available to you in coffee shops, malls, restaurants and hotels - it allows you to access the internet for free. Public Wi-Fi networks are vulnerable to attacks from hackers who can easily breach a device, access the network, and steal data. While the convenience is enticing, the best defense is to completely avoid them. As a matter of being cautious, you should also **turn off wireless connectivity (Wi-Fi and Bluetooth) when you are not using them.** Not only will this help avoid automatic connection to unencrypted networks but also save your battery. If you urgently need access to WiFi and can't ensure that the public WiFi is protected, then it is best to employ the use of VPNs. A VPN will enable you to connect to a network securely and simultaneously protect any browsing activity you do on the public Wi-Fi from prying eyes.
8. **Lock your devices when they are not in use.** Always lock your phone and laptop when they are not in use. It takes a very short time for a hacker to quickly install and run malicious programs and have full access to your laptop. Your device could also get lost or be stolen. The more you get used to always locking your devices, the faster it becomes muscle memory. The easiest trick for laptops is pressing the 'Windows' key and 'L' simultaneously.

9. **Never leave your devices unattended** in public places, in a shared living space or visible for potential intruders. Use inconspicuous carrying cases for your devices which helps avoid potential bag snatchers from targeting your devices.
10. **Use cable locks to protect your computers from theft.** You can prevent theft of your laptop or your computer and its peripherals by using a cable lock that attaches to the security slot built into most devices.

Discussion Question:

1. Have you encountered any physical or logical threats to your devices? If so, what was it and how did you deal with the consequences?
2. From your own evaluation, how secure are your devices? What new technique/method will you implement to enforce device security?