



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

THE NEED FOR SOFTWARE UPDATES, ANTIVIRUS AND DATA BACKUP

Objectives

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

- Update and secure software regularly
- Implement the use of anti-virus software
- Have periodical data backup

Software Updates

Our devices run on operating systems, software and applications that enable us to work effectively. These operating systems, software and applications are always being updated by their developers. It is important that we incorporate these updates as often as they are released. It is easy to skip software updates as they can take up a few minutes of our time, and may not seem that important. But this is a mistake that can allow or facilitate hackers to use the vulnerabilities to access and steal private information which may put you at risk of identity theft, loss of money or even more devastating consequences, not just for you but for your entire learning institution.

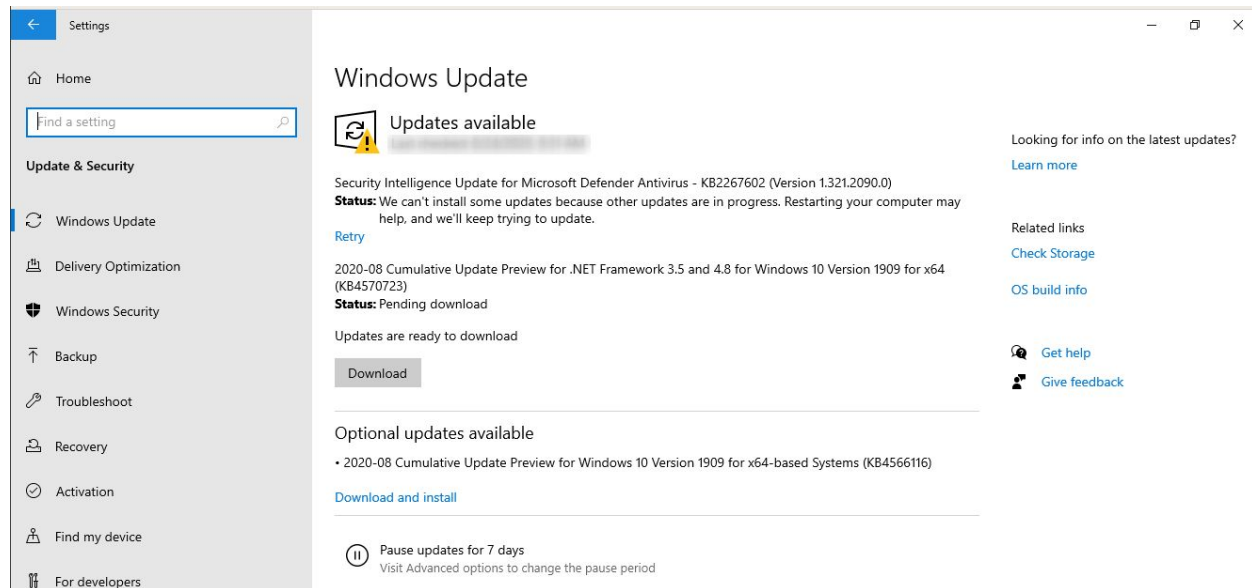
Why are operating systems, applications and software constantly updated?

1. They include critical patches to security vulnerabilities.
2. They can include new features or capabilities that can make our work easier. For example, the WhatsApp update that increased the group participants from 100 to 256 enabled teachers with classes that had more than 100 students to effectively communicate with them in only one group.
3. Updates can also enable better compatibility with different devices or applications.

Updates are aimed at making the user experience much better and can improve your experience in the long run. Across all devices, automating software updates has been designed to be a seamless process. You can auto-update on both your mobile phone as well as your laptop or home computer which ensures that your devices stay current.



CYBERSECURITY TRAINING FOR TEACHERS (CTT)



In summary, keeping your security software up-to-date is critical as this will protect you from most security threats. Auto-updates for software on your mobile devices and computer make the process seamless and regular. Before downloading any software, ensure you read user reviews and do your due diligence in terms of researching the software.

Backup of Data

Educators deal with lots of sensitive and important information. Student records, employee information, curriculum material, assignments and exam results and many other types of critical information. What other critical information do you deal with daily as an educator?

This information needs to be backed up in order to recover from an unplanned event that may lead to loss or corruption of data. How devastating would it be if you lost all your student records and had no point of recovery? Data loss can happen to anyone and having a backup strategy can help in case of a drastic event. It's a good idea to make backing up data as a part of your cyber hygiene.



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Considerations to make for when backing up data:

- How frequently should the data you own be backed up?
- Where do you want to back up your data?
- How safe is the backing up method you intend to use?
- How long must daily, weekly, monthly, annually backup copies to be kept?

Data Backup Options

There are plenty of options when it comes to backing up data. These are the most common options are:

- External Hard drives such as USB flash drives and SSDs. They are portable, easy to use and capable of storing large files.
- Cloud backup options such as Google Drive, OneDrive or DropBox which allows users to back up their data in a remote location and can be accessed anytime through the internet. When backing up data on cloud storage it is important to further encrypt the data, especially if it is sensitive, critical or contains personally identifiable information.
- For countries or cities that are prone to natural disasters that can damage physical data storage locations such as a physical server or hard drives, backup to cloud is recommended. Datto is an example of such a cloud backup service provider.
- Backup services provide companies the protection they need to keep all their data secure.
 - With whom should you share content?
 - Who should you interact with?
 - How do you control who has access to what you post?
 - Should you follow/interact with your students at all?
 - What about parents and colleagues?
 - Are there posts you should avoid posting/reposting or sharing?



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Antivirus

Antivirus software, also referred to as anti-malware software, is a type of software designed to identify and remove malicious software from your computer. Virus and other malicious software can affect your computer and cause your computer to slow down, it can damage or delete files and even reformat your hard disk. Anti-viruses scan a computer for suspicious files and activity, scan specific files or programs, attachments, and downloads.

Antivirus detects viruses through signatures and behavior of programs. If it appears malicious then the antivirus software is able to clean, quarantine or delete the program. Additionally, antivirus software blocks spam and ads, defends against hackers and data thieves, enables and ensures protection from removable devices and as well as protects your personal data and files.

Some examples of antivirus software include:

- Norton Antivirus
- Kaspersky
- McAfee
- AVG
- Microsoft Defender Antivirus

Just as with all other programs, always ensure your antivirus software is updated and always running.

Poll Questions:

1. How often do you update your software and operating systems?
 - a. Never
 - b. Once every month
 - c. Whenever I am prompted
2. Are you aware of any backup policies that your learning institution may have?
 - a. No
 - b. Yes



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Discussion Question:

1. What critical software should you frequently update?
2. What information in your learning institution do you think would benefit from frequent backups? And, why?