



## Cybersecurity Training for Teachers



# Cybersecurity Training for Teachers

*COMMONWEALTH OF LEARNING  
(COL)*

COMMONWEALTH OF LEARNING (COL)  
BURNABY, BRITISH COLUMBIA, CANADA



*Cybersecurity Training for Teachers by Commonwealth of Learning is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/), except where otherwise noted.*

<https://creativecommons.org/licenses/by-sa/4.0/>

This book was produced with Pressbooks (<https://pressbooks.com>) and rendered with Prince.

# Contents

General	vii
Acknowledgement	ix

## Part I. Introduction to Cybersecurity

Introduction to Cybersecurity	3
The CIA Triad	9
Online Learning Platforms	14
Online Learning Platforms Case Studies	22
Cybersecurity and Data Protection Laws: A Legal Perspective	26
Module 1 Infographic	34
Module 1 Files and Resources	35

## Part II. Cybersecurity Threats and Mitigation

Cybersecurity Threats, Vulnerabilities & Risks	39
Classroom Hijacking & Security Breach	44
Ransomware & Identity Theft	45
Identifying Cyber Attacks & Attack Vectors	51
Case Studies on Online Learning Platforms	54
Cyberattacks	
Reporting Cybercrime	58
Module 2 Infographic	59

Module 2 Files and Resources	60
------------------------------	----

### Part III. Best Practices

Password Management	63
Identifying Bad Passwords	71
The Need for Software Updates, Antivirus & Backup	74
Securing Online Communication	78
Device Security	86
Module 3 Infographic	91
Module 3 Files and Resources	92

### Part IV. Cyber Safety for Students

Student Online Protection	95
Online Risks	97
Incorporating Cybersecurity in the Classroom	99
Laws on Child Online Protection	105
Role of Students, Teachers and Parents	114
Module 4 Infographic	119
Module 4 Files and Resources	121

## Course Description

To mitigate the effects of school closures as a result of COVID-19, digital platforms have been variously adopted by governments to enable teachers to deliver blended or full online lessons to the learners. In many families in the developing Commonwealth, learners are increasingly accessing online learning and assessment resources using devices owned by parents or older family members.

The shift to online learning presents various security threats to teachers, learners as well as their parents and carers as they are now more prone to cyber-attacks than before. Recent reports show a spike in cybercrime since the beginning of the COVID-19 pandemic, making cybersecurity a key concern for educators.

The Cybersecurity Training for Teachers (CTT) course is designed to provide teachers with the knowledge they need to protect themselves and their students online, as well as create awareness for the parents and carers.

The course targets secondary and primary school teachers as well as teacher educators and will run over four weeks. It will require up to five hours of time each week. Participants will learn from articles, case studies, videos, as well as discussions with fellow learners and mentors.

## Outcomes of this Course

After completion of this course, the participant is expected to be able to:

1. Understand cybersecurity and its relevance in digital learning
2. Identify and mitigate various cybersecurity threats and attacks
3. Outline various techniques that students can use to protect themselves when using technology
4. Incorporate best cybersecurity practices through protective and preventive measures; and
5. Demonstrate understanding of cybersecurity laws, acts and relevant regulatory organizations and bodies.



# Acknowledgement

The Cybersecurity Training for Teachers (CTT) course was conceptualised by the Teacher Education initiative in liaison with the Technology and Innovation team at the Commonwealth of Learning.

The course material was developed with expertise from e.KRAAL Innovation Hub, Kenya. The course development team included Mr Walter Buyu (Project Lead), Ms Patricia Musomba, Ms Linda Mwibanda, Ms Malusi Faith and Ms Murrey Eddah.



PART I

# INTRODUCTION TO CYBERSECURITY



# Introduction to Cybersecurity



*One or more interactive elements has been excluded from this version of the text. You can view them online here: <https://opentextbooks.colvee.org/cybersecuritytrainingteachers/?p=19#oembed-1>*

## Transcript

Hello, and welcome to this first week of the cybersecurity training for teacher's course. My name is Patricia Musomba. And I'll be your instructor this week. During this week, we'll define cyber security and explore its importance in our lives. We'll also look at various learning platforms such as learning management systems, and video conferencing platforms. Lastly, we'll also look at various cybersecurity laws and regulations.

Before we look at cyber security, let us first look at how technology has changed our lives. Technology has changed how we interact, how we work, how we learn, and even how we teach. For example, through technology, you're taking this course at your own convenience. Through technology, we're also able to teach online using video conferencing platforms such as Zoom. Exams are now even administered online, and teachers and students can

access material via learning platforms. This has positively enhanced distance and online learning therefore, extending the reach of education into rural and remote areas. Despite the life changing impact of technology, it has also raised some security concerns. Cybersecurity attacks are now on the rise due to the incorporation of online learning in learning institutions. With this in mind, let us now look at what cybersecurity is.

Cybersecurity is the practice of protecting systems, devices, networks, programs and information from digital attacks. Its main function is to protect the information stored in these systems for modification and unauthorized access. It is important to remember that cybersecurity is a continuous process and therefore we should bear it in mind and every single time we're online. To properly understand cybersecurity, we also need to understand the cyberspace.

The cyberspace is the global interconnected digital technology. It is the virtual environment on which online communication takes place. The cyberspace enables us to interact online on social platforms, as well as do business, and teach as well as learn. It is made up of systems, devices, networks, as well as information. For example, when you connect to the internet through your mobile phone or your computer, you become a part of the cyber space. In addition, when you're sharing stories online via social platforms, such as Facebook, and Instagram, you also are part of the cyberspace. The

cyberspace is virtual and therefore it is not geographically confined. Because it is a global network, it is very difficult to actually secure the whole network. This is because attacks could come from virtually any place in the world. With an understanding of cybersecurity, let us now explore its importance.

The main aim of cyber security is to secure the information. But what kind of information needs securing, we're looking at information such as financial data. This includes things like fee payments, banking details as well as payroll information. We also have personal information. This information includes employment history, residential addresses, contact information, as well as health information. We also have student records, that is performance grades, health information as well as parent information. Another type of information that we need to protect is credit card information. This is because when an attacker has your credit card data, they are able to pay online using your card, they can also impersonate you.

Lastly, we also need to protect intellectual property. This is data or other content that you have created on your own and you would not want used without your explicit permission. For example, we have books that you created and also training contents that you have created for your students.

What are some of the consequences of not protecting yourself and your information? Failure to protect your data assets, such as your computer,

your mobile phone could lead to cyberattacks. A cyberattack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Usually, the attacker seeks some type of benefit from disrupting the victim's information and computers. Cyberattacks usually have very devastating effects on the person's computer or the organization's network.

Let us look at some of these effects. Cyberattacks can lead to financial losses. For example, when criminals get a hold of your credit card information, they can use it to pay for things online without your permission. They can also lock your school's data and ask for a ransom in return. Thereby, the school will spend a lot of money to gain access back to the data.

Cyberattacks can also lead to damage in the brand reputation and image. I'm sure you've heard of people who have been hacked and the criminals have shared very damaging data about these people online. These days can be very embarrassing, and can damage your reputation. For schools, when this information is shared online. It can also damage the school's reputation and hinder any enrollments of students.

Another effect of cyberattacks is identity theft. When hackers have enough information about you, they can easily impersonate you, and can even go to an extend of taking loans in your name. Lastly, cyberattacks usually inconvenience normal business



operations. This is because, as the IT personnel is trying to rectify the situation, normal operations are disrupted. For example, if hackers prevent access into the learning management system, students will be unable to access the content and classes will be disrupted for the day.

Having looked at what cyber security is, and the impacts or other the consequences of cyber attacks, we need to understand whose responsibility it is to implement cyber security. It is important to mention that cyber security is a collective effort. Therefore, it is your responsibility and mine to make sure that we are protected against cyberattacks. Cyber attackers usually target people by using attacks that are specifically designed to deceive you into divulging confidential information. They also try to trick you into clicking malicious links. This is usually known as social engineering and you will explore this much later.

It is therefore very important for you to learn about cybersecurity through an awareness program or through a course such as this one that you are taking. That way you will know about cyber security, you will know about the attacks and how to protect yourself.

And with that, we have come to the end of this video. In this video, we defined cybersecurity and the cyberspace; we also explored its importance. We then looked at the consequences of cyberattacks, and how it is your responsibility to make sure that you're protected.



# The CIA Triad

## Introduction

The main purpose of cybersecurity is to ensure Confidentiality, Integrity and Availability (CIA) of data and services. The CIA triad is a model that is used to secure information. The CIA triad is essential in cybersecurity as it provides important security considerations to safeguard and protect critical information. In this article, you will learn how the CIA triad enhances your security.



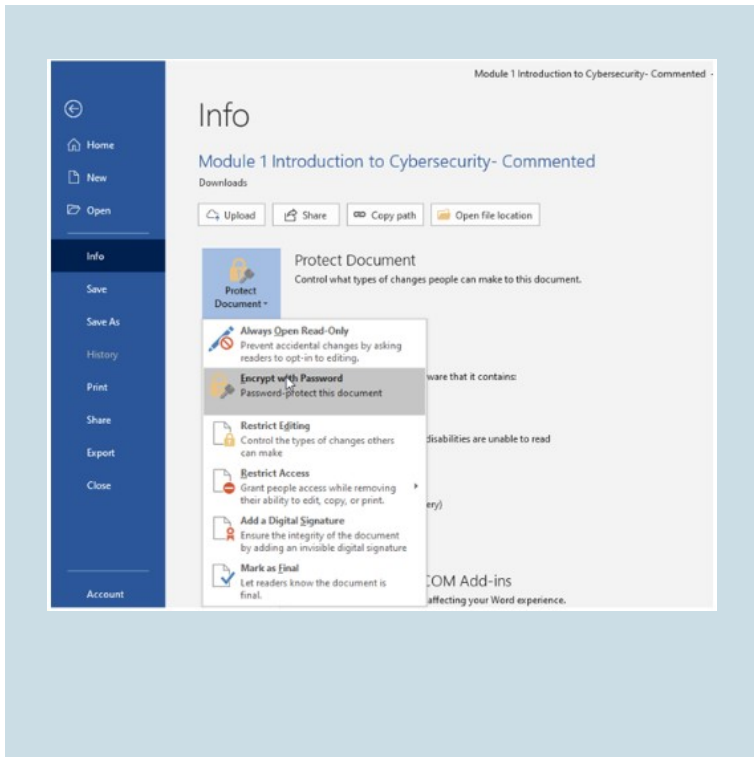
# What is Confidentiality?

Confidentiality refers to efforts to keep data private or secret. Confidentiality ensures that information is accessed only by authorized personnel. For example, access to the student management system should be granted to teachers and denied for non-teaching staff. Unauthorized personnel should not be allowed to access any sensitive data as this could lead to privacy issues and data breaches. A data breach is a security incident that exposes confidential or protected information to the public or to unauthorized parties.

Confidentiality is achieved through effective identification and authentication. This can be done through the use of usernames, passwords, biometrics (e.g. fingerprints) and identification (ID) badges. For confidential files, you can maintain confidentiality by password-protecting the files so that, anyone without the password cannot access the files.

*On Windows you can do this using the following steps:*

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



Confidentiality examples:

- Accessing your laptop or phone using a fingerprint, PIN or a password known only to you.
- Sending emails over a secure communication channel
- Using secure messaging platforms such as WhatsApp and Telegram
- Showing your ID badge to the security personnel at the school gate before being let in.
- Using a password to access your email account.
- Using a password to protect a folder containing your students' exam results.

## What is Integrity?

Integrity is about ensuring that data has not been tampered with. Therefore, integrity prevents unauthorized modification or deletion of data. Only authorized personnel should be allowed to make changes or delete data. It ensures that the data is correct, authentic, and reliable. Data must be protected while in use, in transit, and when stored.

Integrity examples:

- Teachers can only change the grades of the subjects that they teach.
- Students should not be allowed to change their grades.
- Limit access to files because if unauthorized people cannot access the documents, they cannot tamper with them. This can be done by password protecting your devices and documents.
- Maintain backup copies of confidential data to ensure you have a clean copy to revert to in case of any tampering.
- Use secure communication channels to send and share data to prevent it from being intercepted and tampered with.

## What is Availability?

Availability refers to the guarantee of reliable and timely access to information and services by authorized people. This ensures that authorized personnel can access networks, systems, applications and information whenever needed.

Examples of availability:

- Teachers can access the school's student management system any time.

- A good internet connection will ensure availability when accessing information online
- Students can access their results in a timely manner.
- Students can access the learning management systems at their convenience.

Confidentiality, integrity, and availability can all be easily tampered with by cyber-attacks leading to loss and modification of information. When implementing security measures, consider what element of the CIA triad each measure attempts to protect and maintain. For example, implementing a fingerprint lock on your mobile phone protects your information's confidentiality and integrity.

# Online Learning Platforms



*One or more interactive elements has been excluded from this version of the text. You can view them online here: <https://opentextbooks.colvee.org/cybersecuritytrainingteachers/?p=25#oembed-1>*

## Transcript

Having looked at the CIA triad, we're now going to explore various online learning platforms and their security concerns. Online Learning is the future of learning. With rapid advancement of technology, learning has never been easier, both teachers and learners can access quality education via online platforms. Learning has greatly evolved over the years, the traditional class involved face to face instructional learning. Teachers and educators then incorporated technology to aid face to face learning.

For example, through the use of projectors and computers. Today, we have blended learning which is a mixture of face to face and online learning. For online learning, students can access materials remotely. Some courses are usually offered fully online without any face to face interaction with the instructor. This is known as distance learning. Learning institutions have resorted to distance



learning due to the corona pandemic to actively engage their students. Online Learning is usually supported by various platforms. These platforms include, Learning Management Systems, Student Management Systems and Video Conferencing Platforms.

A Learning Management System or LMS is a software application used for administration, documentation, tracking, reporting, automation and delivery of educational courses, training programs or learning and development programs.

LMSs are designed to support teachers and teacher educators in administering and managing accessible courses. Learners can also pace themselves and access the course material from virtually anywhere. The learner's experience can be personalized therefore aiding in better user experience. Learning Management Systems usually store very confidential data such as training content, student's information and teacher information. This information is very crucial in the administering of online courses. Therefore, it should be protected to prevent any data breaches.

Some of the commonly used LMSs include, talent LMS, Canvas, Moodle, and mookIT. However, LMSs usually have some security concerns that we should all take into consideration. Most LMSs are vulnerable to malware.

Malware is any malicious software that can be used to divulge any confidential information or to

gain unauthorized access into a system. Malware can also be used to obtain confidential information such as passwords and usernames. Once an attacker obtains the username and the password, they can easily login to your account and change the password, therefore, you will not be able to log in as a legitimate user.

LMSs are also vulnerable to password guessing attacks. In these attacks, the attacker usually tries different combinations of password and username and tries to guess the correct one. If a user is using a weak password, it is easily guessed and therefore, an attacker can easily gain access into your account. Having explored these two security concerns, it is important to know what security features are available to you for you to implement and prevent these cyberattacks. This learning management system should also be updated regularly. This is because vendors continually release updates that address various security concerns that were found in previous versions.

We also need to use very strong password for our LMS accounts. This is because strong passwords are not easily guessed, and therefore, the attackers will not be able to gain access into your account.

Another platform that supports online learning is Student Management Systems or SMSs. These are platforms that are used to manage student data in any learning institution. Student data is very critical and sensitive in any learning institution. Therefore, it should be protected effectively and properly. A leak

of this data could damage a school's reputation and brand image. Some of the key functionalities of SMSs include, Student Information Storage, faculty management, report generation, access portals for students and parents, as well as enrollment or registration management.

Some of the popular SMS in the market include open SIS and school time. Just as we've mentioned for LMSs, student management systems also vulnerable to malware. This is because SMSs store very critical and sensitive data that is very alluring to attackers, attackers will therefore use malicious software to try and gain access into the Student's Management Systems.

Attackers are always trying to get you to click on links and download malware. For example, they will send you spam emails with various links attached. And when you click on these links, you download malware into your computers or even into your mobile phones. It is very important to consider the security features that are available in the Students Management System. This will prevent attackers from gaining any unauthorized access.

Additionally, remember to use very strong passwords to login into the Student Management System. You should also avoid sharing passwords or even writing them down. This is because unauthorized personnel such as students can get a hold of these passwords and use them to login in to the Student Management System. Students having

these passwords can even use the system to modify their grades.

Lastly, we have video conferencing platforms. These platforms are used to hold live sessions and webinars. These live sessions usually simulate a real classroom and therefore, students and teachers can interact and promote engagement during remote learning. For example, during these live sessions, students can ask real time questions and teachers can provide guidance. Some of the popular video conferencing platforms include Zoom, Microsoft Teams, and Google Meets.

With video conferencing platforms an intruder joining the call is a major security concern. Without proper implementation of security features, unauthorized people can access confidential training sessions and disrupt the sessions. The links to these sessions are usually obtained from social media platforms as well as unsecured networks such as public WiFi. Once intruders have joined the session, they usually post inappropriate content as well as share links that leads to malicious websites on the chat feature or the video conferencing platform. This makes the video conferencing platform vulnerable to malware. We'll also look at various case studies of such incidents where intruders have interrupted a class or training session.

Privacy is also another consideration when using video conferencing platforms. Most platforms usually offer a recording feature where teachers are

able to record training sessions and share with their students for future reference. It is important for teachers and teacher educators to seek permission from the parents before sharing such content. When sharing the recorded sessions, it is also important to share them over secure channels. Before using any video conferencing platform, make sure to explore all the security and privacy features that are provided by the platform. Once you've explored those, make sure that you've implemented them before any virtual meeting.

Having looked at the various security concerns, let us now look at the various guidelines that are provided for teachers and students when using video conferencing platforms. When conducting online classes, teachers should engage their students on video conferencing do's and don'ts. These include, you should ask your students to mute their mics, they can enable the microphone where they need to talk to the rest of the class.

You should also advise students to join using their real names. This will enable the teacher to properly identify and verify the students. Ask the students to only share information related to their lesson on the chats. You should also let them know of the consequences of breaking any of the classroom rules. Students should also use the latest version of the video conferencing solution such as Zoom or Microsoft Teams.

Some of the guidelines for teachers include: be careful about the documents you show on the

screen. This will avoid accidental sharing of confidential data. Make sure to verify the student's identity to prevent intruders from joining. This can be done by enabling the waiting room. In this you should also advise your students to use their real names for easier verification. You should also not allow the students to rename themselves for easier class management. You should also not allow students to share their screen unless it is needed for class presentations.

If need be, remove any students or parents who do not follow the classroom rules this will maintain order. The teacher should also disable private messages to foster transparency and easier management of the chat feature. Lastly, you should always reiterate the guidelines at the beginning of each class. This will ingrain security into your students and ensure they exercise caution while online.

We will now explore various considerations when selecting technology to support online learning.

Before selecting any technology to use for online learning, you should ask and answer some of these questions. Is the online learning technology accessible? How easy is it to use the technology? And is the online planning technology safe and secure for school use? What are some of the security features that are provided by the online learning technology?

By asking these questions, you'll always make sure

that security is a consideration during the selection process. As we have seen, security is an important consideration in online learning. As a teacher, you should ensure that all the systems and applications you use for online learning are secure. This will protect you and your students from cyberattacks, and protect your information.

This brings us to the end of this topic. In this topic, we learnt about various online learning platforms. This includes the Learning Management Systems, Student Management Systems, and Video Conferencing Platforms. We also looked at the security concerns and what to do to make sure that these platforms are secured. Next, we're going to have a discussion on these online learning platforms.

# Online Learning Platforms Case Studies

## Zoom



*Image  
from  
Techcrunch*

In March of 2020, many countries went into lockdown as one of the measures to curb the spread of the Coronavirus. This meant that brick and mortar schools had to close down and transition to online learning. Video conferencing platforms came to the aid of many schools during the transition period, with Zoom being one of the preferred options. With countless number of schools utilizing the video conferencing platforms, malicious attackers started to target these online classroom meetings to disrupt the sessions, share inappropriate content and even links to malicious sites. In the case of Zoom, this type of attack is known as zoombombing.

## Singapore

On Wednesday April 8th, an online Geography class proceeded



as scheduled. However, two male hackers zoom bombed the class and proceeded to share obscene pictures to the teenage girls attending the lesson. The hackers went ahead to ask the girls to show their private parts on camera.

Due to this incident, Singapore suspended the use of Zoom for online learning until the security concerns were addressed. The Ministry of Education encouraged teachers to learn and implement the security features that Zoom offers as well as to use updated versions of the Zoom application. To read more about the case, use this link.

Zoom has since then introduced security features to prevent Zoom bombing such as setting meeting passwords, waiting room features and disabling screen sharing for participants by default. When setting up classes, check the meeting settings to ensure that the security features are implemented.

*Some of the settings to modify include:*

- Disable “Join Before Host” so people can’t cause trouble before you arrive.
- Enabling “Co-Host” so you can assign others to help moderate.
- Disable “File Transfer” so there’s no digital virus sharing.
- Disable “Allow Removed Participants to Rejoin” so booted attendees can’t slip back in.

To explore more security features provided by Zoom, use the link below:

- Zoom security features: <https://zoom.us/security>

For other video conferencing platforms, use the provided links:

- Microsoft Teams: <https://docs.microsoft.com/en-us/microsoftteams/teams-security-guide>
- Cisco WebEx: <https://bit.ly/3gG9EDf>
- Google Meet: <https://support.google.com/a/answer/9822731?hl=en>

## Moodle LMS

In 2017, a security researcher was able to hack into Portugal's University of Porto Moodle learning management system. He was able to access and manage user accounts, view hidden quizzes, download a full backup of the university's site as well as change grades. Luckily, the hacker did not share this data, but proceeded to contact the university and have the weakness resolved. Use this link to learn more about the case.

Moodle now separates user accounts to limit what a user can do on the site. For example, students have learner accounts hence they are only able to read the course content but they are not allowed to change it. Teachers have instructor accounts therefore they are able to create and add content for various classes.

To explore other Moodle security features, use the link below:  
Moodle LMS: <https://docs.moodle.org/19/en/Security>

## Stanford University Data Breach

In 2019, Stanford students were able to view other students' college common applications and high school transcripts.

Accessible documents also contained sensitive personal information including, for some students, Social Security numbers. Other data that was exposed included students' ethnicity, legacy status, home address, citizenship status, criminal status, standardized test scores, personal essays and whether they applied for financial aid. Official standardized test score reports were also accessible. This was caused by the use of an outdated content management system known as NoliWeb. A lot of learning management systems and student management systems are vulnerable to attacks that lead to data breach lead and data leaks. Stanford proceeded to notify the affected by the data breach as is required by the law. They also contacted the vendors to have the vulnerability rectified. Always update all your software to ensure that all the security weaknesses are rectified.

Read further about the case: [Stanford Daily](#)

# Cybersecurity and Data Protection Laws: A Legal Perspective

Having looked at case studies of hackers misusing the internet and the cyberspace to perpetrate malicious attacks, what does the law say about cybercrime? Due to the increasing cost and damage of cybercrime, there is dire need for countries to pass laws designed to prevent cyber attacks and prosecute cyber criminals. Cybersecurity laws and regulations act as directives to aid institutions in the implementation of cybersecurity safeguards to protect them from cyber attacks. These laws also establish offenses and their respective penalties. The heavy fines and penalties are used to deter cyber attackers from committing cybercrime. It is crucial to have an understanding of these laws as they put into perspective the extent of the damage caused by cyber attacks and the government's cybersecurity efforts to curb cybercrime and thwart cyberterrorists.

Common provisions and directives in cybersecurity laws include:

- Increasing penalties for computer crime or addressing specific crimes, e.g., ransomware, unauthorized access, phishing etc.
- Requiring government agencies to implement training or specific types of security policies
- Creating task forces, councils or commissions to study or advise on cybersecurity issues.
- Supporting programs or incentives for cybersecurity training and education.

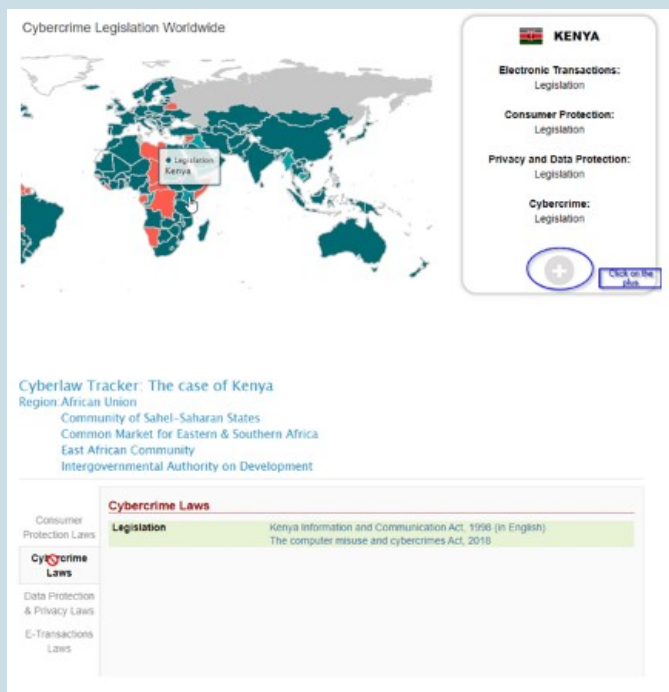
In this article, you will explore various cybersecurity laws and legal stipulations. Globally, 154 countries (79%) have enacted

cyber laws. To check whether your country has implemented any cybersecurity laws, you can utilize the United Nations Conference on Trade and Development (UNCTAD) [website](#).

*Steps to follow:*

1. Click on the link above.
2. On the map provided on the site, click on your country.
3. Click on the Plus (+) to expand and read more on the laws. This will show various legislations grouped in categories such as data protection, cyber laws and consumer protection laws.

Example of checking Kenya's cybersecurity laws:



## Kenya: Computer Misuse and Cybercrimes Act 2018

The Computer Misuse and Cybercrimes Act was enacted in 2018 to protect the confidentiality, integrity and availability of computer systems, programs and data. The Act also provides

guidelines for investigation, prosecution and punishment of cybercrimes.

Some of the key provisions in the Act include:

- The Act establishes various computer misuse and cybercrime offences including unauthorized interference or interception of computer systems programs or data, false publication of data, cyber harassment, cyber terrorism, identity theft and impersonation, phishing, computer fraud, computer forgery, unauthorized disclosure of passcodes, fraudulent use of electronic data among others.
- The Act prescribes hefty penalties for contravention of its provisions. These include fines as significant as 50,000 US dollars, imprisonment of up to 20 years, confiscation of assets purchased from proceeds of an offence and compensation.
- The Act requires service providers to assist in investigation of offences e.g. by collecting and providing data to the investigation officers.
- The Act also establishes investigation procedures for search and seizure, real-time collection of data and evidence preservation.

## **European Union: General Data Protection Regulation (GDPR)**

The GDPR is a set of rules and legal provisions imposed on the European Union member states. The main aim of the GDPR is to ensure that EU citizens have more control over their data.

It applies to all organizations that collect and process EU citizens' data. The GDPR is very similar to the UK's Data Protection Act of 1998.

Some of the key provisions in the GDPR include:

- Consent: Any organization handling sensitive data must seek consent every time they access the data. Consent agreements should be concise and clear.
- Right to access: Owners of any data have the right to request confirmation on what data is being processed and for what purpose.
- Breach notification: Companies to notify all data subjects that a security breach has occurred within 72 hours of first discovering it.
- Right to be forgotten: Companies are required to erase all personal data when asked to do so by the owner of the data (data subject).





# Canada: Personal Information Protection and Electronic Documents Act (PIPEDA)

PIPEDA contains a number of provisions applicable to data protection and cybersecurity, including:

- Organizations are responsible for personal information under their control and must designate an individual or individuals who are accountable for compliance with the principles set out in Schedule 1 of PIPEDA.
- Personal information must be protected by security safeguards appropriate to the sensitivity of the information.
- Security safeguards must protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification, regardless of the format in which it is held.
- The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, format of the information, and the method of storage.
- The methods of protection should include (a) physical measures – e.g., locked filing cabinets and restricted access to offices; (b) organizational measures – e.g. security clearances and limiting access on a “need-to-know” basis; and (c) technological measures – e.g. the use of passwords.

Canada has quite a number of laws and frameworks governing cybersecurity and data protection. Most of these laws are based on principles established in the to erase Canadian Standards Association Model Code for the Protection of Personal Information<sup>7</sup> (CSA Model Code).

These 10 principles include:

1. accountability,
2. identifying purposes,
3. consent,
4. limiting collection,
5. limiting use, disclosure and retention,
6. accuracy,
7. safeguards,
8. openness,
9. individual access and
10. challenging compliance

## **India: Information Technology Act, 2000**

The Act contains some of the most stringent privacy requirements in the world. The Act creates punishable offenses for the following:

- Tampering with computer source documents.
- Publishing or transmitting obscene material in electronic form.
- Publishing or transmitting material depicting children in sexually explicit acts, etc., in electronic form.
- Breach of confidentiality and privacy.
- Punishment for disclosure of information in breach of lawful contract.
- Penalty for publishing electronic signature Certificate false in certain particulars.
- Publication for fraudulent purposes, among others.

India also has an ICT policy for school education. The initiative of ICT Policy in School Education is inspired by the tremendous

potential of ICT for enhancing outreach and improving quality of education. This policy endeavors to provide guidelines to assist the States in optimizing the use of ICT in school education within a national policy framework.


It is important to know and understand the cyber security and data protection laws that exist in your country. This will guide you on how to report cybercrime as well as govern your interaction with digital technology lest you commit an offence unknowingly. Remember, ignorance is not a defense.

---

For more information, use the following links:

- Kenya Law <https://bit.ly/2G6GMyc>
- GDPR <https://gdpr-info.eu/>
- Office of the Privacy Commissioner of Canada <https://bit.ly/3hJhVYI>
- Ministry of Electronics and Information Technology <https://www.meity.gov.in/content/information-technology-act-2000>

# Module 1 Infographic




COMMONWEALTH  
of LEARNING

Teacher  
Education

TeacherFutures

Module 1

Introduction to  
Cybersecurity



CYBERSPACE?

Cyberspace is the global interconnected digital technology.

It is the virtual environment in which online communication occurs.

Made up of systems, devices, networks, applications and information.


CYBERSECURITY TRAINING  
FOR TEACHERS (CTT)

WHAT IS CYBERSECURITY?

The practice of protecting systems, devices, networks, programs and information from digital attacks.

**Main purpose:** to protect the information stored in these systems from modification and unauthorized access.


THE CIA TRIAD




**Confidentiality:** an organization's efforts to keep their data private or secret.

**Integrity:** ensuring that data has not been tampered with and, therefore, can be trusted.

**Availability:** the guarantee of reliable and timely access to information and services by authorized people.



Video conferencing  
do's and don'ts




For students

- Join classes using your real name
- Only share information related to the lesson on the chat
- Use the latest version of video conferencing solutions such as Zoom and Microsoft Teams

For teachers

- Be careful about the documents or screens you share
- Verify the student's identity to prevent intruders from joining
- Enable the 'Waiting Room'
- Don't allow students to screen share unless needed for class presentations
- If needed, remove students or parents who do not follow the classroom rules
- Disable private messages to foster transparency and easier management
- Always reiterate the security guidelines at the beginning of each class



Before selecting technology to use for online learning, ask:

- Is the online learning technology accessible?
- How easy is the technology to use?
- Is the online learning technology safe and secure for school use?

*Security is like locking your house or car – it doesn't stop the bad guys, but if it's good enough they may move on to an easier target.*

- Paul Herbka

# Module 1 Files and Resources

[/wp-content/uploads/24/2023/06/Week-1-CIA-Triad-Article.pdf](#)

[/wp-content/uploads/24/2023/06/Week-1-Cyber-Security-Laws.pdf](#)

[/wp-content/uploads/24/2023/06/Week-1-Introduction-to-Cybersecurity-Transcript.pdf](#)

[/wp-content/uploads/24/2023/06/Week-1-Online-Learning-Attacks-Case-Studies.pdf](#)

[/wp-content/uploads/24/2023/06/Week-1-Online-Learning-Platform-Write-up.pdf](#)

[/wp-content/uploads/24/2023/06/Week-1-Online-Learning-Platforms-Transcript.pdf](#)



PART II

# CYBERSECURITY THREATS AND MITIGATION





# Cybersecurity Threats, Vulnerabilities & Risks



*One or more interactive elements has been excluded from this version of the text. You can view them online here: <https://opentextbooks.colvee.org/cybersecuritytrainingteachers/?p=40#oembed-1>*

## Transcript

Hello everyone. I am Linda Mwibanda. Your instructor for week two. In week two, we are going to learn about cyber security threats and mitigation. Currently, we see that most schools have shifted their learning to online whereby teachers create their content using online platforms. They teach students using these online platforms, administer exams store their content online. As a result of these, schools have become vulnerable to cyber security attacks. For us to be able to protect ourselves against cyber security attacks on online learning platforms, it's important that we learn about the cyber security components.

We shall start by looking at three central components of cyber security. This is vulnerability, threat and risk. Although in many cases, most people use these terms interchangeably but these

times are very distinct and they each hold a different meaning. Now, what is vulnerability? Vulnerability is a known weakness in the system that can be exploited by a hacker to cause harm. What are the various examples of vulnerabilities?

First, we have outdated system or software. When your system is outdated, it will have some security issues which can be easily used by an attacker to cause harm. For instance, Microsoft Windows releases system updates periodically and these updates are used to patch up the system vulnerabilities. They have security features which patch up the system vulnerabilities that can be exploited by a hacker. Therefore, it's important that whenever an update is released, you make sure that you patch up your system according to that particular update.

Another example of vulnerability is removable media. Removable media are things like flash disks, external hard drives or CD-ROMs. How are they vulnerable or how do they cause cyber security vulnerability? You know, when you have your flash disc and you put it in a machine that is affected with a virus, you can easily copy files, those affected files and transfer it to another machine. When you're transferring those files, you are also transferring the virus.

At the end of it all, you will realize that the entire school is affected by this malicious software and that is a virus. When the machines are affected, you'll not be able to access your files because your

files will be corrupted. Therefore, it's important that you do not use this removable media to transfer your documents or your files. Another reason why we say removable media is a vulnerability is because you can easily lose this removable media. For example, you can easily lose your flash disc and once you lose your flash disk, it may end up being accessed by a person who is not authorized. Once this unauthorized person accesses your flash disk, they will copy whatever content is stored in that flash disk.

Another example of system vulnerability is weak authentication. What do I mean by weak authentication? Weak authentication is a situation whereby you have not secured your systems with proper passwords or your systems have these default password settings. For example, it has admin as the username and admin as the password. With this, the hacker can easily log in to your system and compromise your system.

The last vulnerability on online learning systems is the human being and why human beings? They always say human beings are the weakest link in any system. Why are humans the weakest link? Because naturally, human beings are susceptible to tricks. Someone can come and lie to you so that they gain access to the system or gain access to their confidential information.

Another central component of cyber security is a threat. What is a threat? A threat is something that can potentially cause harm to your system and what

are various examples of threats? First, we'll have phishing. What is phishing? Phishing is not this fishing where you go to the Lake and get fish. It is a situation where you receive an email which states that it's coming from a legitimate organization. And in most cases, these emails they tend to ask you for confidential information or for personal identifiable information. Therefore, when you just give this information without verifying the source, you might be causing a cyber-security attack.

Therefore, it's important that when you receive any email requesting you to submit any confidential information, make sure that you call the person or the organization that has sent you the email to verify whether they are authorized persons. Another example of a threat is a malware and a malware is a collective term to mean malicious software. Malicious software comprises things like viruses, we have things like ransom ware, we have things like adware, and we have things like spyware.

You may be wondering what is a virus, what is an adware and what is a spyware? A virus is software that replicates itself from the word virus. Once this virus has affected your system, it corrupts your files in such a manner that you cannot access them. What is an adware? From the word advert, you get the term adware. It's a malicious software that comes in form of an advert. Sometimes when you're accessing the internet, you see those flashy adverts maybe telling you click here and you'll win a million. That is an adware. Once you click on it, that

malicious software will embed itself on your system. What it does, it also corrupts your file.

Another type of malicious software is spyware. From the term spy, what does a spy do? A spy snips around for information. Therefore, these malicious software, these pirates, they also sniff around in your system for information. Once they get this information, they send it to the attacker and the attacker can use this information to compromise you. Therefore, it's advised that you always use antiviruses to protect yourself from these malicious software.

Let us look at the last component which is risk. What is a risk? A risk is the likelihood of a loss or damage. Therefore, when you have a vulnerability and you have a threat, when you combine the two, you get a risk. Once the vulnerability is exploited by the threat, you end up losing your documents or you end up even losing life because when people get your information, they might track you and do you harm or you may lose your credibility as a school.

When your credentials or your confidential information is exposed to the public domain, you will lose your credibility and you may end up losing even your students from registering with your school. Now this marks the end of us learning about the central components of cyber security, which were vulnerability, threat and risk. In the next session, we shall look at various cyber security attacks on online learning platforms.

# Classroom Hijacking & Security Breach



*One or more interactive elements has been excluded from this version of the text. You can view them online here: <https://opentextbooks.college.org/cybersecuritytrainingteachers/?p=42#oembed-1>*

# Ransomware & Identity Theft



One or more interactive elements has been excluded from this version of the text. You can view them online here: <https://opentextbooks.colvee.org/cybersecuritytrainingteachers/?p=44#oembed-1>

## Transcript

In this video, we shall continue learning about more cybersecurity attacks on online learning platforms. We shall start by looking at identity theft as one of the cybersecurity attacks on online learning platforms and now what is identity theft? Identity theft is a situation where an attacker uses your personal identifiable information to compromise you or compromise the system and how does it happen?

One of the ways of how identity theft occurs is through phishing. In phishing is where you get an email requiring you to submit your personal identifiable information. For example, the attacker sends you a form requesting you to fill in that form with your personal identifiable information. Once you fill in that form and send that information, you're not sending that information to the legitimate organization as the mail has said but

instead, you're sending that information to the attacker who will now get access to your personal identifiable information or your confidential credentials. Once they get that information, they will masquerade themselves to be you and compromise you or compromise the system.

Pharming is also another way of how identity theft occurs, and in pharming is why your browser is compromised by a virus or is hijacked without your knowledge. Once your browser is compromised, when you type in your school's legitimate website, it redirects you to a fake site that looks like your school's original site. In this case, the cybercriminal collects your personal identifiable information, which you might have entered on that website.

Malicious software is another way of how identity theft happens. In this case, the attacker uses malicious software like spyware and keyloggers. Spywares just like the word spy come and snoop around for information. Once they get access to this confidential information, they send it to the attacker.

Another way is keyloggers. Keyloggers monitor the activities of your keyboard. When you type in spacebar, the keylogger is able to know that this is a spacebar. When you will type in any letter on your keyboard, the keylogger is able to know that this is a specific letter or a particular letter. Once they collect that information, they will send it to the attacker who will now filter in through that information and



be able to identify your personal identifiable information and use it without your authorization.

Discarded computers or mobile devices are another weak point of how identity theft occurs and how does it happen? When your machine is spoilt or your machine is outdated and you want to dispose it, it's important that you wipe away all your personal identifiable information from that machine. If you do not do that, the attacker might easily get access to that information and use it against you.

Those are the various ways of how identity theft happens. Now how do you protect yourself against identity theft? There are various ways of how you can protect yourself against identity theft. First, build strong passwords. When you build strong passwords on your systems, it's not easy for an attacker to guess your password or to gain unauthorized access into your system.

Avoid over sharing your personal identifiable information on social media. Nowadays, you realize that most of people or most of us, we post our mobile phone numbers, our email addresses, where we come from or where we are currently staying on social media. When these attackers gain access to this information, they will be able to steal your identity and compromise you. It's important that you educate your students and your colleagues on the importance of using strong passwords and maintaining general online hygiene, whereby they

don't over share the information or they do not visit sites which are not secure.

Another way of how you can protect against security breach is establishing protocols. For instance, when I am a teacher in grade one, I should not access grade two exams or results or information because I might be tempted to compromise that information. You are also supposed to monitor access control. Whoever accesses that information should be monitored. Or for example, when you're holding a Zoom class, make use of the waiting room so that you are able to monitor who is accessing your class session. This will help you to avoid being compromised or identity theft.

So, it's of good manner if you always take good care of your personal devices, especially these mobile devices. Lastly, be careful with emails which are requesting you for personal identifiable information. When you receive such emails, always make sure that you call the organization or the person who has sent you the information, so that you're able to verify that actually it's this person who has sent you the information. Otherwise, you will end up sending your personal identifiable information to cyber security attackers.

The last type of security attack we are going to look at is ransomware, and ransomware from the word ransom is malicious software which attackers use to encrypt all your information on the system. Once they encrypt this information, they will

request you to pay a given amount of fee so that they can give you access that will decrypt this information. These threats come with short term deadlines and in case you fail to meet the first deadline, the amount of ransom keeps on rising. So, it puts you in a panic mode which will make you to pay up so that you can be given access to your information or your system.

How does ransomware attack take place? Ransomware attack happens as a result of risky online behavior. What do I mean by risky online behaviors? Naturally, we as humans we like free things. In the process of wanting free things when we are online, we end up on clicking pirated websites for entertainment or for downloading music and videos. These pirated entertainment websites are where most hackers embed their malicious software's there.

System vulnerability is another way of how ransomware attack can take place. When you have not updated your system or installed an antivirus, malicious software can easily spread through the system and compromise you. Therefore, it's advisable that you always patch your systems and install antiviruses on your systems.

The last reason that can cause a school to be compromised by a ransomware is cost. Most schools do not have a budget for cyber security. This causes you as teachers or the students to use free software from online and you know there's nothing like free. This free software are full of viruses or ransomware.

Therefore, it's important as a school to have a budget for cyber security or buy authentic software, which you can use on your system.

How do you protect yourself against ransom ware? First, train all the students or the teachers on the importance of cybersecurity. When you do that, they will understand that it's not advisable to visit websites with pirated content or they will know that when they receive an email, they will verify that this email is from a legitimate source.

Secondly, perform regular system updates. When you perform regular system updates, you will be patching up whatever system vulnerability that is on your system. When you regularly update your system, it prevents the ransomware or any other malicious software from spreading through your system.

Lastly, backup all your information then secure your back up. In case you are hit up with a ransom ware, you are able to retrieve your backed-up information and continue with your learning as normal. This brings us to the end of learning about cybersecurity attacks on online learning platforms. Some of the attacks that you have learned in these lessons are Zoom bombing, identity theft, security breach, and ransom ware. I believe that you have mastered all the ways of how you can protect yourself against these particular attacks.

# Identifying Cyber Attacks & Attack Vectors



*One or more interactive elements has been excluded from this version of the text. You can view them online here: <https://opentextbooks.colvee.org/cybersecuritytrainingteachers/?p=46#oembed-1>*

## Transcript

In the previous video we looked at various cyber security attacks on online learning platforms, and how to mitigate against those attacks. In this video, we are going to look at various cyber security attack vectors and how to identify an attack. Attack vector is a path used by a cyber security criminal, or attacker to gain unauthorized access into a system. What are examples of attack vectors? First, we have weak system login credentials. When your system login credentials are weak, it's so easy for the attacker to guess your password or your credentials and gain unauthorized access to the system. And hence compromise you or compromise the system.

Malicious insiders are another form of attack vector. And what do I mean by malicious insiders? Malicious insiders are people who work within an organization or within the school. In this case, as a

teacher, your colleague can steal your mobile device, or your removable media and gain access to confidential information. We also have misconfiguration as a vector of an attack. In misconfiguration, if you do not secure your system with proper login credentials, you can easily forget them. And now you'll be locked out of the system and you'll not be able to perform your normal functions using that system.

Ransomware is also another attack vector. Through ransomware an attacker gains access to your confidential information and encrypts it so that you're not able to access it unless you pay a given amount of fee to be given a key to access your information.

Lastly, we have phishing as an attack vector. Through phishing, the attacker is able to collect information from you, for example, personal identifiable information. And once they get this information, they'll masquerade themselves to be you. They will gain unauthorized access into the system and compromise the system. That brings us to the end of attack vectors.

Now let us move forward and see how you can identify an attack. There are various ways of identifying a cyber security attack, for instance, you will notice that the speed of your system or your computer has gone down. Once you realize that your system performance is down, it's not like the way it used to be before, that might be one of the signs of a cyber security attack.

Secondly, you will realize that your information is compromised or altered. For instance, when you have stored your records on the online learning system, let's say your students grade results and you come and realize that they have been tampered with, or they have been compromised. That's a sure sign of a cyber security attack. Sometimes when you're using your browser, you might realize that you have several addons or pop ups that come on your screen.

And these pop ups are normally from sites which you do not recognize. When you see numerous pop ups or adverts that's a sign of a cyber security attack. Sometimes your system might shut down or restart on its own. When you see your system shutting down or restarting on its own, it's another sign of a cybersecurity attack. And lastly, you might be denied access to the system or to the information in your system. For instance, in case of ransomware, you will be denied access to your records. That is another sign of a cyber security attack. This brings us to the end of this video. And in This video, we have looked at cyber security attack vectors and how to identify a cyber security attack. In the next video, you will see how a phishing attack is simulated.

# Case Studies on Online Learning Platforms Cyberattacks

## Zoombombing/classroom hijacking scenarios

1. In Massachusetts two schools have reported zoom bombing incidents. One of the schools reported that while a teacher was conducting an online class using Zoom software, an unidentified individual dialed and joined the ongoing session without authorization. This individual yelled and shouted the teacher's home address. In the second school reported that an unidentified individual joined a Zoom class session without authorization. In this incident, the individual was visible on the video camera and displayed body tattoos. Read more about this case study [here](#).
2. In San Francisco Bay Area, a school in Berkley reported a zoombombing attack. In this attack, an unknown adult male joined the session without authorization, exposed himself to teenagers, shouted obscenities and made inappropriate gestures during a virtual art class video conference before the teacher ejected him from the session. Read more about [this case](#).
3. In Kenya, Braeburn School and St Austin's Academy reported zoom bombing attacks. Both schools reported that the Zoom sessions were infiltrated by hackers who posted pornographic material that disrupted the classes. [Read more](#)



## Security breaches case studies

1. In July 2020, security researchers from WizCase discovered unprotected databases belonging to multiple e-learning platforms that were exposed online without password protection. The databases leaked students' personally identifiable information (PII) such as names, emails, passwords, ID numbers, contact numbers, addresses, birth dates, course details, and school information, of one million users. The databases were hosted on insecure servers, which allowed anyone to access it without any authentication. WizCase stated that it found five breaches from separate online educational institutions across the globe. According to WizCase, the e-learning platforms that suffered data breaches include:
  - **Escola Digital**, a Brazil-based online learning platform, suffered a data leak that exposed over 75,000 private records of students and teachers.
  - South Africa-based online learning platform **MyTopDog** lost over 800,000 students' personal records.
  - **Okoo**, a Kazakhstan-based online course portal, lost around 7,200 records that held students' personally identifiable information and administrative data.
  - The U.S.-based online education platform **Square Panda** lost around 15,000 personal records of parents and teachers. [Read more](#)
2. In April 2020, K12 Inc. an online learning platform used by more than 500 schools globally, recorded a security breach which left the personal records of 19,000 students exposed on an unsecured cloud server. [Read more](#)
3. In Kenya it was reported that a group of students from Jomo Kenyatta University of Agriculture and Technology

(JKUAT) gained unauthorized access to Moodle and changed their overall exam grades and fees. [Read more](#)

## Identity theft/masquerading

In July 2020, as millions of Chinese students were sitting for their national university entry exam, cases of how an identity theft scandal robbed hundreds of previous candidates of their dreams emerged. Officials in the eastern province of Shandong said a two-year investigation had found more than 280 people involved in stealing the identities of students sitting the *National College Entrance Examination*. The announcement prompted public outcry and Chinese lawmakers to vow a crackdown on corruption in the sector. [Read more](#)

## Ransomware

1. **Louisiana public schools:** In July 2019, Louisiana Governor declared a state of emergency after three public school districts fell victim to ransomware. A State of Emergency was re-invoked in November when another ransomware attack affected 10% of Louisiana's 5,000 network servers and more than 1,500 computers. [Read more](#)
2. **Rockville Centre School District:** On July 25, 2019, Ryuk ransomware hit Rockville Centre School District. The district's insurance carrier negotiated the ransom demand of US\$176,000 down to US\$88,000, which was covered by them. [Read more](#)
3. **Las Cruces Public Schools:** In late October 2019, a ransomware attack infected thousands of servers and devices in Las Cruces Public Schools, New Mexico. The

district disagreed to pay the ransom and instead ended up reformatting close to 30,000 devices. [Read more](#)

4. **Gadsden Independent School District (ISD).** In February 2020, for the second time in a year, the school district was compromised by ransomware. Because of the attack, the district had to shut down its entire internet and communication systems. This included phone service across all of its 24 school sites, as well as supporting locations. School officials estimated that it would take four to five days to restore their internet and phone communications, as employees worked to clean computers. [Read more](#)

# Reporting Cybercrime

When you realize that you have been compromised, for example, you have lost your data, computer, or you have been denied access to the system, report this issue to the person in charge of IT immediately. They should report it to the local field officer of national law enforcement agencies, sector specific agency, and any of the state agencies within your region.

You can also report the breach online via sector specific agency website within your nation, for example, in UK, the issue can be reported at [www.ico.org.uk](http://www.ico.org.uk). In Kenya, it can be reported at <https://www.ke-cirt.go.ke/>

When reporting the incident, give as much detail as possible and be as accurate as you can.

If the crime poses a high risk to an individual's rights and freedoms, you must inform them without delay.

# Module 2 Infographic



COMMONWEALTH  
of LEARNING

Teacher  
Education

TeacherFutures

## Module 2

## CYBERSECURITY TRAINING FOR TEACHERS (CTT)

# Cybersecurity Threats and Mitigation

**Vulnerability:** A known weakness in the system that hackers could use to cause harm

**Threat:** An incident that has the potential to harm the system

**Risk:** Likelihood of a damage or loss to occur

**A threat exploits a vulnerability in a system which leads to a risk**

### Common cyber-attacks on online learning platforms:

- Classroom hijacking
- Security breach
- Identity theft
- Ransomware



### Signs of an Attack:

- Your computer speed has slowed down significantly
- Your security software has been disabled or compromised
- Software or browser add-ons appear that you don't recognize
- Additional pop-ups are happening
- Random shutdowns and restarts are happening on your machine
- You've lost access to your account



### Attack vectors:

- Malware
- Viruses
- Web pages
- Pop-ups
- Email attachments
- Social engineering



### Important steps to protect yourself online:

- Don't open mail from untrusted sources
- Make sure your devices are up to date
- Use strong passwords
- Use two-factor authentication
- Don't click on strange-looking links
- Avoid using unsecured public Wi-Fi
- Back up your data regularly
- Be smart with personal identifiable information
- Educate students, family and friends about cybersecurity
- Avoid sharing personal information online

### Reporting Cybercrime:

- Report to the IT Administrator within less than 24 hours
- Report online via sector specific agency website within your country



**Note: Cyber threats have evolved, and so have we.**

## Module 2 Files and Resources

[/wp-content/uploads/24/2023/06/Cybersecurity-vulnerabilities-threats-and-mitigations.pptx](#)

[/wp-content/uploads/24/2023/06/Identifying-cybersecurity-attacks-and-attack-vectors.pptx](#)

[/wp-content/uploads/24/2023/06/Week-2-Cyber-Attacks-on-Online-Learning-Platforms-Identity-theft-and-Ransomware-Transcript.pdf](#)

[/wp-content/uploads/24/2023/06/Week-2-Cybersecurity-Threats-Vulnerabilities-and-Risks-Transcript.pdf](#)

[/wp-content/uploads/24/2023/06/Week-2-Cybersecurity-Threats-Vulnerabilities-and-Risks-Writeup.pdf](#)

[/wp-content/uploads/24/2023/06/Week-2-How-to-Identify-an-Attack-and-Attack-Vectors-Write\\_up.pdf](#)

[/wp-content/uploads/24/2023/06/Week-2-Identifying-Cyber-Security-Attacks-and-Attack-Vectors-Transcript.pdf](#)

[/wp-content/uploads/24/2023/06/Week-2-Security-Attacks-on-Online-Learning-Platforms-Identity-Theft-and-Ransomware-Write\\_up.pdf](#)

[/wp-content/uploads/24/2023/06/Week-2-Zoombombing-and-Security-Breach-Writeup.pdf](#)

PART III

# BEST PRACTICES





# Password Management



One or more interactive elements has been excluded from this version of the text. You can view them online here: <https://opentextbooks.colvee.org/cybersecuritytrainingteachers/?p=58#oembed-1>

## Transcript

Welcome to the third week of this training. My name is Malusi Faith and I will be your instructor throughout the week. In this video, we will look at password management and we will have a brief overview over the best password management techniques available.

### Why Do We Need Passwords?

Before we even delve into password management, why do we even need passwords in the first place? We use passwords in all facets of life. We need passwords in the form of pins, passcodes, patterns and even fingerprints in order to access private locations, private information, money and even valuable items in safes.

### Why Do We Need Passwords?

Before we even delve into password management, why do we even need passwords in

the first place? We use passwords in all facets of life. We need passwords in the form of pins, passcodes, patterns and even fingerprints in order to access private locations, private information, money and even valuable items in safes.

### **Common Threats Facing Passwords**

If we don't manage our passwords securely, they face the risk of being stolen by malicious individuals. Common threats facing our passwords include login spoofing, which is where a user is presented with the regular login prompt, which is actually a malicious program where once they enter their details, which is their user name and their password, this information is then relayed to the attacker.

Secondly, we have sniffing attack, which involves intercepting credentials or communication in order to steal credentials as they are in transit. Third, we have shoulder surfing, which involves obtaining sensitive information, such as pin numbers, ATM numbers, passwords, and other confidential data by looking over the victim's shoulder as they type it on their screen. Fourth, we have the brute-force attack, which consists of an attacker using trial and error to guess password combination with the hopes of eventually finding the correct password.

And finally, we have the data breach or password leak, which involves intentional or unintentional release of private or confidential data to an untrusted environment or to the public domain. All of these threats create an opportunity for attackers

to steal user passwords and have unlimited access to your information. This information could be sensitive and critical. It could be your student records, payroll information, financial information of your employees and so on and so forth.

### **Traditional Password Management**

Before we move on to the best practices available, what are some of the typical or traditional methods that individuals and businesses use to manage their passwords? One, we have the use of simple, repetitive, and easy to guess passwords. Two, individuals may create passwords that use identifiable pieces of information, such as their birthdays, their ID numbers, their places of birth, where they live and so on and so forth. Three, individuals and businesses often share passwords through texts, spreadsheets, post-its, sticky notes, and many other ways.

Fourth, individuals may write down passwords on sticky notes and post them on their monitors or on their desks in order to easily remember them. Fifth, individuals and businesses are prone to re-using the same passwords over and over across different or rather multiple websites. And finally, because of how often or how frequently we need passwords, individuals may forget their passwords frequently and may need to use the forgot password option in order to create their passwords all over again.

### **Best Practices**

Hackers are equipped with very advanced tools

and techniques that enable them to steal passwords and credentials. So, what best practices can we employ in order to secure our passwords? We're going to begin with password managers. A password manager is a software application that is designed to store and manage online credentials. View a password manager as a book of your passwords, lock to the master key or phrase that only you know or rather have access to. Password managers not only help you store online credentials, they can help you generate and save strong unique passwords every time you sign up to a new website.

Firefox, Chrome, Safari and Internet Explorers are all browsers that have inbuilt password managers but if you plan to use your passwords across your devices, you should probably employ the use of third-party password managers such as OnePass, Keepass and LastPass. Password managers come with both the free and the premium option, depending on the password manager, the free tier usually allows unlimited syncing across all your devices, auto-filling of your passwords and usernames and basic two factor authentication.

We will look at two factor authentication later. The paid tier offers options to encrypt online storage, safely share passwords with your coworkers or with your students and advanced two factor authentication capability. And because many of the password managers in use have encrypted synchronization across devices, you can take your password with you anywhere even on your phone.

Password managers are designed to provide you with access to all of your passwords in an encrypted format, across all your devices in a manner that is not accessible to hackers or even malicious software. Additionally, they can offer a significant convenience while providing outstanding protection and ensuring that your information stays private and safe. Another best practice is to use strong passwords. Earlier, we had looked at the brute-forcing attack. The stronger the password is the more difficult it is to crack using brute forcing software or technique.

So how exactly do we go about creating strong passwords? One, always use a password length of more than eight characters. The longer the password is, the more secure it is. Two, learn to make your passwords complex. Always include a mix of uppercase and lowercase letters, different numbers as well as different symbols. Avoid passwords that are based on repetition, common dictionary words, letters or number sequences and other easily identifiable pieces of information that may relate to you. These pieces of information include your date of birth, your place of birth, where you live, where you frequent, your best friend, your dog's name and so on and so forth. And finally, you can deliberately misspell a password. You can equally generate strong passwords without having to go through the mental gymnastics of coming up with a strong yet easy to remember password. You can one, use password managers to generate the

passwords for you every time you sign up to a new website.

Two, you can employ the use of passphrases instead of passwords. A passphrase usually involves the use of creating a phrase of many random words. Additionally, you can use sentences even with the spaces as passwords. The easier the sentence it is for you to remember, the easier and stronger it is at the same time. Finally, you can employ visual memory. This involves creating a grid of characters and choosing your passwords at random and eventually muscle memory will kick in every time you have to sign up to a new website. While using visual memory, ensure that you don't want to make it too obvious and into a keyboard safe that is easy to be cracked. For example, a very common password that employs visual memory is a use of the first line of your keyboard from Q all the way to P. While this password appears very strong, it is very easy to crack using brute-forcing software.

### **Additional Password Security Techniques**

Now that we have looked at using strong passwords as well as password managers, what other additional password management techniques exist? One, always learn to update the security questions for your accounts. For example, the answer to the question, what is your mother's maiden name is used a lot in security questions. And while this information is in the public domain, it may be used to impersonate you and eventually change your passwords. Two, set up two-factor

authentication, two-factor authentication is a second layer of security that is used to protect an account or a system. It increases the safety of online accounts by requiring two types of information from the user. You may enter your passwords but using two factor authentication after entering your password, it may require you to enter a security code or a pin number.

Three, test the strength of your passwords using online testing tools to make sure they're strong enough before you actually decide to use them. Four, use and enable biometric authentication. Biometric authentication relies on the unique biological characteristics of an individual in order to verify their identity. Biometric authentication comes in the form of fingerprint scanning, facial recognition as well as iris scanning. You can use these techniques in order to secure your devices. Always learn to separate your personal and business accounts, as well as the passwords used to access all of these accounts.

This makes it easier to spot phishing emails, as well as manage these passwords. Additionally, it compartmentalizes attack. For example, if your personal email is compromised, it is very difficult for the probability of your work email being compromised is low. Another best practice is to always avoid passwords re-use. Use one password for one account. If a password is unknowingly compromised, the window of opportunity a hacker has to use this password is very limited. Once a

hacker has access to a password that you have used across many websites and accounts, it is very easy for them to get as much information as they can from you. Finally, do not write passwords down and leave them in very obvious places such as on your desk or even on your monitor. This brings us to the end of this video. In this video, we have learned about the need of password management, and we have seen the best practices available, which include both a password manager and creating strong passwords. Next, we will look at how to identify a bad password.



# Identifying Bad Passwords

When creating passwords to either access your files, software or even your devices, it is important not to fall into the trap of creating simple passwords that you'll remember. While it is important to create passwords that are easy to remember, also be aware that a little bit of social engineering is enough to make a malicious individual easily crack your passwords. Passwords should be memorable for the user, but difficult for an attacker to guess.

To protect our devices, we should learn the pitfalls of weak passwords. Let's look at some examples of weak and strong passwords.

Weak Password	Why it is Weak
secret	Simple dictionary word
smith	Maiden name of mother
toyota	Make of a car
bob1967	Name and birthday of the user
Blueleaf23	Simple words and numbers

Other unique ones that appear strong, but are really not. If a malicious person was shoulder surfing, marking the order of how you enter your passwords with these passwords is not going to be hard.

**!@#\$\$%^&\***  
**zaq1zaq1**  
**1q2w3e4r**

To emphasize how prevalent this is, take a look at 2019's most common passwords.

**123456**  
**123456789**  
**qwerty**  
**password**

1234567  
12345678  
12345  
iloveyou  
111111  
123123

## Tools to measure the strength of passwords

Let's assume you have taken all this into consideration and you've come up with a password that's unique, employs a combination of both upper- and lower-case characters, numbers and symbols, how do you verify that your password is strong?

There are several tools that you can use to measure the strength of your password. This [website](#) tests how strong your password is and gives the results in the time period it would take to crack your password.



In this example, the password **1q2w3e4r5t** will be cracked instantly.



Other websites include [this one](#) and this [other one](#).

These tools test how easily and quickly a password brute-forcing software is able to crack your password. Password brute-forcing involves trying out all possible combinations of characters until the “correct answer” is found. This process can take a very long time, so dictionaries and lists that include common passwords like “qwerty” or “123456” are usually used.

#### *Task:*

Look up your most frequently used password on [HaveIBeenPwned](#) to see whether your password has been exposed in any data breaches.

# The Need for Software Updates, Antivirus & Backup

## Software Updates

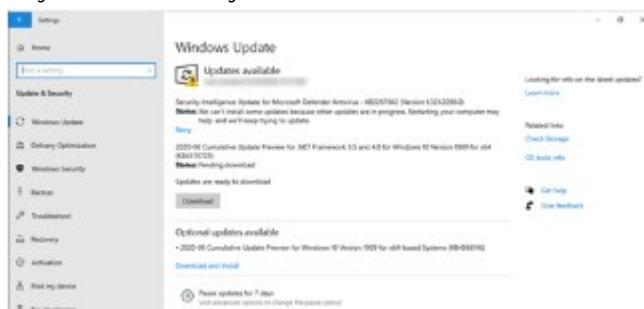
Our devices run on operating systems, software and applications that enable us to work effectively. These operating systems, software and applications are always being updated by their developers. It is important that we incorporate these updates as often as they are released. It is easy to skip software 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.



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.

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?

### Data Backup Options

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

- External drives such as pen/flash drives and hard drives and solid-state drives. 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.
- Backup services provide companies the protection they need to keep all their data secure.

## 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.

# Securing Online Communication

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

- Secure their online communication.
- Protect their personal and organizational information.
- Implement measures to secure their PII.

The world has been a global village because of the easy, quick and friction-less communication we are able to have with each other regardless of how far we are. We are constantly in communication with each other. Think of the email you sent your students regarding an assignment, of the pictures you were able to share with your loved ones over WhatsApp, of the online class you taught on Zoom, of the picture you just liked on Facebook or of the call you just made. All of this is communication over existing channels.

While all of this is amazing, how do we make sure that the communication we have over the internet is safe and secure?

These are some ways to have secure online communication:

1. **Be cognizant of the information you are sharing.** Given the nature of our society, we need to be critical of what we tell people, friendly or hostile, about ourselves. Limit with who you share very personal information and even then, make sure it is with people you trust
2. **Cultivate good password habits.** Employ the use of password managers and use strong, unique, complex and frequently rotated passwords. Use two-factor authentication or biometric authentication whenever possible. When it comes to sharing passwords especially with your co-workers or your students, do so in a safe and secure channel that is private to the involved parties. Password managers can also be utilized for sharing



passwords securely.

3. **Trust your instincts.** If something doesn't feel right, it probably isn't. If an email appears sketchy, examine it further. If someone you are talking to has shady tendencies, maybe they are sketchy. If a software you just installed is making your system react oddly, examine it further. Trust your instinct.
4. **Separate your email accounts according to purpose.** Have a personal email address and a work address. Some people go further and have email addresses for financial purposes and an email just for signing up for apps/services you want to try but aren't too sure or those which might spam you. This makes it easier to quickly recognize phishing emails. If a phishing email claiming to be from your bank gets into your work email, you immediately know it's fake.
5. **Learn to identify click bait and how to not fall prey.** Click-bait comes in all sorts of ways, not just catchy headlines. They can be in emails, on Facebook and even on messaging apps aiming to trick you into clicking links. Don't click links in emails or text messages, unless they come from a source, you're sure of. Even then, always be cautious; your trusted source might have been compromised, or the message might be a fake.
6. When sharing files with your students or co-workers, **make sure you use secure file-sharing methods.** Cloud services such as DropBox and Google Drive are good for daily use and have security features embedded. Additionally, you can put in place access control methods that define who has what rights to your files and folders e.g. only the class representative can add or delete files as required while the rest of the class can only view the contents. Always double-check permission setting on important files and run audits to see who has been accessing your files. If a file is no longer needed, delete it

completely.

7. **Use communication applications and software that have end to end encryption enabled.** End to end encryption is a secure method of communication that prevents third parties from accessing data while it's being transferred from one end device to another. Messaging apps such as WhatsApp and Signal as well as email services such as Tutanota ensure end to end encryption of messages which reinforces security when communicating.

## Social Media and Privacy

Social media is a great tool for educators. It can be used as many are on social media for personal and professional use and for the most part, it is great. Professionally, social media can enhance your network, engage you in important discussions, extend your own learning and even provide a platform for class projects. As educators, how do we ensure that in our social media use for both professional and personal use, we still maintain appropriate use and maintain security? Social media services and apps can also be used as educational tools.

### Appropriate use

Educators have responsibilities that can cause them to think twice about social media. It is important to put into consideration the following:

- What is appropriate to post?
- 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?

## Protecting your privacy on social media

The first thing before using any social media service is to understand its privacy settings. Almost all services have some control over who can see what you post. When posting, there are limits on who sees what you post but if you are worried about the nature of your post, it is best to avoid it completely.

## Interacting with students, parents and colleagues

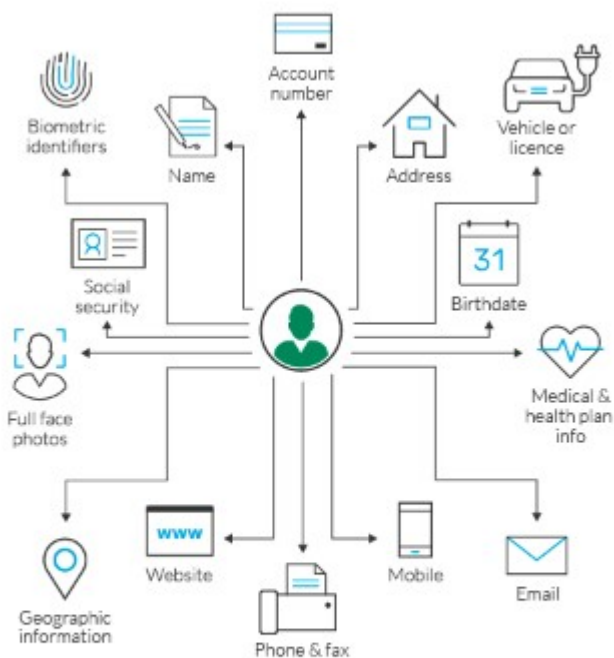
Regardless of the policies in place regarding interaction with students, it is always important to think about the post you are sending before sending them. Some teachers use social media to discuss classroom projects, class updates and share resources with students. In this scenario, it would be advisable to set up Pages or Groups that their students can join without having to 'friend' their students. When it comes to parents and colleagues, it is paramount to maintain professionalism and always be aware of your audience and only post what is appropriate.

## Teaching your students about Internet safety

Students also need to understand the importance of critical thinking while using social media. While it is very enjoyable for them and they tend to share a lot of personal information on social media, it is important as educators to inform them of the potential dangers lurking on these sites. Additionally, emphasizing kindness, critical thinking and personal responsibility when using social media and the internet in general is all it takes.

### Personally Identifiable Information

We should be very critical about the information we share with others regarding ourselves. Information that identifies you uniquely is called **Personally Identifiable Information**. This includes your name, physical home address, email address, telephone numbers, date of birth, marital status, and other information relating to your medical status, family members, employment, and education. This data can be used on its own or with other information to identify, contact or locate you in context. For example, your physical home address paired with your work address, can aid in identifying when you are home and when you may be at work.



### *What Is Considered PII?*

[Image from [imperva.com](https://imperva.com)]

PII can either be sensitive or non-sensitive. Sensitive PII identifies you uniquely and directly such as your ID number, employment number, a student's ID number, driving license, passport number and even your medical records. Non-sensitive information is easily accessible from public sources such as the internet and is not as delicate as sensitive PII. Non-sensitive information includes your gender, race, date of birth etc. Non-sensitive PII is not enough to identify an individual but combined with sensitive PII, it makes it very easy.

## Potential Dangers of Exposure of PII

PII is very critical and marketable these days. When this data is stolen either in phishing schemes or data breaches, it can provide attackers with enough information to perform identity theft which may enable them to take out huge loans in your name, file fraudulent insurance claims or perform other serious crimes. Additionally, with the amount of information that one can post about themselves online, it is easy to become a victim of stalking without even being aware of the risk.

## Securing and Safeguarding PII

1. Before you send that social media post, think first. Assess the image or the information you want to share and consider whether it is safe and 'vague' with regard to PII before sharing it especially on social media. Additionally, don't fill your social media with too much information about yourself.
2. Shred all files that have PII before discarding them. Physical documents such as bills, receipts, physical copies of your personal documents, bank statements etc. can be stolen if an individual's home is broken into. Cybercriminals will literally dump the businesses' trash in search of sensitive data because of how profitable PII is.
3. If you have access to others' PII, such as that of your students, ensure you protect and secure it using good data backup procedures, by safely destroying old media with sensitive data, employing appropriate and thorough [device security](#) measures and having accountability measures in case of mishandling of data.
4. Educate your students on the importance of online privacy. Preteens and early-teenagers are most susceptible

to oversharing especially on social media. It is important that they understand how to protect themselves online, and the detrimental consequences that could come from sharing too much personal information online.

5. Read through the privacy statements of the applications you use. It may look tedious but we tend to agree to Terms of Use without truly understanding what we are consenting to.

# Device Security

At the end of this article, 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



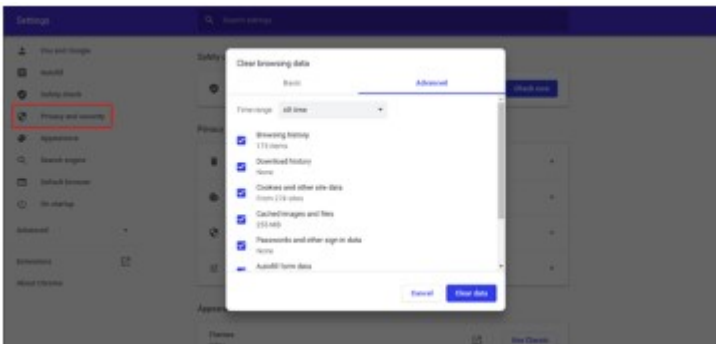
consequently secure your data and that of your students and learning institution:

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 bio-metric authentication such as facial recognition or 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.

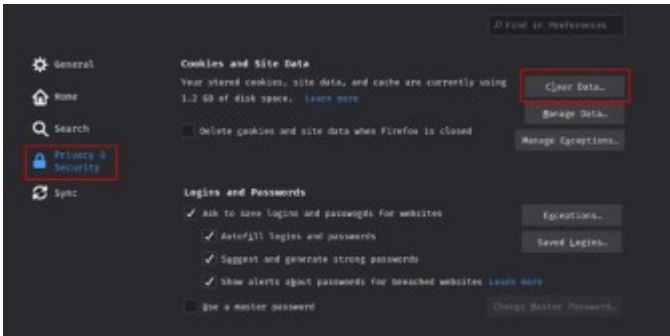
## On Chrome:

1. On your computer, open Chrome.
2. At the top right, click More .
3. Click **More tools** **Clear browsing data**.
4. At the top, choose a time range. To delete everything, select **All time**.
5. Next to “Cookies and other site data” and “Cached images and files,” check the boxes.
6. Click **Clear data**.



## On Firefox:

1. Click the menu button and select Preferences.
2. Select the Privacy & Security panel.
3. 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.

# Module 3 Infographic



COMMONWEALTH  
of LEARNING

Teacher  
Education

CYBERSECURITY TRAINING  
FOR TEACHERS (CTT)

TeacherFutures

Module 3

### PASSWORD GUIDELINES



Use password managers to store and generate passwords efficiently. Do not write passwords down and leave them in obvious places.




Employ the use of passphrases instead of passwords. Passphrases are easier to remember and harder to crack.



Avoid password re-use across websites. If a password is unknowingly compromised, the window of opportunity for the attacker to use the password is limited.




Enable two-factor authentication and biometric authentication. These methods add an extra layer of protection which decreases the probability that an attacker can impersonate a user successfully.



Separate business and personal accounts and their passwords.

### BEST PRACTICES



Be selective over the information you share online. You never know who is watching.



Have an updated antivirus that's always running.



Clear your cache and your browser history frequently.



Ensure that your operating system, software, and mobile applications are updated to the latest versions.



Always backup all your important data frequently in a safe location.

## Module 3 Files and Resources

[/wp-content/uploads/24/2023/06/Week-3-Password-Management-Transcript.pdf](#)

[/wp-content/uploads/24/2023/06/Week-3\\_-Existing-Threats-and-Enforcing-Device-Security-Article.pdf](#)

[/wp-content/uploads/24/2023/06/Week-3\\_-Identifying-A-Bad-Password.pdf](#)

[/wp-content/uploads/24/2023/06/Week-3\\_-Password-Management-Video-Writeup.pdf](#)

[/wp-content/uploads/24/2023/06/Week-3\\_-Securing-Online-Communication-and-PII-Article.pdf](#)

[/wp-content/uploads/24/2023/06/Week-3\\_-The-need-for-software-updates-antivirus-and-data-backup-article.pdf](#)

PART IV

# CYBER SAFETY FOR STUDENTS





# Student Online Protection



*One or more interactive elements has been excluded from this version of the text. You can view them online here: <https://opentextbooks.colvee.org/cybersecuritytrainingteachers/?p=81#oembed-1>*

## Transcript

Hello everyone. I'm Murrey Eddah. I'll be your instructor for this module. In this module, we'll cover on cyber safety for students. We'll begin by looking at student online protection. So what is student online protection? This is the safeguarding of students against online risks. It aims at protecting students while learning online. Students under the age of 18 are considered minors, thus are most vulnerable when it comes to the consumption of the internet.

One way of protecting students online is by monitoring their activities. The major key players in ensuring student online protection are; the students, parents, guardians, and teachers. They all have a role to play when it comes to online safety of students and their protection of their personal information. Now that you have an understanding

on student online risks, in the next topic, we'll cover online risks and indicators of an online abuse.

# Online Risks



One or more interactive elements has been excluded from this version of the text. You can view them online here: <https://opentextbooks.colvee.org/cybersecuritytrainingteachers/?p=83#oembed-1>

## Transcript

In this video, we're going to cover online risks that students face while learning online, as well as indicators of an online abuse. What is an online risk? An online risk is simply anything that can cause damage or harm a computer user while online. Risks can result to a computer being hacked or even the information being altered or stolen. Some of the most common online risk students can face are: One, exposure to inappropriate materials, such as pornography. Two, cyber bullying. Three, giving out of personal information online, such as passwords and addresses. Four, online scams. Five, cyber predators. Six, cyber-attacks through phishing or accidental malware download.

We'll now look at a research conducted by EU kids online. In this research, children from different parts of Europe were asked to mention things that made them uncomfortable while online. Some of the

responses were; strangers messaging them violence, sexual contents, and photos of them being taken without their consent. The image below shows some of the responses from the children. The pie chart on the left shows some of the risks identified by the children. The highest being pornographic content. The pie chart on the right shows, some of the platform used. The major platform being websites followed by video sites. What then are the indicators of a student facing online abuse? A student facing online abuse can exhibit the following behaviors.

One, spends most of his or her time online either by texting, social media or gaming. Two, hide who they interact with in the internet through texts, calls or even emails. And lastly shows withdrawal signs of phasing the internet. This could be through; anger, stress, anxiety, and depression. Parents, guardians, and teachers should study behaviors of students while online to identify if the student is facing any kind of online abuse. In this topic, we've covered the following: One, identification of online risks faced by the students. Two, common activities that bothered students online. And lastly, indicators of a student facing online abuse. This marks the end of this topic.

# **Incorporating Cybersecurity in the Classroom**

Cyber security is quickly becoming a much-needed skill in the world regardless how basic. Technology has become part of our lives be it schools through online learning, homes through smart appliances or transport system through self-driving cars. Online learning for students has positive impact in that students have more learning alternatives; they can learn in a comfortable environment and parents are more involved in their children's learning.

Despite such positive impact of learning online, there are a number of risks students and teachers could face during an online class such as classroom hijacking and security breach of student data. This could cause harm to an individual and institution depending on the type of attack or risk and platform being used. For example, breach of student data could expose the identity of the students and lead to identity theft and intrusion of privacy. This can damage the mental health of a child who is still growing up.

## **How then can we incorporate cyber security in the classroom?**

There are different and creative ways we can do this while conducting an online class. Children learn and understand better by observing, listening, exploring, experimenting and asking questions. Teachers should ensure that they make cyber security learning highly interactive and include visuals. This could be through videos, activities and exercises.

## Use of separate login accounts

During online learning, students should not use a shared account to login into a computer while learning. This is because having shared accounts have more risks involved. For example, out of curiosity a student could accidentally share private information from the shared computer or account belonging to their parent or guardian like birth certificate, driver's license number, bank account number, passport number and email address without knowing the effects it may cause.

## Disable or cover Webcam when not in use

Hackers have come up with more sophisticated ways of spying an individual through use of web cameras. When there is a class that does not require use of web camera students should disable or block them using web camera cover.



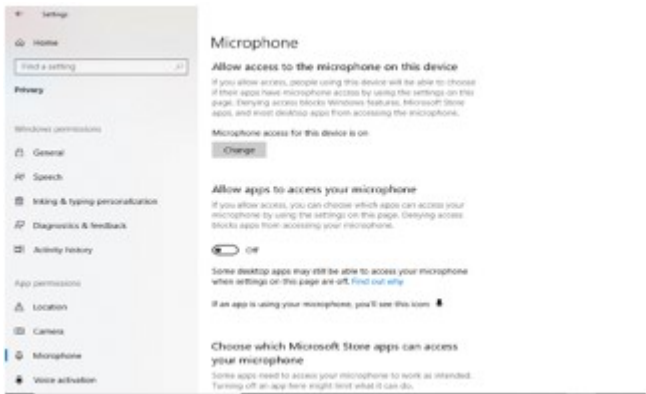
## Use of passwords and password managers

Password enables one to protect information in our devices and give access to only those with an authorized password to gain access.

Students can use password managers instead of writing down their passwords in books or papers that could be easily accessible by anyone. Password managers will enable one to generate secure passwords that cannot be reused instead of using names and date of birth. Password managers enable students to access legitimate saved links like school portal and prevent clicking on rogue links that may resemble the school portal.

## Disable microphones

Another way a hacker can spy is through microphones to eavesdrop on conversations. Students should disable their microphones when not in use to avoid hackers from listening in a private discussion.



## Use of student friendly search engine

Students should use kid friendly search engines such as kiddie, kidrex and wackysafe. These are safe search engines that allow

students to search for information, images, videos, and news that's appropriate for them.



## Identifying Personally Identifiable Information

Before starting a class, teachers can bring up with the conversation of what Personally Identifiable Information (PII), why it is important not to share this information and the risks of sharing this information. The students could participate by identifying what they think PII is and examples.

## Updating computer software

Students should ensure that their devices are up to date. They should constantly check for any available software updates and consult with their parents, guardians or teachers before doing so. Updates will enable your device to have current software and decrease the likelihood of cyber-attacks.

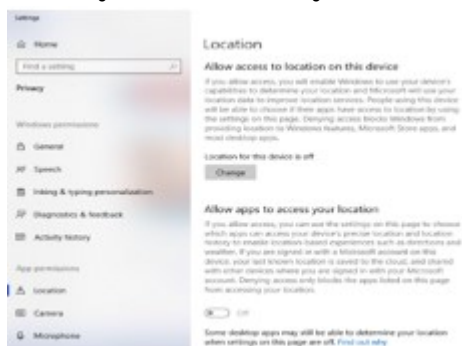


## Shut down or lock devices

Students should shut down or lock computers, laptops or tablets when not in use. These Devices should be protected using strong passwords. Devices left on when not in use are at risk of attacks and access by unauthorized persons.

## Turn off location services

Devices have a feature that can attach data such as web search and pictures to the location. In order to have anonymity, disable such features so that your movements cannot be tracked based on your online activity.



## Links and Downloads

Clicking on links and downloading content from the internet, especially if malicious, could cause harm such as stealing information like passwords, slowing down or crashing a device, etc. Students should consult with their parents, teachers and guardians before clicking on links they are not sure of or downloading content from the internet, especially, on emails.

International Telecommunication Union (ITU), a specialized agency of the United Nations that is responsible for issues that concern information and communication technologies has an [activity book](#) for students and a [guide for teachers](#) to facilitate teaching on online safety.

# Laws on Child Online Protection

As technology keeps on progressing, there is a need for blending technology in teaching and learning. One way is by students learning online using smart devices and computers. This has made learning and teaching easier especially during the Covid-19 pandemic. However, as students learn online, there are several risks they may face like cyber bullying, violent content, child pornography and cyber-attacks.

Laws are used to rule and govern how a country or state will run by protecting people and maintaining public order. Countries and states around the world have implemented laws that ensure the protection of children while online. Most of these laws are acts and we will look at different acts in countries within the different commonwealth regions including Africa, Asia, Europe, Pacific, Caribbean and Americas.

Non-Governmental organizations have also highly contributed to ensuring child online protection. For example, the International Telecommunication Union (ITU) – a United Nations agency that came up with guidelines for parents and educators on Child Online Protection. The key objective of the guidelines is to identify risks and vulnerabilities to children in cyberspace, create awareness, develop practical tools to help minimize risks and lastly share knowledge and experience.

These guidelines are for children, parents, guardians and educators, industry and policymakers and they aim at setting up a base for safer and secure internet services and technology for children.

The official guidelines for parents and educators documentation can be found on this link

The organization has also developed [a workbook for students](#) (9-12years) to teach them about their rights and safety

online by providing six scenarios which they may face while learning online. The scenarios are:

1. Right to play online
2. Managing screen time
3. Exposure to inappropriate content
4. Right to use digital media to learn
5. Privacy
6. Adult role modelling of positive use of digital media

There is also a [teacher's guide](#) that provides online safety exercises in a classroom setting with the aim of inspiring students to tackle online safety through their teachers.

Most countries in the commonwealth have collaborated with ITU with the aim of developing localized guidelines for child online protection.

## Commonwealth Regions

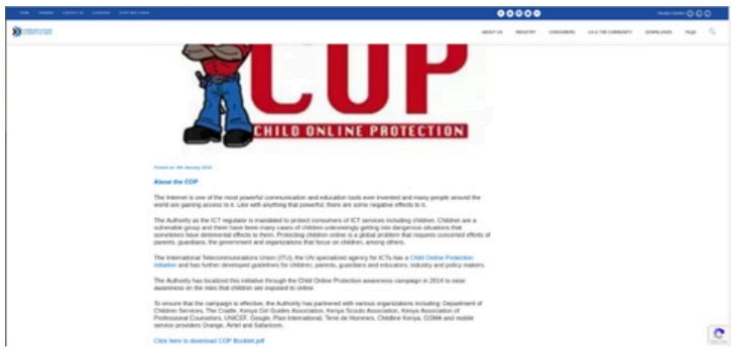
### Africa

For this region, we will look at laws and measures taken by Kenya to ensure child online protection.

**In Kenya**, the Communication Authority of Kenya, an ICT regulator under the Ministry of ICT, is responsible for ensuring child online protection. One way the authority does this is by creating awareness through campaigns on risks that children are exposed to while accessing online services like virtual learning.

The authority works closely with several local institutions like mobile service providers and the Department of Children Services to create awareness. The authority has a website that

a parent, guardian or teacher can use to report any cyber risk a student has faced while learning online.



[Image from [ca.go.ke](http://ca.go.ke)]

The Children's Act No.8 of 2000 makes provision for parental responsibility, fostering, adoption, custody, maintenance, guardianship, care and protection of children. This provision extends to protecting children while learning online.

The Data Protection Act No. 24 of 2019 says the following when it comes to protection of children's data

**33.** (1) Every data controller or data processor shall not process personal data relating to a child unless —

Processing of personal data relating to a child.

- (a) consent is given by the child's parent or guardian; and
- (b) the processing is in such a manner that protects and advances the rights and best interests of the child.

(2) A data controller or data processor shall incorporate appropriate mechanisms for age verification and consent in order to process personal data of a child.

(3) Mechanisms contemplated under sub-section (2) shall be determined on the basis of—

- (a) available technology;
- (b) volume of personal data processed;
- (c) proportion of such personal data likely to be that of a child;
- (d) possibility of harm to a child arising out of processing of personal data; and
- (e) such other factors as may be specified by the Data Commissioner.

(4) A data controller or data processor that exclusively provides counselling or child protection services to a child may not be required to obtain parental consent as set out under sub-section (1).

[Image from [kenyalaw.org](http://kenyalaw.org)]

## Asia

For this region, we will look at laws and measures present in India to ensure child online protection.

In India, the Information Technology Act 2000 Section 67 B talks about punishment for anyone who facilitates abuse of children online. He or she may be imprisoned for up to seven years and fined up to ten lakh rupees (\$13539.00).

**67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.** Whoever,—

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

25

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates abusing children online; or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

[Image from [indiacode.nic.in](http://indiacode.nic.in)]

The National Policy of ICT in Schools (2012), focuses on regulating ICT to protect students from [online risks](#). It has provisions for regulating and monitoring access to the internet.

The National Cyber Security Policy (2013), covers on the prevention, investigation, and prosecution of cybercrimes. This includes cyber-crimes against children and online students. The law enforcing agencies e.g. the police, will investigate these crimes and collate information for prosecution.

The Computer Emergency Response Team (CERT) website can be used to report cyber incidents faced by students while learning online. CERT in India conducts training to create cyber security awareness. Such training impacts teachers and parents on cyber security and ways they can protect their children online.

## Europe

For this region, we will look at laws and measures present in the United Kingdom to ensure child online protection.

In the UK, Child Exploitation and Online Protection Command (CEOP), a command of National Crime Agency, is responsible for taking national and international online child sex offenders to court. This includes persons involved in production, watching, sharing and distribution of such material. Anyone, be it a child, parent or guardian can report child online exploitation concerns like inappropriate or potentially illegal activity with or towards a child online to the CEOP safety centre.

Sexual Offences Act 2003, Protection of Children Act 1978, Criminal Justice and Immigration Act 2008, and Malicious Communications Act 1988, can be used in the court of law to support cyber related crimes against a child.

Cyber related concerns related to a student can reported on the Computer Emergency Response Team website.

## Pacific

For this region, we will look at laws and measures present in New Zealand to ensure child online protection.

In New Zealand, the Crimes Act 1961 (Section 124B) focuses on indecent communication with young people under 16 years in whatever manner (this includes through online means). This law is used to protect students against online predators who are after gullible students. It is therefore important to create cyber awareness in schools and homes to protect students from such incidents.<sup>6</sup>

The Films, Videos, and Publications Classification Act 1993 (Section 127) protects children online by posing a hefty punishment of a fine of up to \$30,000 for exhibiting an objectionable publication to a minor. A different section of the same act considers publication as age restricted if it has highly offensive language that may cause harm to persons under a



certain age. This act can be used to protect students online from sensitive adverts and videos.

The New Zealand Cyber Security Strategy aims at ensuring protection of children online through the Online Child Exploitation Across New Zealand (OCEANZ). This is a specialized police unit responsible for protecting children from online abuse.

How then can a teacher, guardian or parent report a cyber incident? CERT NZ provides a website where one can report cyber incidents. Another way is through filling forms available on the National Cyber Security Centre website and sending them through email indicated on the forms.



CYBER SECURITY INCIDENT - REPORT FORM

This form can be used to report cyber security incidents to the National Cyber Security Centre (NCSC), which is part of the Government Communications Security Bureau.

If you would like to request assistance from NCSC in relation to the incident, please use the Cyber Security Incident - Request for Assistance Form (Evaluation Services). You do not need to complete this form if you complete a Request for Assistance Form.

Send this completed Cyber Security Incident Report form to NCSC by email [incident@ncsc.govt.nz](mailto:incident@ncsc.govt.nz) or post (National Cyber Security Centre, PO Box 12-209, Wellington 6144). If the completed form contains confidential or classified information please contact NCSC to arrange an alternative method of receipt.

If you have any questions about this Cyber Security Incident Report Form, you can contact NCSC by phone on (04) 498 7654.

PART 1: YOUR CONTACT DETAILS

YOUR ORGANISATION

Organisation Name:	Click here to enter text.
Physical Address:	Click here to enter text.
Postal Address:	Click here to enter text.

CONTACT PERSON

First Name:	Click here to enter text.	Last Name:	Click here to enter text.
Job Title:	Click here to enter text.		

[Image from [ncsc.govt.nz](https://ncsc.govt.nz)]

## Caribbean & Americas

For this region we will look at laws and measures present in Canada to ensure child online protection.

In Canada, the Criminal code 1985 touches on PII in regard

to credit card and passwords, unauthorized use of computer and identity theft. This code can be used in a court of law to prosecute anyone who risks the safety of a student while studying online.

Canadian Centre for Cyber Security oversees the handling of cyber incidents. Reported incidents are also analyzed before forwarded to responsible law enforcement agencies. This includes risks students can face online such as identity theft or fraud.

Online concerns touching on online sexual exploitation of students or children can be reported using the cybertip website. This platform is operated by the Canadian Centre for Child Protection. Reports made through cybertip are analysed based on the criminal code to determine if the incident is illegal. If it is, it is forwarded to the law enforcement agency.



[Image from [cybertip.ca](https://cybertip.ca)]

## Case Study on Child Online Abuse

1. [Cyber Bullying](#)
2. [Cyber predator](#)

## Additional Reading Material

1. [Child Online Protection Act – USA](#)
2. [Data Protection Act – Kenya](#)
3. [Information Technology Act – India](#)
4. [Criminal code – Canada](#)
5. [Crimes Act – New Zealand](#)
6. [Films, Videos, and Publications Classification Act – New Zealand](#)
7. [Protection of Children Act – United Kingdom](#)
8. [Guidelines for parents and educators on Child Online Protection by ITU](#)

# Role of Students, Teachers and Parents



*One or more interactive elements has been excluded from this version of the text. You can view them online here: <https://opentextbooks.colvee.org/cybersecuritytrainingteachers/?p=98#oembed-1>*

## Transcript

Eddah: In this video, we're going to cover the roles of the teachers, students, parents, and guardians. Who then is responsible when it comes to the student's online activities? We have three main key role players. That is the students, the teachers, the parents, and the guardians. We'll begin by looking at the roles of the teachers.

Teachers should educate the students on online risks and safety. When it comes to the online risk, they should inform the students about the risks they can face when learning online. An example of an online risk is cyber bullying. A measure that a student can take to ensure that they're safe online is; blocking the web camera when not in use. Teachers should get the parents and guardians involved in the student online activities. They should inform them of the danger students can face while

online, especially without being monitored. They can further direct them to resources readily available with information on children online safety.

Another role is that, teachers should learn about organizations in charge of child online protection. These organizations provide a platform and channel that they can report cyber incidents faced by students. The teachers can also provide parents with an online guide or plan for online learning. This plan can have a comprehensive explanation on different roles and responsibilities of the students, teachers, parents, and guardians. It can also have an explanation on attendance guidelines, learning expectations, content and timing, assessment, and progress monitoring.

Lastly, it is the role of the teacher to set up rules and regulations for a virtual classroom. Just like the physical classroom, a virtual classroom should have rules to ensure that students are disciplined when learning. A school or an institution has a role to play when ensuring that students are safe online. One is by ensuring that the devices are secure.

School computers should be secured with strong passwords and locked when not in use. Software, such as antivirus and firewall should be installed to detect malicious activities that could harm their devices. Secondly, is filtering and monitoring. The school internet should be monitored and filtered to ensure students cannot access harmful or age restricted content. Downloaded content and links

accessed by the students can be tracked and blocked.

Number three is school policy. The school should have an ICT policy that protects the use of technology in the institution. The policy should guide teachers on use of school devices and student images for educational purposes only.

Number four is online personality. The school staff should be aware that anything that they post online can affect the reputation of the school. They should therefore separate their personal life from their work life and be professional.

Number five is training. An institution should train all their staff on online risks and safety. The school can further appoint an online safety coordinator to conduct this training to students, parents, and also the school staff. This should include how to report cyber incidents crimes and channels to use. Lastly, is auditing the school system. The school should ensure that there are no loopholes in the school system that an attacker may use to hack the system.

We now look at the roles of the parents and the guardians. They should learn and understand the risks that students may face online. One way to do this is to familiarize with the cases that have occurred and the effect they've had on the students. Secondly, the parents should set reasonable guides and rules when it comes to computer use. This can be the time to use the computers. This will ensure

that the students don't spend too much time on the internet and will curb internet addiction.

Number three is to install parent control software, to monitor the activities of the students. This is so that it would prevent them from accessing harmful websites and also to learn and familiarize with the online platform the students use and monitor their activities by looking through the history, to see the sites they've accessed.

The next role is to communicate freely and honestly to the children about the online risks. Parents are responsible for introducing children to online safety and inform them of the do's and the don'ts when learning online. An example is, a child should not give information about who they are or where they live to strangers online. Parents should take interest in the activities of the students while online. This will help them understand the kind of risks they're exposed to. And parents should also ensure that the students are not accessing age restricted content or websites. They should further inform the students on child friendly search engines such as Kiddle that monitors and filters content to be accessed.

Lastly, parents should attend cyber awareness training. These trainings are normally conducted by the Ministry of ICT and other relevant institutions. This will help them understand the organizations in charge of child online protection and how they can report cyber incidents.

Lastly, it's the role of students. They should report any cyber incidents that they've experienced to their parents or teachers. This will also include any uncomfortable activities they've experienced while online. Secondly, they should obey and follow rules and regulations set up by their parents and teachers while learning online. Thirdly, they should not share any personal information to strangers online. This can be their physical address or even their email addresses.

The next role is they should ensure that they don't post or send videos of themselves to strangers online. And lastly, they should ask for permission from their parents or teachers about downloading any content while online.

This marks the end of this topic. We've seen that the key main role players are the students, parents, and guardians, and the teachers. As we all know, the internet never forgets. Therefore, we should be cautious on whatever we post online. We will now look at incorporating cyber security in the classroom. Thank you.



# Module 4 Infographic



COMMONWEALTH  
of Learning

Teacher  
Education

Teacher**Futures**

## Module 4

# Cyber Safety for Students

CYBERSECURITY TRAINING  
FOR TEACHERS (CTT)

## Student Online Protection

### What is Student Online Protection?



This is the safeguarding  
of students from risks  
while learning online.

### Online risks faced by students:

- Cyber bullying
- Exposure to Inappropriate Material
- Giving out personal information online
- Online Scams
- Cyber Predators
- Cyber-attacks

### Indicators of student facing online abuse:

- Spends most of the time online
- Hides about persons they interact with online
- Shows withdrawal signs after using the internet



### Key Role Players: Teachers

- Be informed on online child risks
- Educate students on existing online risks
- Get parents involved in the safety of students
- Set rules for a virtual classroom
- Attend training on online safety and cyber awareness

### Key Role Players: PARENTS AND GUARDIANS

- Set up parental controls
- Teach children about social media etiquette
- Attend cyber and online safety awareness training
- Take interest in their children online activities
- Learn of online risks faced by children



### Key Role Players: STUDENTS



- Report any cyber incident experienced online
- Obey and follow rules put in place while learning online
- Do not give personal information to strangers online
- Do not post or send pictures and videos to strangers online
- Ask for permission before signing in into a new website

### Cyber Security in the Classroom

Students should:

- Ensure the software on their devices are up to date
- Shut down or lock devices when not in use
- Turn off location services
- Use kid friendly search engines such as kiddie
- Disable microphones when not in use
- Use strong passwords and password managers



### Laws on Child Online Protection

Some of the laws in the commonwealth countries that support child online protection:

**Kenya** - Data Protection Act 2019

**India** - Information Technology Act 2000

**United Kingdom** - Protection of Children Act 1978

**New Zealand** - Crimes Act 1961

**Canada** - Criminal code 1985

*Technology will not replace great teachers but technology in the hands of great teachers can be transformational.*

- George Couros



## Module 4 Files and Resources

[/wp-content/uploads/24/2023/06/Week-4-Incorporating-cyber-security-in-the-classroom-Article.pdf](#)

[/wp-content/uploads/24/2023/06/Week-4-Laws-on-child-online-protection-Article.pdf](#)

[/wp-content/uploads/24/2023/06/Week-4-Role-of-Students-Teachers-Parents-and-Guardians-Transcript.pdf](#)

[/wp-content/uploads/24/2023/06/Week-4-Student-Online-Protection-Transcript.pdf](#)

[/wp-content/uploads/24/2023/06/Week-4-Student-Online-Protection-Transcript.pdf](#)

[/wp-content/uploads/24/2023/06/Week-4-Student-Online-Protection-Writeup.pdf](#)

[/wp-content/uploads/24/2023/06/Week-4-Student-Online-Risks-Transcript.pdf](#)

[/wp-content/uploads/24/2023/06/Week-4-Student-Online-Risks-Writeup.pdf](#)