Advanced Cybersecurity Training for Teachers

Advanced Cybersecurity Training for Teachers

COMMONWEALTH OF LEARNING (COL)

Advanced Cybersecurity Training for Teachers by Commonwealth of Learning (COL) is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License, except where otherwise noted.

Contents

General vii

Part I. Advanced Cyber Attacks in Online Learning

Attack Vectors – Video 3
Attack Vectors 8
Wireless and Mobile Device Attacks 19
Software Application and Web Attacks 35
Internal Threats – Video 43
Internal Threats 49
Module 1 Summary Infographic 56
Module 1 Files and Resources 57

Part II. Protecting Data

Introduction to Data Security 61
Data Access Controls 67
Data Protection 72
Data Loss Prevention 78
Data Recovery 83
Module 2 Summary Infographic 87
Module 2 Files and Resources 89

Part III. Securing Online Communication and Learning Devices

Online Privacy 93
Endpoint Security 102
Understanding Encryption 109
Secure Communications 112
Module 3 Summary Infographic 120
Module 3 Files and Resources 121

Part IV. Cybersecurity Concerns in Emerging Educational Technologies

Introduction to Emerging Technologies 125
Benefits of Emerging Technologies 131
Cybersecurity Risks and Preparedness 136
Module 4 Summary Infographic 141
Module 4 Files and Resources 143

Overview of Course Content

Part 1: Advanced Cyber Attacks in Online Learning

During the first week, participants will explore

1. Attack vectors
2. Attacks targeting websites, mobile devices and commonly used computer applications devices and commonly used computer applications
3. Internal threats to learning institutions

Part 2: Protecting Data

During the second week, participants will learn

1. Access controls to protect files on devices and in the cloud devices and in the cloud
2. Techniques to prevent loss of critical data
3. Data recovery tools and techniques

Part 3: Securing Online Communication and Learning Devices

In the third week, participants will explore

1. Online anonymity and privacy
2. Secure communication channels to use when engaging with

peers and students remotely
3. Ways of protecting devices from malware and unauthorised access

Part 4: Cybersecurity Concerns in Emerging Educational Technologies

In the final week, participants will

1. Learning emerging technologies and their benefits
2. Learn cyber risks posed by the technologies
3. Develop a cybersecurity preparedness plan

Outcomes of this course

After completion of this course, the participant should be able to

- Outline the advanced cyber-attacks that may be encountered while teaching online and apply the appropriate mitigations.
- Employ various techniques to protect data created and processed by learning institutions from

alteration, loss, and unauthorised access.

- Apply advanced techniques in online communication, personal security, and device security.
- Appraise the benefits of emerging technologies in digital learning and how to use securely.

PART I

ADVANCED CYBER ATTACKS IN ONLINE LEARNING

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/advancedcybersecuritytrainingteachers/?p=19#oembed-1

Transcript

Hello participant, welcome to the first week of the ACTT course. I am your instructor, Murrey Eddah. This week will focus on advanced cyber–attacks and build–up on the knowledge you have on cyber–attacks. The first topic on this module is Attack Vectors, but before that, it is important to first understand the term, attack surface. Attack surface and attack vectors are easily mistaken to mean the same. On the contrary, they mean different. An attack surface is the number of feasible ways an attacker can exploit to get into a device or network while an attack vector is simply the method an attacker uses to compromise a device or network and gain unauthorized access for example by stealing usernames and passwords. The common types of attack vectors are; Compromised credentials, Weak and stolen

credentials, Malicious insiders, Misconfiguration, Vulnerabilities and Malware.

An attack vector can be classified as either active or passive. Active attack vector affects the integrity and availability of information whereby an attacker tries to alter or modify a system through malware, exploiting vulnerabilities or ransomware. The figure below demonstrates an active vector attack, an attacker captures the message from the sender and changes its contents before sending the misleading message to the receiver. Active attacks are in the form of; Interruption where an attacker tries to deny users from accessing the system, Modification where an attacker captures a message and alters its contents and Fabrication where an attacker inserts fake information, resources or services into the network The types of active attacks are; Masquerade, Repudiation, Replay and Denial of service.

In masquerade, the main goal is identity and data theft. An attacker impersonates a legitimate user to gain unauthorized access to network resources. The image illustrates, Darth sening a message to Alice that appears to be from Bob. Darth, who is an illegitimate user, is masquerading as Bob. Repudiation can be by the sender or receiver. A user denies having executed action or malicious transaction that caused a loss or resulted in a cyber–attack. For example, a student can use the school computer to access a malicious website causing a cyber–attack. The student then denies accessing the websites as he or she knows it is against school guidelines. In the replay, A threat actor eavesdrops on

secure network communication, intercepts it then fraudulently delays or resends it to misdirect the receiver into doing what the hacker wants. In the image, Darth who is the attacker intercepts the message from Bob to Alice and changes its contents before redirecting it to the intended receiver Alice.

Lastly in Denial of service, an attacker prevents a legitimate user from accessing network resources such as a school management system or student portal. An attacker floods the server with traffic or sends an action through code to cause a crash. In the image, Darth (attacker) interrupts Bob, who is a legitimate user from accessing services provided by the server. We will now look at the Passive attack vector. A passive attack vector is a threat to data confidentiality. An attacker strives to gain access or gather information about the target without altering the system resources, unlike an active attack vector. The figure shows how a passive attack occurs. An attacker reads the message from a sender to a receiver without modifying its contents.

The types of passive attacks are: Message Release and Traffic Analysis In Message release, an attacker monitors the contents of data in transmission. The information could be in the form of a telephonic conversation, an e–mail message or a transferred file. In traffic analysis, an attacker examines traffic coming and leaving the network without making any changes. From the information, the attacker can guess the nature of the activities and communications happening in the network. The attacker can further determine the location and identity of the host in the network.

Passive attacks are conducted using various social engineering attacks such as: Dumpster diving where an attacker goes through abandoned computers, devices or trash bins to try and acquire information from them. To prevent this, a school should always shred documents and format devices that are no longer in use. In phishing, an attacker can use SMS, e–mails or web advert to try and trick a user into giving sensitive information or visit a malicious website. The image shows an example of a phishing email. We can identify this from the sender's email that looks suspicious, redirecting link and a sense of urgency. We will look more into this in the topics to come. Baiting involves luring a user with an offer such as branded corporate branded flash disks in exchange for private information.

In piggybacking or tailgating is when an unauthorized person physically follows an authorized person into a restricted corporate area, for example, a computer class or server room. In Pretexting, an attacker tries to persuade a user into giving sensitive information by providing a fictional backstory. The image shows an example of pretext social engineering where an attacker disguises as the CEO and tries to make a financial transaction. We have learned about active and passive attack vectors at in–depth. Can you identify similarities between them?

In both, an attacker identifies a potential target, collects information about a target using social engineering, malware or phishing, gains unauthorized access to the system and steal sensitive data or install malicious code and monitors the computer or network,

steals information or use computing resources. What are the differences between active and passive attack vectors? The table shows how they differentiate. Kindly, pause the video and take a minute to study and understand the table.

A school or institution can take the following measures to protect themselves from attack vectors: Training of staff and students, Apply the Principle of Least Privilege where a user is given minimal access rights to perform the needed task. For example, a student can be granted permission to access the internet using kid–friendly search engines only, Use cybersecurity tools such as firewalls, password managers and VPNs for secure communications, Patch operating system and update device software to the latest version, Encrypt sensitive information and data at rest, in–transit and in processing, Monitor data and network access for all users and devices to unmask insider risk and Use two–factor authentication via a trusted second factor to minimize the number of breaches.

We have come to the end of this video. The next topic we will learn about Wireless and Mobile Device attacks.

Attack Vectors

Before tackling attack vectors, we must first understand the term attack surface. Attack surface and attack vectors are easily mistaken to mean the same. On the contrary, they mean different. An attack surface is the number of feasible ways an attacker can exploit to get into a device or network. What is an attack vector? An attack vector is simply the method an a tacker uses to compromise a device or network and gain unauthorized access.

Common types of attack vectors

1. Compromised credentials
2. Weak and stolen credentials
3. Malicious insiders
4. Misconfiguration
5. Vulnerabilities
6. Malware

An attack vector can be classified as either:

1. Active attack vector
2. Passive attack vector

Active attack vector

Active attack vectors affect the integrity and availability of information. An attacker tries to alter or modify a system through malware, exploiting vulnerabilities, man–in–the–middle attacks and ransomware.

In the figure below, an attacker captures the message from the sender and changes its contents before sending the misleading message to the receiver.

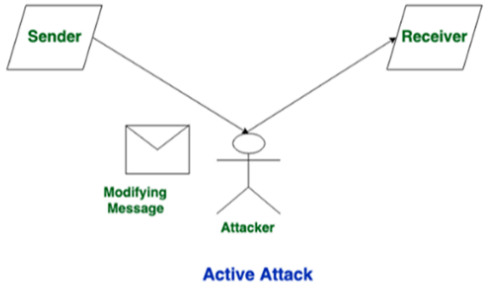


Image from: geeksforgeeks.org

Active attacks are in the form of:

1. Interruption – An attacker tries to deny users access to the system
2. Modification – An attacker captures a message and alters its contents
3. Fabrication – An attacker inserts fake information, resources or services into the network

Types of Active Attacks

Masquerade

A threat actor or attacker impersonates a legitimate user to gain unauthorized access to network resources. The main goal is identity and data theft.

In the image below, Darth is sending a message to Alice that appears to be from Bob. Darth, who is an illegitimate user, is masquerading as Bob.

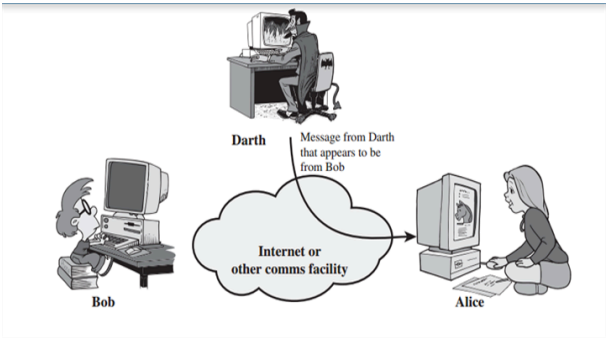


Image from: techblogmu.blogspot.com

Repudiation

A user can deny having executed a certain action or initiated a malicious transaction that caused a loss. Repudiation can be by the sender or receiver.

For example, a student can use the school computer to access a malicious website causing a cyber–attack. The student then denies accessing the websites as he or she knows it is against school guidelines.

Replay

A threat actor eavesdrops on secure network communication, intercepts it then fraudulently delays or resends it to misdirect the receiver into doing what the hacker wants. In the image below, Darth (attacker) intercepts the message from Bob (sender) to Alice and changes its contents before redirecting it to the intended receiver Alice.

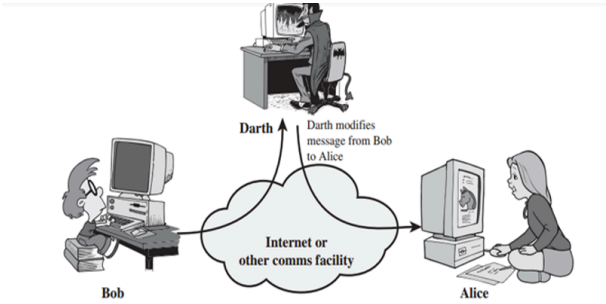


Image from: techblogmu.blogspot.com

Denial of Service

An attacker prevents a legitimate user from accessing network resources such as a school management system or student portal. An attacker floods the server with traffic or sends an action through code to cause a crash.

In the image below, Darth (attacker) interrupts Bob, who is a legitimate user from accessing services provided by the server.

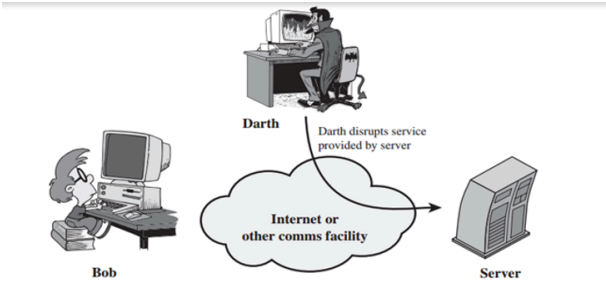


Image from: techblogmu.blogspot.com

Passive attack vector

Passive attacks are a threat to data confidentiality. An attacker strives to gain access or gather information about the target without altering the system resources.

The figure below explains how a passive attack occurs. An attacker reads the message from a sender to a receiver without modifying its contents.

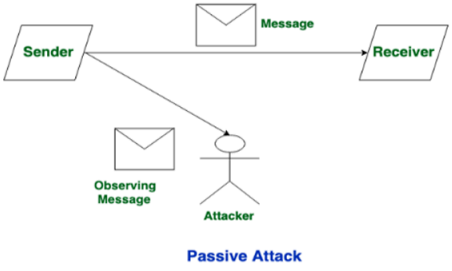


Image from: geeksforgeeks.org

Types of Passive Attacks

Message Release

An attacker monitors the contents of data in transmission. The information could be in the form of a telephonic conversation, an e–mail message or a transferred file.

Traffic Analysis

An attacker analyses traffic coming and leaving the network without making any changes. From the information, the attacker can guess the nature of the activities and communications happening in the network. The attacker can further determine the location and identity of the host in the network.

Passive attacks can be conducted through various social engineering attacks

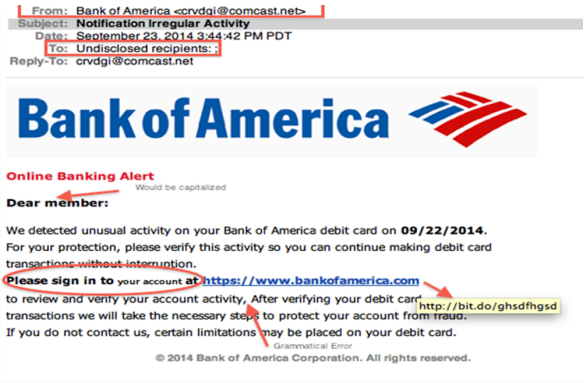
Dumpster diving

An attacker goes through abandoned computers, devices or trash bins to try and acquire information from them. To prevent this, always shred documents and format devices that are no longer in use.

Image from: sciencedirect .com

Phishing

An attacker can use SMS, e–mails or web advert to try and trick a user into giving sensitive information or visit a malicious website.



mage from: onlineowls.com

Baiting

This involves luring a user with an offer such as branded corporate branded flash disks in exchange for private information.

Image from: osu.edu

Piggybacking / Tailgating

This is when an unauthorized person physically follows an authorized person into a restricted corporate area, for example, a building or server room.

Image from: trustaira.com

Pretexting

An attacker tries to persuade a user into giving sensitive information by providing a fictional backstory. The image below shows examples of pretext social engineering.

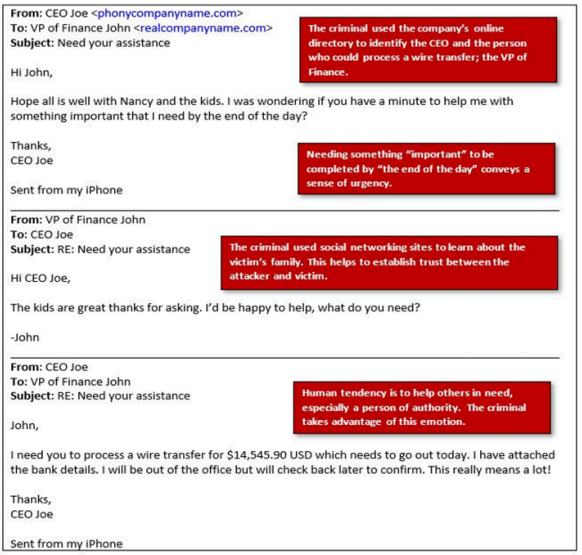


Image from: cmu.edu

Similarities between active and passive attack vectors

1. An attacker identifies a potential target
2. An attacker collects information about a target using social engineering, malware or phishing
3. Information acquired is used to identify possible attack vectors and create or use tools to exploit them
4. Attackers gain unauthorized access to the system and steal sensitive data or install malicious code
5. Attackers monitor the computer or network, steal information or use computing resources

Difference between Active and Passive attack vector

Active Attack Vector	Passive Attack Vector
A threat to the integrity and availability of the data	A threat to data confidentiality
Accomplished by gaining the physical control over the communication link to capture and insert transmission	The attacker requires to observe the transmission
Involves a modification of data	Involves the monitoring of data
The victim is aware of the attack	The victim is unaware of the attack
Affects the system and is easily detected	It does not affect the system and is not easily detected
Difficult to prevent the network from active attack	It can be prevented

Protection against attack vectors

1. Training of staff and students
2. Apply the Principle of Least Privilege where a user is given minimal access rights to perform the needed task. A student can be granted permission to access the internet using kid friendly search engines only.
3. Use cybersecurity tools such as firewalls, password managers and VPNs for secure communications
4. Patch operating system and update device software to the latest version

5. Encrypt sensitive information and data at rest, in–transit and in processing
6. Monitor data and network access for all users and devices to unmask insider risk
7. Use two–factor authentication via a trusted second factor to minimize the number of breaches

Wireless and Mobile Device Attacks

Wireless Attacks

Wireless networks have made life easier, especially during the Covid-19 pandemic, whereby schools closed, and learning and teaching from home became the new norm. However, wireless networks are susceptible to attacks that can cause great harm to a device and the user. A wireless attack is a malicious action against wireless networks or wireless system information. An example is a rogue access point.

Common Wireless Vulnerabilities

A vulnerability is a weakness that can be exploited by a hacker to compromise a device or network. Below is a list of common weakness a threat actor can take advantage of:

Default SSIDs and Passwords

SSID (Service Set IDentifier) is the name used to identify a wireless network before connecting. The image below shows Wi-Fi networks available under different SSIDs or Wi-Fi name.

Image: SSID

Wi-Fi devices such as access points and home routers come with default credentials. Depending on the brand, default credentials are the same across these devices. This makes it easy for an attacker to compromise a wireless network by logging in and taking over the router, loading malicious scripts or redirecting network traffic to a their server. An attacker can steal user information such as bank details or the identity of a user, and use it for fraudulent activities or sell it in the dark web. Default usernames and passwords must be changed immediately to prevent a hacker from accessing the wireless network.

Access Point Location

An access point should not be in a place where it is easily accessible. An attacker, in a matter of seconds, can revert the access point to default settings and set the configurations to redirect traffic to him.

Wired Equivalent Privacy (WEP) Protocol

WEP is a wireless traffic encryption protocol that has been deprecated; hence it is no longer secure. Through the use of tools, an attacker can easily crack the password or reverse the encryption

process and view information in the wireless network. A user should instead use Wi-Fi Protected Access 2 (WPA2) or Wi-Fi Protected Access 3 (WPA3) encryption protocols that are more secure.

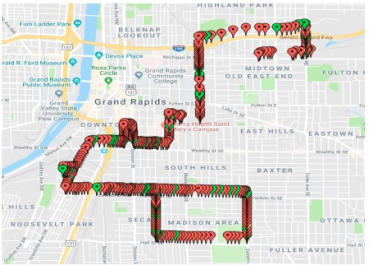
Types of Wireless Attacks

War-driving

It is also referred to as access point mapping. This is the act of looking for wireless networks by moving around a town or city using a GPS device while recording the location of wireless networks. The information is then uploaded to a website to digitally map the networks in that area.

Image: gettyimage.com

An example of War-driving mapping



mage: secjuice.com

Jamming

This can also be referred to as network interference. Its main intention is to disrupt the network. Objects such as Bluetooth headphones, microwave and walls can cause interference when a user tries to connect to Wi-Fi. An attacker can combine jamming techniques to intentionally cause network interference. A spectrum analyser will prevent jamming by boosting the signal strength of the access points. A user can also set up the router to use different frequencies, 2.5 GHz and 5 GHz.

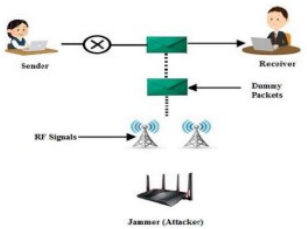


Image: ijircce.com

Rogue Access Points

A rogue access point is an unauthorized access point that an individual has set up without informing the network administrator. A wireless access point is easy to install. Using a Windows machine, a user can create a wireless network. However, these access points are not protected hence can easily be hacked or an attacker can create one to entice valid users away from their corporate network and capture the traffic.

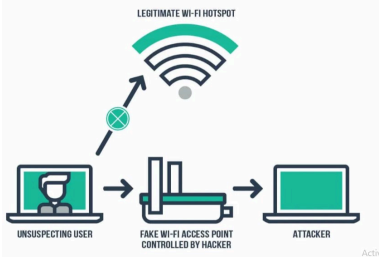


Image: medium.com

Two high school students in New Jersey, hacked into the school Wi-Fi and brought down all the network services. The attack paralyzed all online activities in the school. The staff could not access the school systems, and the students could not access their work and classes. The two students conducted the hack simply because they did not want to sit for an exam.

Videos demonstrating the dangers of connecting to insecure Wi-Fi network:

1. Hacker Demonstrates Security Risks Of Free Public Wi-Fi
2. What happens when you connect to an unsecured public Wi-Fi network?

Evil Twin Access Points

This is an illicit wireless access point that appears genuine but is set up to eavesdrop on wireless communications. An attacker can use a malicious website and steal their information and take over their computers.

Video demonstration of an evil twin access point.

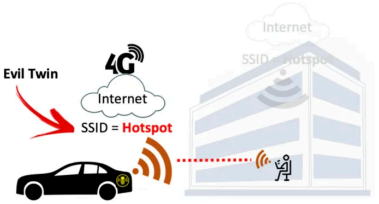


Image: darkreadings.com

Packet capturing and sniffing

An attacker captures incoming and outgoing packets in the network traffic and reads information sent between the sender and the receiver. Most information sent is in plaintext, and no form of encryption is in use. Through packet capture analysis, a threat actor can acquire sensitive information such as passwords, usernames and credit card information. There are tools used for this including Wireshark, Ettercap, BetterCAP, Tcpdump and WinDump.

Image: greycampus.com

War shipping

This comes from the term 'package shipping' which is common in online shopping websites such as eBay, Amazon or Jumia. An attacker sends a package with malicious hardware to the physical address of a target, for example, school premises or home using shipping services. The hardware is remotely accessed by the attacker and used to orchestrate an attack.

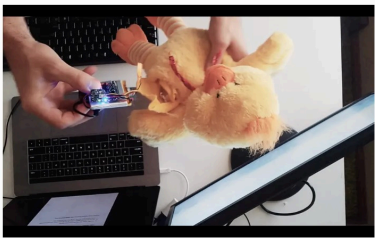


Image: forbes.com

Wireless Attacks Scenarios

1. A 12-year-old student in Baker County Middle School hacked the school's Wi-Fi because he did not want to go to school. The student shut down the school's phone lines and internet. https://www.firstcoastnews.com/article/news/education/baker-co-student-could-face-felony-forreportedly-hacking-schools-wifi-to-avoid-doing-school-work/77-046439b4-e8c8-4b95-b847-ea0d455c91a3
2. Amazon CEO Jeff Bezos' phone was allegedly hacked by a Saudi Crown Prince in 2018. https://www.businessinsider.com/jeff-bezos-phone-hacked-whatsapp-security-experts-2020-1?IR=T
3. Colleges are turning students' phones into surveillance machines, tracking the locations of hundreds of thousands. https://www.washingtonpost.com/technology/2019/12/24/colleges-are-turning-students-phonesinto-surveillance-machines-tracking-locations-hundreds-thousands/
4. Russian agents camped outside hotels to try hack victims remotely. https://www.wired.com/story/russian-spies-indictment-hotel-wi-fi-hacking/

Wireless Attacks Countermeasure

1. Users should avoid using untrusted networks especially public Wi-Fi
2. Ensure your devices have the latest software update
3. Enable a firewall or VPN to protect your information
4. Use strong and unique passwords for your network
5. Turn off the wireless home network when you are not at home
6. Disable Remote Access

Mobile Device Attacks

What do your mobile devices know about you?

Mobile devices have become an important part of our lives because they make work easier. We use mobile devices to conduct financial transactions, teach or learn online, access websites, government platforms, browse social media platforms, download private files and so on. This means that our devices know almost everything about us. For instance, if you lose you smartphone and a malicious person gets hold of it, they are able to access your passwords, social security information, files, passwords, messages, emails, addresses, location information, web history and banking information. The person can further impersonate you by stealing your identity and committing a crime.

What are mobile device attacks?

A mobile device attack is an exploit targeting handheld or portable communication devices such as a cell phone, smartwatch, Bluetooth headset, laptops and tablets.1 Most educators and learners use smartphones and laptops during online classes.

Types of mobile threats

App-based

Applications available in platforms such as play store and App-Store have made the smartphone experience better. However, it is difficult to detect a malicious app because it may look genuine on a download site. A legitimate application can also be exploited for fraudulent intentions.

Web-based

Mobile devices can connect to the internet and access web services such as banking services, school websites, staff portal and learning management systems. When a user visits a malicious site, malware can be automatically downloaded to the device without the user's knowledge.

Network-based

Mobile devices support Wi-Fi and Bluetooth technologies. An attacker can take advantage of this when a user leaves the Bluetooth enabled or connects to an unsecured Wi-Fi network and installs malware. An attacker makes use of any weakness present in an application or operating system (Windows, Android or iOS) to install harmful code.

Physical

This involves the loss of a mobile device to an attacker. Sensitive information in the phone is vulnerable as the attacker has full access to the physical device. A threat actor can also get into your institution's network using your identity and cause havoc.

Effects of a mobile device attack

An attacker can:

- Listen to actual phone calls as they happen
- Secretly read SMS texts, capture call logs and emails
- Listen to the phone surroundings
- View the device's GPS location
- Forward all email correspondence to another inbox
- Remotely control all phone functions via SMS
- Have total control of the mobile device

Types of mobile device attacks

Malware

Malicious software that targets devices such as laptops, smartphones and tablets with the aim of accessing sensitive data or taking control of the device. Examples are:

Adware

An attacker attempts to flood malicious and unwanted adverts to a user's computer or smartphone's. Adware can be used to collect data, redirect to malicious sites or change your browser's settings. The danger of adware is that data collected can be sold in the dark market and used for identity theft.

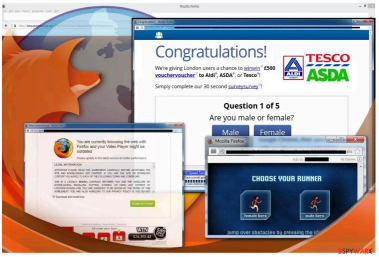


Image: Adware

Browser exploit

Mobile browsers are not completely safe. Therefore, an attacker can take advantage of its weakness and change browser settings without your knowledge. An example of an application that works in a browser and abuses this is PDF readers.

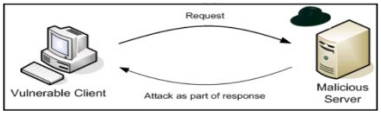


Image: Browser exploit

Trojan

It masks and presents itself as a legitimate entity. It is commonly used in SMS and applications whereby a user downloads an application thinking it is genuine only for their device to be compromised. Through SMS, an attacker sends a message to premium-rates numbers around the world using a user's device without their knowledge. The user receives a message that they have subscribed to the service. The message is tied to the hacker who is able to intercept text messages, especially those in relation to financial information.

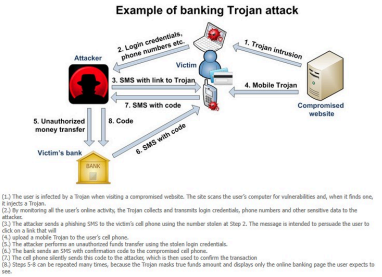


Image: Online banking Trojans

Spyware

Hackers use spyware to track the online activities of users without their knowledge or consent. It can spread easily by exploiting the weakness in a software application. It is able to acquire information through activity monitoring, collecting keystrokes (keyboard inputs) and harvesting of account information such as logins and financial data.

Image: Spyware

Phishing

A cyber-attack where an attacker tries to get information from a user by disguising as a trusted entity and tricks a user into giving sensitive information such as username and password. This can be done through an email, instant message, phone call or text message.

Clone phishing

An attacker uses a legitimate email message from a trusted source and alters it to fit his or her objective and appear like it is from the original source. He or she may add a malicious link or attachment that downloads a virus, compromising the user's device.

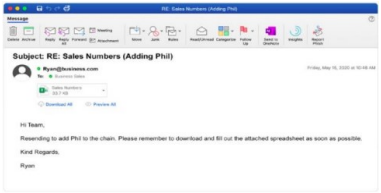


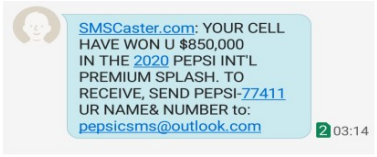
Image: webroot.com

Email phishing

An attacker sends an email that is very convincing, sometimes containing a malicious link that downloads malware into the computer of the user or redirects them to a harmful website.

SMiShing

This attack uses Short Message Services (SMS) to send malicious or fraudulent texts or links. The attacker tries to acquire information when the user clicks on the malicious link. A user can also receive a text message that looks like it is from a trusted source, for example, a bank. The attacker, however, through the convincing text message is trying to trick you into providing confidential information.



Vishing

Also known as voice phishing. An attacker attempts to trick a person into giving up sensitive information by providing a convincing fictional story. This is conducted through phone calls using mobile phones or VoIP devices.

Image: infosysblogs.com

Bluetooth Exploits

Image Blue Tooth exploits

Bluejacking

This involves sending unsolicited messages to a Bluetooth enabled device in a certain range, usually 10 meters. The messages can be either texts, images, videos or audio. The attacker can only send messages but cannot extract data from your device.

Bluebugging

An attacker takes full control of a mobile device. He or she can listen in on phone conversations, enable call forwarding, send messages, access contact list and access applications.

Bluesnarfing

An attacker uses tools to attack a mobile device, gain access and steal data using Bluetooth without the user's knowledge. Target data include International Mobile Equipment Identity (IMEI) to route a

person's incoming calls to their cell phones, bank details, calendar information or addresses.

Blue Borne

Blue Borne is an attack that gets into a device (Android, iOS, Linux or Windows) via Bluetooth and takes full control of the device. It affects computers, mobile phones, and IoT devices (smart cars and wearables). The attack does not require the targeted device to be paired to the attacker's device, or set on discoverable mode. If your Bluetooth is on and you are in the vicinity of an already infected device, then the virus will get easily transferred to your device without asking for any permission.

How to keep your mobile device secure?

1. Keep your phone locked when not in use
2. Use a secure application that encrypts communications such as Signal, WhatsApp, ChatSecure
3. Set secure protection measures for your device such as complex patterns or passwords, fingerprint, or face recognition
4. Keep your device's OS up-to-date to the latest Android or iOS
5. Connect to secure Wi-Fi networks only
6. Beware of malicious downloads or links
7. Encrypt your data using encryption tools such as ZealCrypt and Crypto
8. Install anti-virus software for your device
9. Install an advert blocking application such as Adblock Plus, Ad-Blocker and AdGuard

WhatsApp is currently the most used application for communication. Teachers around the globe use it to conduct online classes and pass information to students and their parents or guardians. You can secure your WhatsApp account through the following tips:

- Never share your registration code or two-step verification PIN with others
- Enable two-step verification and provide an email address in case you forget your PIN
- Set a device code
- Be aware of who has physical access to your phone (If someone has physical access to your phone, they can use your WhatsApp account without your permission)

How to enable two-step verification in your WhatsApp account

Image: WhatsApp two-step verification

Additional Reading Material on WhatsApp Security

1. https://www.howtogeek.com/658977/how-to-secure-your-whatsapp-account/
2. https://www.timesnownews.com/technology-science/article/whatsapp-security-features-five-tipsto-keep-your-whatsapp-chats-safe-and-secure/593244
3. https://indianexpress.com/article/technology/social/5-whatsapp-security-features-that-you-shouldenable-right-away-627796

Software Application and Web Attacks

In these attacks, a hacker takes advantage of weaknesses present in an application or website to gain access and get data.

Software Application Attack

Threat actors exploit an application installed in a laptop or phone by leveraging the vulnerabilities present. This can result in unauthorized access to privileged information such as a physical address, teacher profiles and student profiles. The following online learning platforms can be affected by a software application attack: Learning Management Systems (LMS), Student Management Systems (SMS) and video conferencing (Zoom, Microsoft Teams, Google Meets, Webex).

Common Software Application Attacks

1. *Ransomware*

A type of malware that prevents or locks out a user from accessing files, databases or applications and demands for payment mostly in the form of bitcoins. It is designed to spread across a network and target database and file servers, and can quickly cripple an entire organization.

Image: zdnet.com

2. Phishing

An attack common in emails where an attacker sends a user an email with a malicious link. Once the user clicks on the link, the threat actor is able to download malware into the computer and affect the school system. This attack can be propagated by using enterprise email clients such as Mozilla Thunderbird, Microsoft Outlook and Mail bird.

An attacker can modify their malicious email addresses inserting terms like 'principal,' 'head of department,' 'school,' and 'chairperson' to make them appear legitimate.

mage: kratikal.medium.com

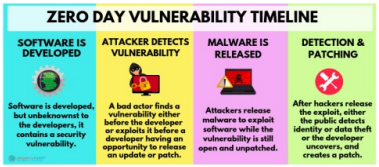
3. Brute force attack

A trial and error method used to get sensitive data. An attacker tries to gain access to a system by submitting many guessed passwords and usernames until the correct one is found. It tries to use dictionary passwords which consist of commonly used usernames and passwords.

Brute force attack

4. Zero-day attack

A cyber-attack that occurs before vendors can detect or fix the vulnerability. It's mostly used to target high profile businesses and governments. A vendor or developer can easily fail to detect it hence, very dangerous. An attacker can steal or modify your data and take unauthorized control of the computer.



phoenixnap.com

Web Attack

Humans are considered the weakest link in cybersecurity. Most

users are confident that information stored in a trusted website is safe and will be kept private. However, a threat actor can identify loopholes in the website, gain access and read the user's confidential information. A web attack can affect a school's website, student and staff portal.

Common Web Attacks

1. Watering Hole Attack

An attacker targets frequently used websites in an organization, for example, school website and install malware that infects user's devices. The attacker can gain unauthorized access and take over the network.

Video: What is a water hole attack?

2. Drive-by Download Attack

Accidental or unintentional download of malicious code onto a computer or mobile device without your consent, which exposes you to a cyber-attack. A user does not have to click on a link, press download or open a malicious email attachment to become infected.

Image: Drive-by download

3. Malvertising

An attacker inserts malicious code into a genuine online advert and affects users viewing the webpage. The main aim is to spread malware and compromise systems.

For example, in the image below, an attacker can insert malicious code into Gmail's advert and host it on a website so that whoever clicks on the advert gets infected. This can happen to a school's website.

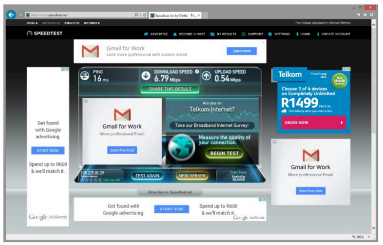


Image: Malvertise attack

4. Website Spoofing

An attacker creates a fake web site that mimics a legitimate institution's website, for example, a school portal, with the intention of tricking users and gaining trust. Users may be duped into giving sensitive information, wiring money into a fraudulent account or engaging in activities harmful to the institution.

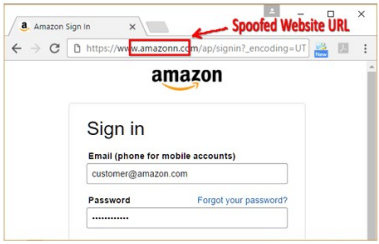


Image: Website spoofing

5. Insecure connections

Users should carefully analyze a website link before clicking on it. HTTP (Hypertext Transfer Protocol) is a protocol that enables a user to interact with a website. A website should be secured by using HTTPS (Hypertext Transfer Protocol Secure) instead of HTTP because it adds a layer of security by ensuring safe and private online communication. Kindly check if your school website is secure and if not inform the IT department.

The image below shows an example of an insecure website as it uses HTTP for communication.

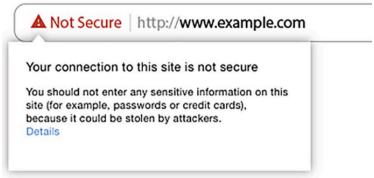


Image: Insecure connection

Case Studies

1. Zoom bombing attacks disrupt online learning

- https://www.insidehighered.com/news/2020/03/26/zoombombers-disrupt-online-classesracist-pornographic-content
- https://www.the-star.co.ke/news/2020-07-20-intruders-flood-online-classes-with-pornthreats/
- https://www.latimes.com/california/story/2020-10-10/ucla-zoom-bombing-attacks

2. Mount Kenya University Students' information leaked and posted online. The data consists of names, postal addresses and phone numbers.

- https://techtrendske.co.ke/data-of-thousands-of-mount-kenya-universitys-students-leakedonline/

3. Ethical hackers break into several universities' networks in two hours. They mostly used phishing emails to execute the attack.

- https://www.zdnet.com/article/hackers-broke-into-university-networks-in-just-two-hours/

4. A bored teen hacked into blackboard, an online learning platform used by his school and found bugs that exposed student data.

- https://www.wired.com/story/teen-hacker-school-software-blackboard-follett/

5. Learnaholic, an IT vendor in Singapore fined $60,000 after more than 47,000 personal data of students, parents and staff of various schools were hacked.

- https://www.channelnewsasia.com/news/singapore/learnaholic-it-vendor-fined-pdpc-hackschool-student-data-12160418

6. A hacker released confidential information after the school district refused to pay a ransom.

- https://edition.cnn.com/2020/09/29/us/nevada-school-district-hack-ransom/index.html

Countermeasures

- Patch and update your software applications. Companies such as Microsoft often send patches on Windows 10 when a vulnerability is discovered.
- Scan for any malware in your device using anti-malware, anti-virus or anti-spyware
- Ensure the websites you visit are secure. Do not accept anything over HTTP connections

- Use safe browsing tools provided by various antivirus vendors such as AVG Secure Browser
- Use two-factor authentication tools to prevent unauthorized access. An example is Google Authenticator used for validating a user before accessing a Gmail account.

Internal Threats

One or more interactive elements has been excluded from this version of the text. You can view them online here: https://opentextbooks.colvee.org/advancedcybersecuritytrainingteachers/?p=63#oembed-1

Transcript

Hello participant, welcome to the last topic of week one. I am your instructor, Murrey Eddah. In this video, we will learn about internal threats, how to identify them and their consequences.

An internal threat refers to the risk emerging inside a company, government agency, or institution and affects the computer system.

Internal threats can be caused by:

Employee sabotage and theft of data and/or physical equipment

- Unauthorized access by employees to secure areas and administration functions
- Weak cybersecurity measures and unsafe practices
- Accidental loss or disclosure of data
- Damage to computer equipment from fire,

flooding, power loss or terrorism

When it comes to the implementation of cybersecurity, humans are regarded as the weakest link. An insider threat is a person inside an institution who can exploit a system in a way to cause damage or

Steal data. A former, current employee or contractor with access to sensitive information or privileged accounts may be manipulated into orchestrating the damage or threat to a school. An insider threat can result in the following:

1. Financial loss
2. The ruined reputation of a school
3. Loss of trust from parents and students
4. Compromise of student and staff data
5. Disclosure of the institution's secrets
6. Laws suits from parents

The three types of insider threats in this topic are; malicious insider/turn cloak, Careless insider/ pawn/ mistake maker and mole/imposter.

A malicious insider is a person who intentionally misuses legitimate credentials or privilege access to steal information for personal or financial gain. An advantage a malicious insider has over external attackers is that they are familiar with the security guidelines and procedures present in the institution. This can be an employee, contractor or student.

A careless insider can be an employee or student who makes an honest mistake that exposes the system to an

outside threat. This mostly results from phishing emails, leaving a device unlocked or writing down credentials on a paper lying around.

A mole is an outsider who has illegally managed to gain access to an institution's or company's network.

In most cases, a mole steals credentials belonging to an authorized user.

According to a study conducted by Ponemon Institute, the highest number of insider threats are a result of mistake makers or careless insiders through phishing schemes.

The common causes of insider threats are; An employee acting on the opportunity to use data for Personal gain or steals and sells the data, Disgruntled employees stealing and leaking data online to get back at their former employer for a perceived justice and Negligence or lack of awareness from an employee which is the most common cause of insider threats.

What are the indicators of a malicious insider threat? We can identify an insider threat through digital and behavioural warning signs. The digital warning signs are:

- Downloading or accessing substantial amounts of data
- Accessing sensitive data not associated with their job function
- Accessing data that is outside of their unique behavioural profile
- Multiple requests for access to resources not

associated with their job function

- Using unauthorized storage devices (e.g. USB drives or floppy disks)
- Network searches for sensitive data
- Data hoarding, copying files from sensitive folders
- Emailing sensitive data outside the school

While the behavioural warning signs are:

Attempting to bypass security for example through tail gaiting

- Frequently in the school during off-hours
- Displaying disgruntled behaviour toward co-workers
- Violation of school guidelines
- Discussions of resigning or new opportunities

Prevention is better than cure. The best way to prevent an internal threat incident from occurring is by a school or institution taking the approach to prevent attacks causing loss, detect attacks, respond to incidents and return to a secure state.

The school can take the following measures:

1. Conduct thorough background checks on employees before hiring them
2. Use the principle of least privilege where new accounts in the organization should have the least access permissions needed to perform a task.
3. Document guidelines indicating the security procedures all students and staff should follow

4. Implement a security monitoring tool in the network to track data access and activities of all users and identify privileged users misusing their righ An example is Microsoft Network Monitor.
5. Create an insider threat detection team that monitors behavioural activities of all users
6. Educate and train students and staff on attack vectors such as phishing email and the dangers of breaching security guidelines
7. Establish physical security in the school or institution. This may involve the implementation of biometrics in the server room or IT department
8. Perform risk assessments by first identifying critical assets, possible vulnerabilities and threats that may affect them.

The following are case studies of cyber incidents that occurred in schools and prominent companies as a result of result of an insider threat,

1. The first incident, in 2018, a temporary IT worker in Chicago public schools was arrested and charged with stealing personal data of 70,000 staff, volunteers and students. The employee stole data containing personal identifiable information, criminal histories, and records of individuals associated with the Department of Children and Family services because he was fired.
2. A high school teacher in Japan, accidentally leaked private information on the school's website. The data contained students' names, health conditions and records. The teacher was

uploading a notice to address parents and guardians on an upcoming swimming class when the incident occurred.

3. Henry Park Primary School, in Singapore, accidentally sent personal data of over 1900 pupils to 1200 parents through email in an attached Microsoft Excel file. The document contained students' and parents' names, phone numbers and email addresses.

We have come to the end of week one. In week two, we will concentrate on data security. Thank you for your continued effort and participation.

Internal Threats

Humans are the weakest link when it comes to the implementation of cybersecurity. An internal threat refers to the risk emerging inside a company, government agency, or institution and affects the computer system.
Internal threats can be caused by:

- Employee sabotage and theft of data and/or physical equipment
- Unauthorized access by employees to secure areas and administration functions
- Weak cybersecurity measures and unsafe practices
- Accidental loss or disclosure of data
- Damage to computer equipment from fire, flooding, power loss or terrorism

Insider Threat

A person inside an institution who can exploit a system in a way to cause damage or steal data. A former or current employee or contractor with access to sensitive information or privileged accounts may be manipulated into orchestrating the damage or threat to a company[1].

Image: Insider threats effects

Types of insider threats

According to a study conducted by Ponemon Institute, the highest number of insider threats are a result of mistake makers or careless insiders through phishing schemes.

Image: Insider Threat Percentile

1. Malicious insider/ turn cloak

A person who intentionally misuses legitimate credentials or privilege access to steal information for personal or financial gain. An advantage a turn cloak has over external attackers is that they are familiar with the security guidelines and procedures present in the institution. This can be an employee or contractor or student.

2. Careless insider/ pawn/ mistake maker

An employee who makes an honest mistake that exposes the system to outside threat. This mostly results from phishing emails, leaving a device unlocked or writing down credentials on a sticking note.

3. A mole/ imposter

An outsider who has illegally managed to gain access to an institution's or company's network. In most cases, a mole steals credentials belonging to an authorized user.

Common Causes of Insider Threats

1. An employee acts on the opportunity to use data for personal gain or steals and sells the data
2. Disgruntled employees steal and leak data online to get back at their former employer for a perceived justice
3. Negligence or lack of awareness from an employee. This is the most common cause of insider threats

Indicators of a Malicious Insider Threat

Digital Warning Signs

- Downloading or accessing substantial amounts of data
- Accessing sensitive data not associated with their job function
- Accessing data that is outside of their unique behavioural profile
- Multiple requests for access to resources not associated with their job function
- Using unauthorized storage devices (e.g. USB drives or floppy disks)
- Network searches for sensitive data
- Data hoarding, copying files from sensitive folders
- Emailing sensitive data outside the school

Behavioural Warning Signs

- Attempts to bypass security
- Frequently in the school during off-hours
- Displays disgruntled behaviour toward co-workers
- Violation of school guidelines
- Discussions of resigning or new opportunities

Fighting Internal Threats

Prevention is better than cure. The best way to prevent an internal threat incident from occurring is by a school or institution taking the approach to deter attacks causing loss, detect attacks, respond to incidents and return to a secure state.

The school can take the following measures:

1. Conduct thorough background checks on employees before hiring them
2. Use the principle of least privilege. New accounts in the organization should have the least access permissions needed to perform a task.

3. Document guidelines indicating the security procedures all students and staff should follow
4. Implement a security monitoring tool in the network to track data access and activities of all users and identify privileged users misusing their rights. An example is Microsoft Network Monitor
5. Create an insider threat detection team that monitors behavioural activities of all users
6. Educate and train students and staff on attack vectors such as phishing email and the dangers of breaching security guidelines
7. Establish physical security in the school or institution. This could involve the implementation of biometrics in the server room or IT department
8. Perform risk assessments by first identifying critical assets, possible vulnerabilities and threats that may affect them

Insider Threat Examples

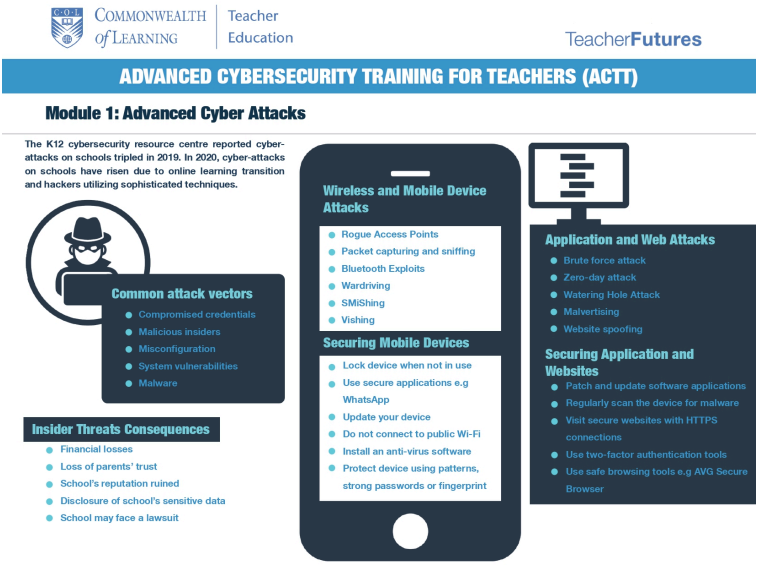
1. In 2018, a temporary IT worker in Chicago public schools was arrested and charged with stealing personal data of 70,000 staff, volunteers, students and others. The employee stole data containing names, employee ID numbers, phone numbers, addresses, birth dates, criminal histories, and records of individuals associated with the Department of Children and Family services because he was fired.https://www.cbsnews.com/chicago/news/cps-data-breach-fired-employee-kristi-sims-charged-stolen-database-personal-information-identity-theft/

2. A high school teacher in Kobe accidentally leaked private information on the school's website. The data contained students' names, health conditions and records. The teacher was uploading a notice to address parents and guardians on an upcoming swimming class when the incident occurred.https://japantoday.com/category/national/teacher-accidentally-leaks-names-health-records-of-students-on-school-website
3. In a period of two years, from 2012 to 2014, a computer contractor for Korea Credit Bureaus copied sensitive data (customer names, phone numbers, social security numbers, credit card numbers and expiration dates) on a USB stick and sold it to marketing firms. Over 20 million records were stolen and sold. https://www.bbc.com/news/technology-25808189
4. Microsoft Corporation database leak discovered in 2019 by a research company. The leak was as a result of employee negligence and affected over 250 million customers. The database servers containing the records spanning from 2005 through December 2019, were insecure and anyone could access them through a web browser. https://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online/?sh=1f121dd4d1b3
5. Henry Park Primary School accidentally sent personal data of over 1900 pupils to 1200 parents through email in an attached Microsoft Excel file. The document contained students' names and birth certificate numbers, parents' names, phone numbers and email addresses. https://www.asiaone.com/singapore/details-more-1900-pupils-henry-park-primary-school-leaked

---

1. https://www.knowitallninja.com/lessons/how-internal-threats-occur/#:~:text=An%20internal%20threat%20refers%20to,which%20can%20easily%20be%20abused

Module 1 Summary Infographic



Module 1 Files and Resources

/wp-content/uploads/23/2023/06/Activity-1B-Blocking-Websites-on-a-Personal-Computer-Using-Linux.pdf

/wp-content/uploads/23/2023/06/Activity-1B-Blocking-Websites-on-a-Personal-Computer-Using-MacOS.pdf

/wp-content/uploads/23/2023/06/Activity-1A-Identifying-Phishing-Emails.pdf

/wp-content/uploads/23/2023/06/Activity-1B-Blocking-Websites-on-a-Personal-Computer-Using-Windows-Firewall.pdf

/wp-content/uploads/23/2023/06/Week-1-Advanced-Cyber-Attacks-Resources-.pdf

/wp-content/uploads/23/2023/06/Week-1-Attack-Vector-Transcript.pdf

/wp-content/uploads/23/2023/06/Week-1-Attack-Vectors-Writeup-1.pdf

/wp-content/uploads/23/2023/06/Week-1-Internal-Threats-Transcript.pdf

/wp-content/uploads/23/2023/06/Week-1-Internal-Threats-Writeup.pdf

/wp-content/uploads/23/2023/06/Week-1-Software-Application-and-Web-Attacks-Article-1.pdf

/wp-content/uploads/23/2023/06/Week-1-Wireless-and-Mobile-Device-Attacks-Article-1.pdf

PART II

PROTECTING DATA

Introduction to Data Security

One or more interactive elements has been excluded from this version of the text. You can view them online here: https://opentextbooks.colvee.org/advancedcybersecuritytrainingteachers/?p=76#oembed-1

Transcript

Hello and welcome to the second week of the Advanced Cybersecurity Training for Teachers course. My name is Patricia Musomba and I will be your instructor this week.

During this week, we will explore data security and various techniques used to protect data created and processed by learning institutions from alteration, loss and unauthorized access. This module will provide you with the necessary skills and techniques to protect important and critical data such as the curriculum, student data and assessments.

With continuous integration of technology in educational institutions, data security and data management have become more important.

Data security is a set of standards and processes used to protect data against intentional or accidental

destruction, modification or disclosure. Its main aim is to protect all the data that an organization creates, collects, stores, receives or transmits. Learning institutions create, collect and store data that is very critical. Primarily, any unauthorized access to this data could lead to a data breach and result in financial losses and damage of brand image. It is thus important for teachers and teacher educators to learn about data security.

Now, let us look at some of the data processed by learning institutions.

Learning institutions are data driven. They utilize data collected to make informed decisions about delivery of quality education, service delivery, resource allocation and fulfilling their mandate to key stakeholders such as parents, students and education ministries. Some of the critical data created, collected and processed by learning institutions includes:

1. Financial data including fee payments, payroll information
2. Employee information such as employment history, residential addresses, contact information, health information
3. Student records including performance grades, health information, parent information, behavioral reports
4. Intellectual property such as training materials, courses, tests, booklets

It is the responsibility of the learning institutions and every personnel that handles the data in any manner to

protect and preserve the confidentiality and integrity of the data during its entire life cycle. The data lifecycle includes ordered steps from data acquisition to destruction of data. As shown, data is first created or collected. For example, in learning institutions, data creation could involve filled student application forms or parents providing copies of identification documents such as National IDs or driving license. Data is then processed and analyzed. This could be analysis of student performance to draw insights and conclusions. Data is then preserved through the use of various techniques to maintain its integrity and confidentiality. This data may need to be accessed from time to time by authorized parties.

To apply proper data protection controls, an understanding of the three data states is required. The three data states ensure that data is protected throughout its lifecycle.

Data at rest refers to data not being accessed and is stored on a physical or logical medium.

Examples of data at rest include:

1. Files such as curriculum and examination documents stored in a file server
2. Student records in databases
3. Documents in a flash disk
4. Video training content stored in a hard drive/disk

How can data at rest be protected?

Data at rest can be protected using the following techniques:

1. **Encryption**: This is a technique that scrambles or encodes data in a way that only authorized personnel with a particular key can access and unscramble it. If unauthorized personnel access the data, it will be unintelligible to them because they do not have a special key to decrypt the data. Encryption can thus be applied to data storage such as databases, flash disks and hard drives. If a device such as a laptop is lost but encryption has been enabled, the data stored in the laptop will be protected. There are various free tools that can be used to encrypt our devices such as Vera Crypt and Bit locker. These two tools will be discussed later.
2. Another technique is **Multi-factor authentication**: To access data stored in the cloud, multi-factor authentication should be enabled. For example, when accessing your Google Drive, you should authenticate yourself with a password and a code sent to your mobile phone. This adds another layer of security. If an attacker tries to access the drive, they will need the code. Multi factor authentication can also help you detect unauthorized access. If you did not initiate the connection, then receiving a code would translate to an attempted unauthorized access.

The second data state is Data in transit is also

referred to data in motion or data in flight. This is data that is transmitted or travels through an email, web or collaborative work applications. Here are some examples of data in transit:

- Email communication using clients such as Gmail and Microsoft Outlook
- Instant messaging communication using WhatsApp, Telegram
- Team collaboration using Microsoft Teams, Slack
- And downloading and uploading files on the internet

Data in transit can be protected by:

1. Using secure communication channels. Most secure communication channels have encryption enabled, hence if and when the data is intercepted while in transmission, the unauthorized personnel will not be able to read it.
2. It can also be protected using secure websites to access data on the internet. Secure sites usually have a padlock at the beginning of the URL as shown.

The last data state is data in use. This is data that is being consumed or accessed by a user. When data is opened by one or more applications, it is considered to be in use.

Examples of data in use include:

- Requesting for access into a learning

management system such as Moodle or Google Classroom

- Another example is accessing fee payment transaction history

Data in use is protected through:

1. Tracking and monitoring who is accessing any critical information. This is why users have accounts used to log into any critical systems such as the student information system or the learning management system.
2. It can also be protected by implementing data access controls to govern what each user can do to the data. For example, students can request access to view their performance grades but cannot modify them.
3. Lastly, tracking and monitoring any changes or modification to data can be used to protect data in use. If any unauthorized changes are made, a previous version of the data can be restored and the perpetrator can be identified.

We have now come to the end of the first topic. In this video, we learned about data security, and the three data states. Next, we are going to look at data access controls.

Data Access Controls

One or more interactive elements has been excluded from this version of the text. You can view them online here: https://opentextbooks.colvee.org/advancedcybersecuritytrainingteachers/?p=78#oembed-1

Transcript

Hello, my name is Patricia Musomba and welcome to this video. In this topic, we will learn about data access controls.

Access control is a key component of data security. Access controls authenticate and authorize individuals to access the information they are allowed to see and use. Data access controls should be based on the following questions:

1. Who is allowed to view/access this data?
2. Who is allowed to modify the data?
3. Under what circumstances do you deny access to a user with access privileges?

The foundation of data security is Authentication and authorization. Authentication is a way of identifying users to make sure they are who they claim to be, while authorization is the process of establishing a user's rights or privileges. Authorization usually happens after

authentication. The most common means of authentication is by the use of a password and username. For example, in a school, a teacher authenticates themselves or logs into the learning management system using a username and password. After successful authentication, the teacher is given access to the system and can perform various tasks in the system such as creation of course, uploading course materials or updating course content. This is authorization that is what the teacher is allowed to do within the system.

Authentication is achieved through the use of passwords or through biometrics.

Passwords: Passwords are used to prove that an account belongs to you. For all school systems such as learning management systems and student management systems, strong passwords should be used to log in. Strong passwords cannot be compromised easily by attackers. Strong passwords are more than eight characters long, alphanumerical and have special characters. The use of passphrases is encouraged because they are easier to remember. Another recommendation is to enable Two Factor Authentication where more than one authentication factor is used for verification. For example, once a user provides their username and password, for successful login, they also have to provide a code that is usually sent to their mobile phone or email address. This adds another layer of security.

Biometrics: Biometric authentication is a security process that relies on the unique biological

characteristics of an individual. This can be implemented through facial recognition, fingerprint scanners, eye scanners or voice recognition.

How can a school implement data access control?

Schools store data both physically and digitally. For protection of physical data such as physical student records, physical security must be enforced. Physical security can be implemented using:

- Visitor management systems
- Badge systems to identify personnel
- Biometric devices to gain access into the premises
- Video surveillance for example through CCTV
- Fences and gates
- Locks
- Security guards
- Motion detectors

To protect digital data, schools can implement logical access controls. Logical access controls are used to restrict access to services and information based on a criterion determined by the administrators. The role of the user is one of the most common criteria used to implement access controls. Role-based access controls provides a user with access to the resources that enable them to perform their duties satisfactorily. For example, the role of a teacher determines what data they need access to. Data access controls are mostly implemented using permissions.

Permissions are the various access rights assigned to

different users and groups of users. In an organization, groups can be based on the role of the user. For example, in learning institutions, the following groups exist; teachers, students, suppliers, and support staff. The different groups will have different levels of access in the organization's network.

When sharing files and documents, it is important to specify the level of access the user has. A user or a group can have the following permissions:

View/Read-only: When this is enabled, the user can only read or view the file, without making any modifications. They can also copy the contents of the file. This type of permission is useful when sharing files that individuals are not allowed to change. For example, when sharing educational notes with students, share them with read-only rights enabled. To enable this on a file, right-click on a file, select 'Properties' and tick 'Read-Only'. Click on 'Apply' to effect the changes as shown.

- Another type of permissions is Edit or Write: Users with this level of permission can edit, rename, and move files. This type of file permission is used during collaboration because colleagues can edit or modify the file to add new information or provide feedback. Files without the Read-Only property selected can be edited by others.
- Lastly, we have Execute: This is a permission used mostly with applications. Users with this permission can run a specific program or type of

program file. In most organizations, users are restricted from running applications. This is a security measure to prevent them from running potentially harmful software that could have catastrophic effects in the institution's network.

These permissions also apply when sharing documents on the cloud. Sometimes when collaboration is needed between colleagues, cloud drives can be used to facilitate this. Cloud drives offer additional storage from a cloud provider. These include Google Drive, OneDrive, iCloud and Drop Box. For example, when sharing documents on Google Drive, one can specify the rights each person has to the document. There are two types of permissions, that is Editor and Viewer.

These permissions will allow the owner of a file on the cloud to control what other people can do to the document. This protects against unauthorized access and or modification.

We have come to the end of this video. We learned about data access controls such as the use of passwords, multifactor authentication and permissions. Next, we will explore various data protection techniques.

Data Protection

Figure 1: Data Protection

Data protection is the process of safeguarding important information from corruption, compromise or loss. It is approximated that each person in the world generates 1.7 MB of data every second. This data is a goldmine for hackers and thus needs to be protected as they can use it to perpetrate attacks or steal identities. Data protection employs various techniques to safeguard the confidentiality, integrity and availability of data. Due to large volumes of data, it is vital to classify data according to its sensitivity as this will determine the levels of security applied to each class of data. One of the most commonly used data protection techniques is encryption.

Encryption

Encryption is a technique that allows information to be hidden

so that it cannot be read without special knowledge, such as a password or a secret key. Encryption uses a secret key to change data into an unreadable or unintelligible format. The scrambled information is said to be encrypted and is known as ciphertext. Decryption is a way to convert encrypted data into a readable format or plaintext. Data that is stored or in transit should be encrypted to protect it from unauthorized access and modification, hence preserving its confidentiality and integrity. The figure below shows the encryption and decryption process. The user is sending confidential information about the password to a system. The message which is 'Your password is unitedkingdom' is encrypted into an unreadable format. A key is then used to convert the ciphertext into readable format once the data reaches its destination. Note that the password used in this example is weak and should not be used.

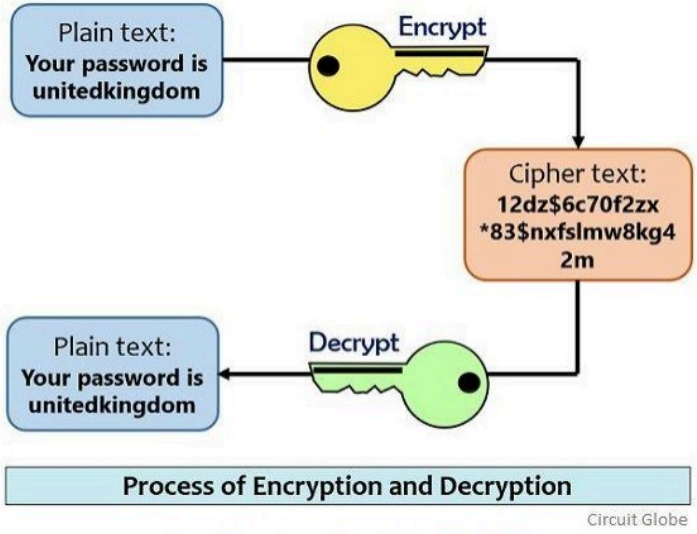


Figure 2 Encryption and Decryption from Circuit Globe

Circuit Globe

There are two popular solutions used to perform full drive/volume encryption; BitLocker and VeraCrypt.

BitLocker

BitLocker is a Microsoft proprietary encryption solution that is included with Microsoft Windows versions starting with Windows Vista. It protects the data on your device so it can only be accessed by people who have authorization. To turn BitLocker on, follow these steps:

1. In the search box on the taskbar, type Manage BitLocker and then select it from the list of results as shown in Figure 3

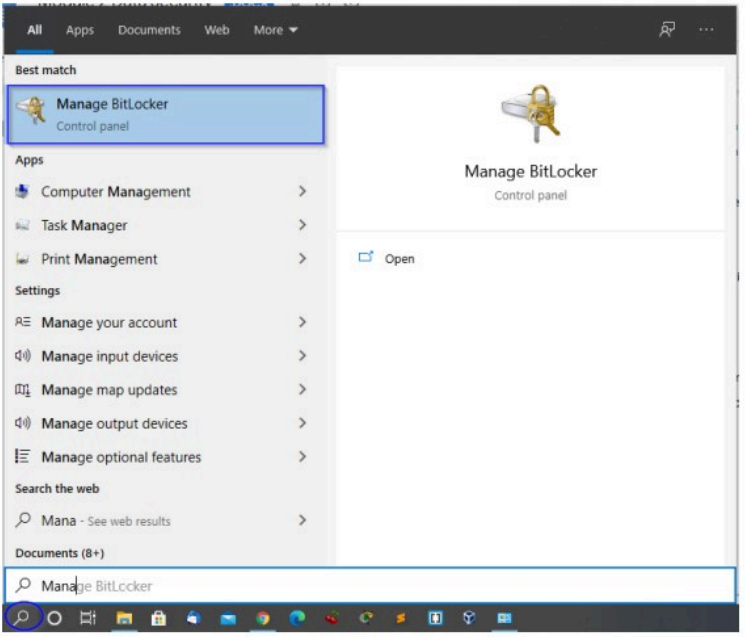


Figure 3 BitLocker

2. Click Turn on BitLocker then follow the instructions as shown in the figure below.

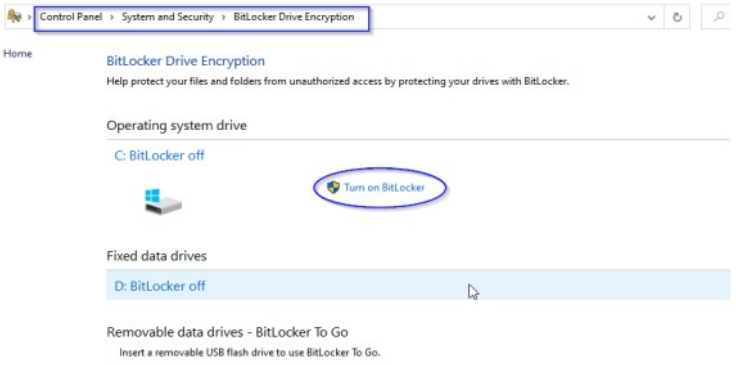


Figure 4 BitLocker Instructions

BitLocker also offers encryption of external drives such as USB drives. This solution is known as BitLocker To Go, and it protects the data stored in these external drives against tampering or unauthorized access. In case the drive is lost, the data will remain intact as someone would require the password used for encryption. This option is viable when sharing sensitive data with colleagues using external drives. To use this capability:

1. Insert the USB drive or external drive to encrypt
2. Search for Manage BitLocker using the search box on the taskbar
3. Select BitLocker To Go and follow instructions. You'll be prompted for your unlock method—for example, a password—when you connect the drive to your computer. If someone doesn't have the unlock method, they can't access the files on the drive.
4. Back up the recovery key: After setting up BitLocker, it is crucial that the recovery key be backed up in case one forgets the password. This key can be backed up on an external drive

such as USB drives. Avoid backing up the key to the cloud as cloud drives can be compromised.

VeraCrypt

VeraCrypt is a more sophisticated and robust encryption solution that enables full volume encryption, creation of hidden drives/ folders and encryption of specific folders or files. Due to its robustness, VeraCrypt is recommended more than BitLocker. However, these two tools can be used together, BitLocker for full disk encryption at the push of a button, and VeraCrypt for specific folder encryption. To learn how to set up VeraCrypt, watch the video available at the link below.

VeraCrypt Getting Started

Other than encryption, here are other guidelines and techniques that can be used to protect data:

1. Back up sensitive data: Creating duplicates of files can ensure that if the device is lost, stolen, or compromised, you don't also lose your important information. Backups can be created on the cloud. However, ensure the cloud service is secure.
2. Remote location and device wiping: If your mobile phone or laptop has this feature, enable it. In case the device is lost or stolen, you can track it and delete all your information to prevent it from landing on the wrong hands.
3. Lock your devices using passwords, PINs or fingerprint to prevent unauthorized access.
4. Factory reset your devices before donating or reselling. This prevents the accidental leaking of data.
5. Sharing personal data: Be overly cautious when sharing personal information, especially over the internet. Sharing too much information could make you a target for malicious attacks.

6. Shred: Any old documents should be discarded through shredding. This prevents leaking of any personal information.
7. Whenever possible, enable two-factor authentication. This will prevent access to email accounts and social media sites that have a sea of information about you.
8. Avoid sharing any sensitive data over public WiFi as this data can be easily hijacked by attackers. For example, do not enter any credit card information on a website while using public WiFi.
9. Always sign out from your accounts when using shared devices. This prevents other people from accessing data stored in your accounts.
10. Separate personal data and work/professional data. Store this data separately. This will limit the extent of access an unauthorized person has in case you are compromised.
11. Store most sensitive data locally. It is important to backup data in the cloud. However, your most sensitive data is most safe when stored in the devices you own. You can back up this data on encrypted external drives.

Data Loss Prevention

Data loss prevention is increasingly taking centre stage in data security due to vast amounts of data created, generated and collected by institutions. Most decisions made in organizations are data-driven; therefore, data is the 21st century oil and must be protected from loss through digital attacks and data breaches. Data loss prevention (DLP) is a set of tools and processes used to ensure that sensitive data is not lost or misused. Its primary aim is to prevent end-users from accidentally or maliciously sharing data that could put them or their organizations at risk. For learning institutions, DLP is used to comply with various laws on the protection of student data. DLP protects data such as personally identifiable information, intellectual property such as training content and other educational content, and student information such as contact information, health information. Learning institutions must also protect their financial data such as fee payments, grants received from governments and payroll information.

In summary, organizations and individuals use DLP to:

- Protect Personally Identifiable Information (PII) and comply with relevant regulations
- Protect Intellectual Property critical for the organization and for the individual
- Secure data on remote cloud systems

Some causes of data loss include:

- Insider threats: An insider such as an employee who abuses their right of access to move data outside the organization
- Digital attackers: Malicious attackers target sensitive data to sell it, tarnish an organization's brand image, or blackmail.
- Negligent exposure: People with access to the data can

accidentally share confidential information

- Missing devices: Stolen or missing devices that store confidential data. Missing devices contribute to 42% of data breaches globally, as shown in Figure 1.
- Accidental deletion of data
- Corruption of files due to operating system errors.

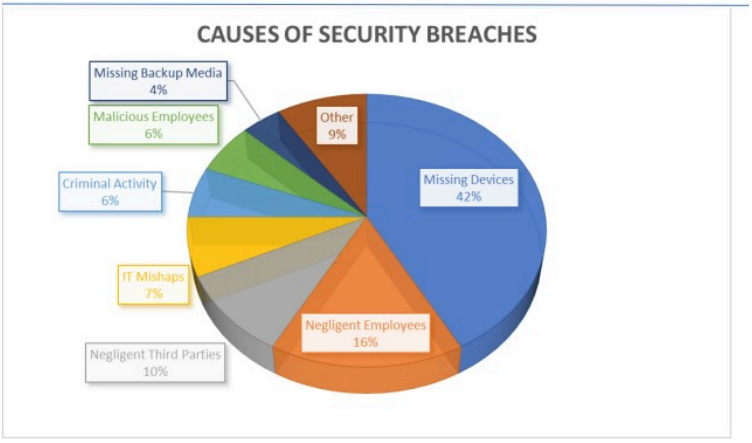


Figure 1 Data Loss Causes from Cipher

Cipher

The figure above shows the various contributors to security and data breaches with the biggest being missing devices and negligence by employees.

Data Loss Prevention Techniques

Data loss can be implemented through various solutions tailored to data protection. These solutions are suitable for institutions. However, enterprise solutions are not ideal for individuals because

they can be quite costly. What simple techniques can an individual use to prevent data loss?

Limit the use of portable devices

Most data loss prevention strategies focus on preventing data leakages from the school's network over the internet, but neglect one of the biggest challenges to any DLP strategy; portable devices. Missing devices account for 42% of data losses; therefore, it is important to limit the use of portable devices in the learning institution. Portable devices are easily lost; hence they are a great weakness in any institutions. An institution can completely disallow them or use only organization issued portable USBs. These USBs should allow automatic encryption to protect any sensitive data that is stored in them.

Individuals should also purchase USBs with such features, or ensure they use tools like BitLocker to encrypt the contents of their portable devices.

Partitions

Another technique used to prevent data loss is the use of partitions. A partition is a logical division of a hard drive. The most common criteria for creating partitions is to have one for the operating system and another for data. By utilizing partitions, you prevent errors in one partition from affecting data in the other partitions and causing data loss. To effectively use partitions, the best time to partition hard drives is before the installation of the operating system. Remember to back up data before using partitioning software, as mistakes could lead to data loss. Some data partitioning software include EaseUS, MiniTool partition wizard and GParted

To create, resize or delete partitions, follow the steps detailed in this article
All external hard drives should also be partitioned to prevent data losses in case one partition fails...

Back-Up

Even after implementing various data loss prevention methods, data loss is still probable. It is important to back up any important data so that in case of any loss, you can restore this data from the backup location. You can use external drives or the cloud to store backups. Most used cloud services include Google Drive, One Drive and Dropbox. Due to the large volumes of data, it is crucial to manage the storage space in the cloud drives available to us as individuals. It is advised that automatic backing up be disabled so that one can decide on the specific data they want to back up.

As earlier mentioned, data can also be lost through accidental deletion. To prevent such loss:

1. Always maintain a regular backup of essential data such as performance grades, class plans, research
2. Organize files into folders depending on the importance. For example, one can have a folder with student grades and another with research. This limits data loss in case one folder gets corrupted or is accidentally deleted.
3. Do not save important data in frequently used partitions or locations to avoid accidental deletion. For example, the Documents folder and the Desktop are frequently used; therefore they are not a good place to store any important data
4. Verify the Recycle Bin before emptying.

Additionally, to prevent data loss through corruption, implement the following guidelines:

1. Have anti-virus software installed as some malware may cause corruption of files
2. Do not interrupt any data transfers as this could lead to corruption of the files being transferred
3. Use the recommended procedure to terminate any applications that access data
4. Safely removing external storage devices like hard drives and flash drives
5. Follow proper shutdown procedures

In conclusion, data losses can be devastating for both organizations and individuals with effects such as financial losses, damage to brand reputation and privacy infringement. However, most data losses can be prevented through caution and use of the mentioned preventive measures.

Data Recovery

Even with the application of data protection and loss prevention techniques, data still gets lost or corrupted and needs to be recovered. Data recovery is the process of retrieving inaccessible, lost, corrupted, damaged or formatted data from storage devices when the data cannot be accessed in the usual way. Data can be recovered from any of the following storage devices:

- Internal (In-built) Hard Disk Drives (HDD)
- Internal Solid-State Drives (SSD)
- External HDDs and SSDs
- Flash memory devices
- Optical Storage Devices
- Floppy Disks

Data recovery is usually required due to physical damage of the storage device or when a logical damage has caused a malfunction of the file system used by the storage device. It could also be needed in case of accidental deletion of data or operating system failure. File corruption can also be caused by certain malware such as viruses. In any case, the goal is to restore data to its normal state and make it accessible. The chances of data recovery usually depend on the data loss scenario. For example, with accidental file deletion, it is easier to recover because when data is deleted, it technically is not wiped permanently from the storage device. It remains on the device until it is overwritten by new data or files. Deleted files can also be easily recovered from the recycle bin. It is important to note that data cannot be recovered after it is overwritten. Therefore, more data should not be saved or transferred into the storage device until the data has been recovered. By avoiding this, you increase the chances of data recovery. Data that was not saved to a location is also impossible to recover. For example, if a document was being modified and had

not yet been saved, a power outage could lead to permanent loss of the changes. It is advised that we enable automatic saving, and still remember to frequently save any documents that we are working on to prevent inconvenience and data losses.

What is the procedure used to recover data? The figure below shows the five steps used to recover data.

Figure 1 Data Recovery Process

1. Identify the cause

The first step to data recovery is determining the cause of the data

loss. The cause will inform the tools to use. Evaluate whether data is recoverable or to count your losses. If you cannot identify the cause, it might be best to consult a data recovery expert to avoid permanent data loss.

2. Classify the lost data

Identify the important data stored in the device so as to prioritize data recovery. For example, curriculum development files will have a higher priority to music. Once lost data has been identified, always check any available backup. If a backup exists, then the whole data recovery process can be foregone and the backup restored.

3. Data recovery solution

The root cause of the data loss will determine the resources needed for recovery. Download any software available online for data recovery. Most software available is comprehensive and provides data recovery for various causes. Data recovery solutions include Recuva, EaseUS Data Recovery Wizard and recoverit.

These tools have free and paid versions. The free versions provide limited capability. However, for simple data recovery, the free version usually suffices. You can also contact your institution's IT department for help because they are likely to have the tools needed to perform data recovery.

4. Document

Document the process used to recover the data. In case of any mistakes, you can be sure of what happened. If you take the device to an expert, you can better explain what you have tried.

5. Preventive measures

After data recovery, enforce measures to prevent the same scenario from happening again. These preventive measures include data backups and partitioning.

Data recovery is time-consuming and can be overwhelming. It is thus better to have backups of all confidential and sensitive data to avoid the hassle. To watch a video on data recovery, use the links below:

One or more interactive elements has been excluded from this version of the text. You can view them online here: https://opentextbooks.colvee.org/advancedcybersecuritytrainingteachers/?p=90#oembed-1

One or more interactive elements has been excluded from this version of the text. You can view them online here: https://opentextbooks.colvee.org/advancedcybersecuritytrainingteachers/?p=90#oembed-2

Module 2 Summary Infographic


7. Lock your devices
Use passwords, PINs or fingerprint to prevent unauthorized access.
8. Remote location and device wiping
If your device has feature, enable it. In case the device is lost or stolen, you can track it and delete all your information to prevent it from landing on the wrong hands.

Module 2 Files and Resources

/wp-content/uploads/23/2023/06/Week-2-Data-Access-Controls-Transcript.pdf

/wp-content/uploads/23/2023/06/Week-2-Data-Access-Controls-1.pdf

/wp-content/uploads/23/2023/06/Week-2-Data-Loss-Prevention-1.pdf

/wp-content/uploads/23/2023/06/Week-2-Data-Protection-1.pdf

/wp-content/uploads/23/2023/06/Week-2-Data-Recovery-1.pdf

/wp-content/uploads/23/2023/06/Week-2-Data-Security-Transcript.pdf

/wp-content/uploads/23/2023/06/Week-2-Data-Security.pdf

PART III

SECURING ONLINE COMMUNICATION AND LEARNING DEVICES

Online Privacy

What is Online Privacy?

Online privacy, which is also referred to as internet or digital privacy, refers to how much of your personal, financial, and browsing information and data remains private when you are online. According to Wikipedia, Internet privacy involves the right or mandate of personal privacy concerning the storing, repurposing, provision to third parties, and displaying of information pertaining to oneself via the Internet.

The amount of information shared online is a lot and the diversity therein is equally a lot. We share all sorts of information with businesses, institutions, on social media platforms as well as with friends and family. Just as we are cognizant of the information we share with others in real life, we should also value data privacy while online. On the internet, nothing is free: whether it is downloading apps, using an email service such as Gmail or Yahoo, or even using platforms such as Facebook, Instagram or WhatsApp, they all have an expense attached to their usage. When online, remember that you are always sharing data about yourself. And the truth is online privacy exists on a spectrum: some online entities gather and store more information about you than other platforms.

Internet privacy involves both personal and sensitive information. Personal information has identifiers that can identify you such as your username, your IP Address, home address and so on and so forth. Sensitive information, as we saw in the CTT course, has very private data such as medical records, employee financial information, student records, and even information that you might not be ready to share publicly, such as your political views or even your sexual orientation

Internet Privacy Issues

1. Online Tracking

Anytime you have been online through a web browser such as Chrome, Firefox, Opera or even Edge, then you probably have picked up a few cookies and you have probably clicked on a popup that looks like Figure 1.

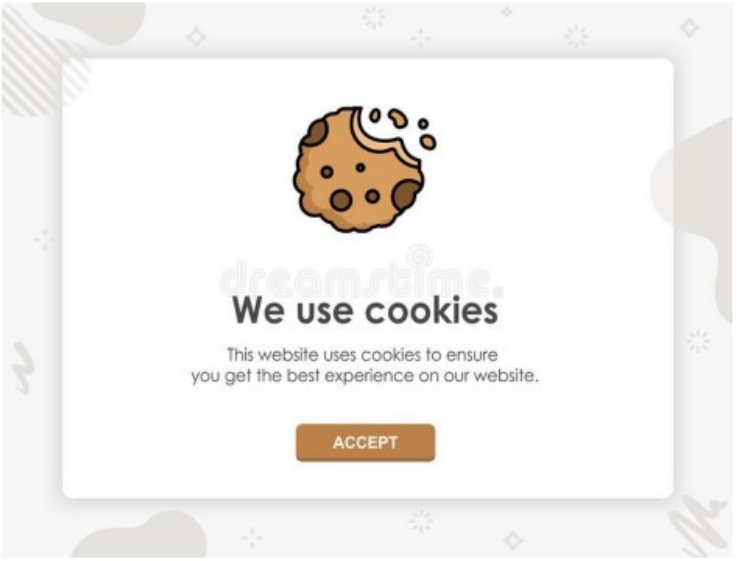


Figure 1: Sample Accept-Cookie Popup from Dreamstime

Dreamstime

Cookies are small bits of information that are used to remember things about the websites you visit such as your login information, your location, your ad settings,
what's on your shopping cart or even what language you prefer.

Most cookies are harmless and make your online experience seamless. Others, however, remain active even on websites that they did not originate from gathering information about your behaviour and what you clicked on. These are called **third party persistent cookies or tracking cookies.**

Resources on the web that use a lot of tracking cooking include advertisements and social media widgets such as like and share buttons. You do not even need to click on an ad or social media sharing button for a tracking cookie's information about you to be transmitted back to a server owned by the person or company who created it. As soon as you load the page, the cookie is sent to the server where it originated. If no cookie exists yet, the resource can create one. Tracking cookies are particularly notorious for collecting all sorts of information: search queries, purchases, device information, location, when and where you saw previous advertisements, how many times you've seen an ad, and what links you click on. All of this and more is collected, often without your consent or knowledge. Tracking cookies are usually used for advertising purposes such as retargeting. Retargeting is a tactic that often relies on tracking cookies to show ads to people who have previously visited a specific site or shown interest in a particular product. If you have ever bought or even looked at a product on Facebook or Instagram and then started seeing ads for similar products on other websites, you've been retargeted. This can become a huge concern especially if you are trying to maintain a sense of anonymity while online.

2. Mobile Apps and Privacy

We all use apps on our phone, whether to socialize with our colleagues or students, keep track of what is happening around our world or even to pass time through entertaining games. We know our favourite apps but they tend to have a lot more information

about us. Many apps request and require permissions that they frankly do not need. These "dangerous" permissions pose a risk to users' privacy by allowing access to sensitive information such as users' location, mobile phone data, phone status, and a lot more. This is especially prevalent among free apps. A recent study from researchers from Oxford University found that a whopping 90% of free apps on the Google Play store share data with organizations. Say for example you installed a simple chess game app on your phone, do you think it is necessary for the application to have access to your location, contact book or even camera? It makes sense for a taxi app to require permissions to your location but not a chess game application. When providing access/permissions to applications, a good rule of thumb is to consider whether you trust the app provider/company to hold this information. If there is anything you feel uncomfortable with, you can deny access, either instantaneously or in the app's settings.

3. Search Engine User Tracking

Search engines are websites through which users can search for internet content. The most famous one is Google. There are others such as Yahoo and Bing. When it comes to search engines, users are especially sensitive to tracking – search engines have access to a lot of private and revealing information, your search history. Some search engines can track every search you do on a single website – down to IP address-level. Additionally, if the search engine provider also makes the browser (Google Chrome, Firefox, Internet Explorer), then they have your browsing history regardless of whether you searched for the site. Search engines can collect a lot of information about you. They:

- Have access to your history – both browsing and click through
- Track what you do on a certain website

- Recognise that you have visited again through cookies, local storage or even your IP address
- Build a profile of all the things you like to search for and note changes over time, e.g. if you start searching for a new medical condition, if you start looking for jobs, if you are planning on moving/travelling

This is tremendous information gathered about you just from you using your search engine.

4. Social Media Data Harvesting

According to Wikipedia, Social media mining is the process of obtaining big data from user-generated content on social media sites and mobile apps in order to extract patterns, form conclusions about users, and act upon the information, often for the purpose of advertising to users or conducting research. While this appears harmless, over the past couple of years, we have all been aware of the rampant and large scale data mining that was being conducted by Facebook and other big social media companies without the explicit consent of the users of these applications. Social media privacy hit the spotlight mostly thanks to a string of large and very public scandals including the Cambridge Analytica story in which data was used to manipulate voters in countries such as Kenya and USA, cyber bullying and "doxing" which involves sharing private information publicly with the intent of damaging their reputation or extorting them.

Enforcing Online Security

So, now that we are aware of how prevalent tracking of our data and

information is while online, how do we then ensure that we remain anonymous and maintain a sense of privacy while still enjoying the full benefits of the internet?

- **Change your search engine**. If you are concerned about what information your search engine has on you, consider getting a different one. There are more privacy-centered search engines such as DuckDuckGo, Mojeek and Qwant. DuckDuckGo in particular is very popular with privacy enthusiasts and is the default search engine in the Tor Browser, which is a browser that is unique in that it provides anonymous access to both the ‘‘clear” and Dark net.
- **Browse in Incognito Mode**. Many popular browsers offer the option of browsing privately. This is the incognito mode. While Incognito browsing offers some privacy, it does not provide total anonymity. In fact, when you open an Incognito window, it explicitly states that your browsing activity might still be visible to websites you visit, your employer or school, and your internet service provider. The main thing it does is hide your browsing history from other people who use the same computer. It essentially deletes the history of any websites you may visit during the session, saves no information you may enter in forms you fill out and deletes any “cookies” that you might collect along the way. Figure 2 below shows th Incognito Mode on Google Chrome while Figure 3 shows how it appears on Firefox.

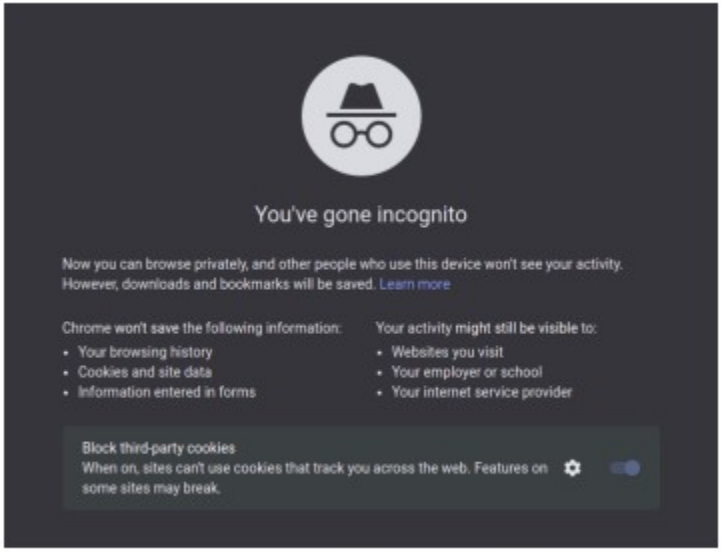


Figure 2: Incognito Mode on Google Chrome

Figure 2: Incognito Mode on Firefox

- **Use VPNs while browsing online**. VPNs (Virtual Private Networks) usually route your online traffic through an encrypted tunnel and in turn a remote server will pose as you. What this does is that it keeps your IP address and location secret from sites you access, protects you from hackers and in some cases, VPNs can give you access to some sites and services that may be unavailable in your country. You can have a VPN on both your phone and laptop/computer. There are many VPN providers available, some free and some paid. There are many considerations to make while selecting the best VPN provider. Resources have been provided that may be useful to you as you make that decision. Additional resources have been attached that may help you better understand how VPNs work and why they are important.
- **Clear your cookies as often as possible**. Another way to manage cookies, especially tracking cookies is to **enable the**

DNT (Do Not Track) setting. Enabling this feature will send a request to the website you're currently on to disable its cross-site user tracking of individual users. This includes tracking cookies. While some sites honor your choice to opt out with Do Not Track, many will not. Do Not Track does not add any technical limitations and there's no enforcement from any authority. You should definitely enable Do Not Track in your browser, but you'll need to go a step further if you want to put a halt to tracking cookies. You further prevent tracking cookies from sharing your information, you can **install anti-tracking browser extensions** which block advertisers that use tracking cookies from loading any content in your browser. Disconnect, Privacy Badger and Adblock Plus are good examples.

- Finally, **always review privacy policies carefully** of the applications you use and/or install. This also applies to online browsing. A common mistake when it comes to online browsing is to simply click "agree" to user agreements and privacy policies without reading them. It is advisable you take a look at any document before clicking "agree" or "accept". If you don't have time to read it (and some user agreements are hundreds of pages long), research what the app or site asks of its users and whether you're comfortable with what they know about users. When it comes to mobile apps, opt **out of app tracking**. To do this you have to go to your app settings (either within the app or in your phone settings) and out of the app tracking information.

So, let's recap, to maintain online privacy and anonymity, it is paramount to use VPNs, browse as much as possible on Incognito Mode, review privacy policies on both apps and websites especially if they will have access to a lot of your personal information. And finally, if you can, change your search engine.

Endpoint Security

One or more interactive elements has been excluded from this version of the text. You can view them online here: https://opentextbooks.colvee.org/advancedcybersecuritytrainingteachers/?p=105#oembed-1

Transcript

Hello, my name is Malusi Faith and I am your instructor for week 3. In the second topic of Week 3, we will look at Endpoint Security. However, before we begin, it is important to understand what we mean when we talk about an endpoint.

The term endpoint can be defined in many ways. However, contextually, we can call any device on a network that can be accessed by another device as an endpoint. If a device is connected to a network, it is considered an endpoint. With the growing popularity of Bring Your Own Device policy that allows employees to bring their own devices for use in the organization or institution and IoT which is the Internet of Things, the number of individual devices connected to an organization's network can quickly reach into the tens or even hundreds of thousands.

Endpoints are usually the easiest entry points for threats and malware and as such they are a favorite target for malicious people. Endpoints can range from the more commonly thought of devices such as laptops, tablets, mobile devices, computers, printers, servers to smart watches, smart devices such as light bulbs, car sensors, cameras, pacemakers, and even your smart refrigerator. As the different types of endpoints have evolved and expanded, the security solutions that protect them have also had to adapt.

There are many ways to secure endpoints, and in this case we'll talk about the more predominant devices like our computers, laptops and mobile phones. Typically, endpoint security software, especially in an organizational environment will include these key components:

1. Advanced antimalware and antivirus protection to protect, detect, and correct malware across multiple endpoint devices and operating systems
2. Proactive web security to ensure safe browsing on the web
3. Data classification and data loss prevention to prevent data loss and exfiltration by malicious actors
4. An Integrated firewall to block hostile network attacks
5. Email gateway to block phishing and social engineering attempts targeting your employees
6. Insider threat protection to safeguard against unintentional and malicious actions

7. Endpoint, email and disk encryption which helps prevent data exfiltration

However, in this course, we'll focus more on techniques that work really well for individuals as well as in a simple school network. These techniques are:

- Antimalware Software
- Host-Based Firewalls

Antimalware Software

We will begin with Antimalware software which is commonly referred to as an Antivirus. This is software that is installed on a device to detect and mitigate viruses and malware. Malware is a broad term, which comes from the combination of the words 'malicious software', that is used to describe all kinds of malicious or unwanted software. Common types of malware include:

- Viruses which are a piece of malicious code capable of copying or multiplying itself, thereby deleting data, stealing data, and corrupting or crashing the system.
- Trojans which is Malware disguised as legitimate software, but it performs illicit activities such as stealing passwords, deleting data when a user runs it.
- Keyloggers which is a Spyware that records keystrokes made by a computer user in order to fraudulently access confidential data such as passwords, bank account details, etc.

- Ransomware which Locks down your system or displays threatening messages to force you to pay a ransom to the attacker to regain access.
- And finally Worms which harm host networks by self-replicating to overload web servers and consume large amounts of bandwidth.

Antivirus solutions are usually installed on individual devices such as desktops, laptops and smartphones as well as on servers. They normally run constantly in the background and conduct periodic scans of device directories and files for malicious patterns which may indicate the presence of malware.

Since new malware is developed every day, antivirus software vendors constantly update their existing databases; it is these updates that pop up as notifications on your screen.

It is important to note that, if you don't keep your antivirus software up to date, it will continue to rely on old virus definitions and will fail to detect new viruses, making you more prone to attacks. Additionally, antiviruses offer additional services such as:

- Web protection: Helps to keep your online browsing sessions and downloads from the internet safe by blocking bad results or warning you when you are about to visit a malicious web page.
- Threat identification: Identifies various types of malware.
- File quarantine: Removes or isolates infected

files depending upon the severity of damage.

- Alerts and notifications: Notifies you about periodic scans and updates as well as sending alerts about infected files and potentially malicious software.
- Automatic updates: Provides remote updates about virus scan rules to keep the software upto-date and capture new viruses and threats.

Antivirus software is usually available as a stand-alone solution or as one component of an endpoint protection platform. There is a wide range of antivirus software available on the market. Examples are Windows Defender Virus & Threat Protection which comes preinstalled in all Windows Operating Systems, Kaspersky Antivirus, Bitdefender Antivirus Plus, Norton Security, McAfee, Trend Micro, and many others.

Host-Based Firewalls

Next we will look at firewalls and in particular Host-Based firewalls. This is a software that's installed on an endpoint, usually a server or a laptop or computer that restricts incoming and outgoing connections to and from the device. Basically, firewalls work as a filtration system for the data attempting to enter or leave your computer or network. Firewalls can scan network traffic for malicious code or attack vectors that have already been identified as established threats and should a packet be flagged and determined to be a security risk, the firewall prevents it from entering the network or reaching your computer.

Firewalls are customizable depending on your needs. This means that you can add or remove filters based on several conditions. Some filters include specific IP addresses, websites, or even specific words and phrases. For example, you could instruct the firewall to block any traffic with the word "X-rated" in it. The key here is that it has to be an exact match. The "X-rated" filter would not catch "X rated" keyword because it lacks a hyphen. But you can include as many words, phrases and variations of them as you need. Whether installed completely on the host or distributed, host-based firewalls are an important

layer of network security along with network-based firewalls. Here are some examples of host based firewalls:

- First we have the Windows Defender Firewall. First included with Windows XP, Windows Firewall (now Windows Defender Firewall) uses a profile-based approach to firewall functionality. Access to public networks is assigned the restrictive Public firewall profile. The Private profile is for computers that are isolated from the internet by other security devices, such as a home router with firewall functionality. The Domain profile is the third available profile. It is chosen for connections to a trusted network, such as a business network that is assumed to have an adequate security infrastructure. Windows Firewall has logging functionality which can be used to log traffic.
- Secondly we have the UFW which stands for

(Uncomplicated Firewall) – This is a simple application that allows Linux system administrators to configure network access rules.

- Finally, for devices that run Mac OSs, we have the Mac OS X Firewall – This is a built in firewall in macOS devices. By default it is not turned on, therefore it would be prudent to enable it on your device.

Now that we have looked at how antivirus software and firewalls work, it is now up to you to employ the use of these tools on your devices, to ensure that your data and information remain safe.

Understanding Encryption

One or more interactive elements has been excluded from this version of the text. You can view them online here: https://opentextbooks.colvee.org/advancedcybersecuritytrainingteachers/?p=107#oembed-1

Transcript

Hello, my name is Malusi Faith and in this subsection of the third topic of Week 3 we will be looking at encryption as a means of securing our communication especially while online. We have seen encryption being mentioned quite a lot in week two's content. Securing online communication depends a lot on whether data in transit is encrypted or not. Security is a major concern on the internet, especially when you're using it to send sensitive information between parties. There's a lot of information that we don't want other people to see such as credit card information, social security numbers, private correspondence, personal details, sensitive company information and even bank-account information. Institutional data such as staff and student private information, institutional intellectual property and financial information should also be kept away from unauthorized parties. Providers of services that enable us to perform services like these have a mandate to

protect our information from malicious actors and this is where encryption comes in.

So, what is encryption? Encryption is a process that encodes a message or file so that it can only be read by certain authorized people. It scrambles or encrypts data, and then uses a key for the receiving party to unscramble, or decrypt, the information. The message contained in an encrypted message is referred to as plaintext. In its encrypted, unreadable form it is referred to as ciphertext. For example, let's say you want to send a secret message to your colleague. You would create a coded message in which each letter is substituted with the letter that is two steps down from it in the alphabet. So "A" becomes "C," and "B" becomes "D" and so on and so forth. You have already told your colleague that the code is "Shift by 2". Your friend gets the message and is then able to decode it. Anyone else who sees the message will see only nonsense. In this scenario, shifting the alphabet is the algorithm and 'Shift by 2' is the key that will be used to decode the ciphertext into plaintext.

Password protecting your school documents such as those with student grades, health or financial information of your students, teachers or school staff is an example of encryption. The password then becomes the key through which the information is retrieved. Additionally, there are online tools that can help in encrypting important and sensitive information. These tools have been added as part of the resources within this week's content. So, all you need to do to make sure no one is able to access important information in transit is to ensure that you password protect your information

and simply send the password securely to the recipient together with the scrambled file.

In the article which follows this video, we will look at different tools, which employ end to end encryption, that ensure secure communication online between parties.

Secure Communications

The internet, telecommunication networks, advancement in technology and ease of access to the internet have made communicating with people easier than ever, but as we've seen previously, it has also made surveillance more prevalent. The COVID pandemic has further accelerated wider adoption of online communication. Online communication in almost all sectors of the economy has become the norm and contextually, online learning has become something that both educators and learners have had to learn and adapt to over a very short period of time. Without taking extra steps to protect your privacy, every phone call, text message, email, instant message, video and audio chat, and social media message that you share with your students or colleagues could be vulnerable to eavesdroppers.

Often the most privacy-protective way to communicate with others is in person, without computers or phones being involved at all. Because this isn't always possible, especially now, the next best thing is to use end-to-end encryption. We have looked at encryption in the video preceding this article and by now you have a clear understanding of how encryption works. So, how do we ensure that our communication, especially online is secure and encrypted? We'll look at 3 major ways that we communicate online: via our mobile phones, over email and on other channels especially while teaching and learning.

Securing Mobile Communication

When you make a call from a landline or from your mobile phone, your call is not end-to-end encrypted, The same is true for text messages. This can allow governments, law enforcement, malicious actors or anyone else with the expertise to read your text messages

or even record your phone calls. To ensure that no one can intercept your communication, you may prefer to use encrypted alternatives that operate over the Internet. As a bonus, many of these encrypted alternatives also offer video capabilities.

Some examples of services or software that offer end-to-end encrypted texting and voice and video calls include:

- Signal (for iOS and Android
- WhatsApp (for iOS and Android)
- Wire

Some examples of services that do not offer end-to-end encryption by default include:

- Google Hangouts
- Kakao Talk
- Line
- Snapchat
- WeChat
- Yahoo Messenger

And some services, like Facebook Messenger and Telegram, only offer end-to-end encryption if you deliberately turn it on. Others, like iMessage, only offer end-to-end encryption when both users are using a particular device (in the case of iMessage, both users need to be using an iPhone).

It is a good idea to do some research on whatever software you use to communicate digitally. Doing so will help you make appropriate choices based on your needs. Before choosing a chat application, it is important to consider the following:

- **Is it end-to-end encrypted?**
- **Is it open-source?** Open-source software means the code is published online, and freely available to be studied and commented on by anyone in
  the world. The benefit of open-source technology is that if

there is a security vulnerability in the code, there is a higher chance of someone catching it and speaking up about it, and that issue getting fixed quickly.

- **What does the company collect and store about you?** The less a chat app collects about you, the less they can divulge about you.
- **Do you have to connect your phone number to the app?** While most chat apps require your phone number to sign up, there are a few privacy conscious chat apps that give you the option to create a username, rather than connect to your phone number. Wire is one such example.

With about 2 billion users, WhatsApp is one of the most commonly used channels of communication. So, what security features does it have and how can we ensure that WhatsApp is more secure and private?

1. **Turn on security notifications.** When a new phone or laptop accesses an existing chat, a new security code is generated for both phones. And
   WhatsApp can send a notification when the security code changes. This way, you can check the encryption with your friend over a different messenger, ensuring its security. To turn on security notifications, go to **WhatsApp > Settings > Account > Security > Show security notifications** and flip the toggle to green.
2. **Enable two factor authentication** if it is supported. 2FA adds a periodic passcode to WhatsApp, and also ensures that your data isn't accessed by
   someone else. This is perfect because unfortunately there's no way to lock WhatsApp with a password, unless with a third party locking app on Android. Apple doesn't allow locking WhatsApp with a passcode or Touch ID. To activate 2FA, go to **Menu > Settings > Account > Two-step verification > Enable**. Follow the steps to create a six-digit PIN code that you can

easily remember. Importantly, add your email address to retrieve that code in case you forget it.

3. **Disable Cloud Backups.** Cloud backups are really important because it keeps a repository of all your old messages, however if you really care about
your privacy, then you should consider disabling your cloud backup. If you back up your WhatsApp messages to iCloud or Google Drive, for example, they're no longer encrypted and anyone with access to these databases can read all your messages. To disable automatic cloud backups:
On iPhone: Go to **WhatsApp > Settings > Chats > Chat Backup > Auto Backup > Off**
On Android: Go to **WhatsApp > Menu > Settings > Chats > Chat Backup > Backup to Google Drive > Never**
4. **Protect your privacy on Whatsapp. Control what information other users have access to**. You can control who can see your Last Seen, profile
photo, about, status, and live location. You can also turn off Read Receipts here, so the blue check marks are switched off. This depends entirely on what works best for you and for your audience. Go to **Settings > Account > Privacy** to see everything at your disposal.

The biggest concern with WhatsApp, other than the fact that it doesn't encrypt its backups, both local and cloud, is the fact that it does not encrypt your metadata which includes for example sender information, recipient information, the dates and times when messages are sent and received, how much information was sent and various data about the devices used. Metadata might seem relatively insignificant, but it can reveal quite a lot about your social networks and about your personal and work-related communication patterns, especially if someone is able to analyse a large volume of it. This is where Signal comes in.

Signal is much better compared to WhatsApp when it comes to

security concerns. Other than the features on WhatsApp, Signal also provides:

1. **Disappearing messages.** This feature allows you to set a length of time after which messages to and from a user will disappear. Assuming you want to share the password to a Google Drive containing sensitive information about your students to your colleague, you can send the message to them that's only visible for 1 hour, after which it disappears. This is an easy way to limit the information that might be exposed if a device is lost, stolen, confiscated or infected with malware. Keep in mind, however, that features like this will not prevent the sender or the recipient of a message from making a copy of it. Wire also has this feature.
2. Signal is also **able to encrypt metadata**. In order to protect user privacy from all corners, Signal devised a new way to communicate between the sender and the recipient and it's called Sealed Sender. Basically, with Sealed Sender, no one will be able to know — not even Signal — who is messaging whom, which is amazing.
3. You can also **lock the Signal app with a passcode or biometrics. Additionally there is 2FA and an option to block screenshots within the app and the recent screen. And to top it off, Signal by default encrypts all the local files with a 4-digit passphrase. And if you want to create an encrypted local backup** then you can do that as well. All in all, in terms of security and privacy protection, Signal stands head and shoulder above WhatsApp and that makes it the most secure messaging app.

However, before you decide to migrate or enforce any of these options, you should do some research about your audience, what both your needs are, and where they intersect. How do your students normally communicate? What channel is mostly used in your school?

Securing Email Communication

Other than our phones, the most prevalent form of communication in schools and learning institutions is through emails. So how do we ensure that what we share over email is safe and secure? Once again, encryption comes into play. Some educators access their emails through a website such as Gmail, which is very common, while other institutions send and receive using email clients such as Thunderbird, Apple Mail or Outlook. Regardless of how you access your emails, it is important that you employ the use of end-to-end encryption and one of the most well-known forms of end-to-end encryption is called Gnu Privacy Guard (GPG) which can be implemented in emails. PGP which stands for Pretty Good Privacy, is used interchangeably with GPG. As part of the resources, links have been provided on how to use and install PGP in Thunderbird, Outlook, Apple Mail and Gmail as well as some reading for how GPG works.

Some email services already are privacy oriented. Usually, they already have PGP integrated and they are usually affordable and accessible. They include:

- ProtonMail (Web, Android, iOS)
- Tutanota (Web, Android, iOS)
- Posteo (Web)
- Kolab Now (Web)
- mailbox.org (Web)

Securing Other Forms of Online Communication

Other than using emails and communicating via our phones, we log onto school portals, we communicate with friends, family and

colleagues over social media, we make transactions online with banking institutions, we buy stuff online, we learn new things by watching videos and entertain ourselves with music and movies online. Most of the time, we access all this information through websites or web applications. While interacting with these sites, how can we confirm that while sharing sensitive information such as student/employee data, banking information, credentials, and even PII, that it is not tampered with while in transit or even in storage?

How do we know we are interacting with a secure website?

When you visit a secure website, the Uniform Resource Locator (URL) in your browser's address bar should begin with HTTPS:// rather than HTTP://: If it does, and if your browser does not display any errors, then you should be communicating through an encrypted connection between your browser and the server where the website is hosted. You may also notice a 'lock' symbol near the Web address. These are clues to let you know that it will be much harder for someone to eavesdrop on your communication with that particular website. Some browsers also flag HTTP websites as "not secure."

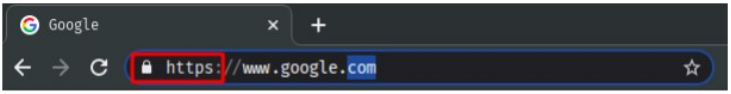


Figure 1: Secure Site with https indicator and padlock.

Figure 2: A sample insecure site

You should avoid typing your password, or any other sensitive information, into a website that does not support HTTPS. In addition to passwords and financial transactions, HTTPS also helps

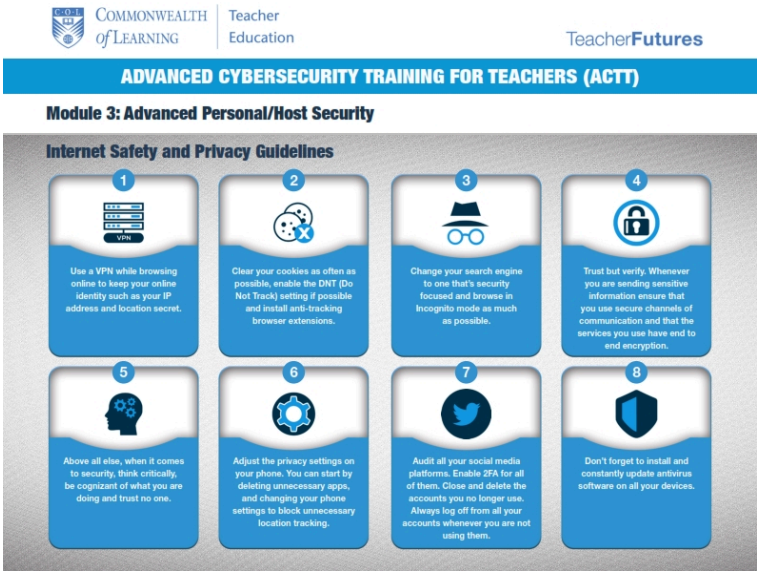
protect your webmail messages, search engine queries and social media communication as they travel between you and your provider. If you are using a service like this, and it does not offer you an HTTPS connection, you should switch providers.

If you use Firefox or Chrome as your browser, you can also install the **HTTPS Everywhere** extension. It will try to ensure that you do not end up using an insecure connection when you visit sites that do support HTTPS.

When it comes to social media communications, employ wisdom and the tried and tested methods we talked about in the CTT course. Just as a recap, ensure that you:

1. Practise good password hygiene. Use different passwords for your social media accounts, and also make sure each password is complex and unusual. Avoid password re-use. Enable 2FA for all your accounts to prevent unauthorized parties from accessing your accounts. If possible, create a whole new email specifically for social media accounts so that if you are compromised, hackers won't have access to any valuable information.
2. Check what apps are connected to your social media. This usually happens when you use Facebook or Google to sign into other applications. Assess thoroughly if this level of access is necessary.
3. Keep your mobile apps and software updated.
4. Close the accounts that you're not using. Forgotten social media accounts may be compromised without being noticed. Hackers can leverage these, and access other accounts linked to it, like your email.
5. Limit access to corporate social media accounts to only those who are authorized to have access to them. Additionally, monitor all correspondence that occurs through the corporate social media accounts.

Module 3 Summary Infographic



Module 3 Files and Resources

/wp-content/uploads/23/2023/06/Week-3-Endpoint-Security-Transcript.pdf

/wp-content/uploads/23/2023/06/Week-3-Understanding-Encryption-Transcript.pdf

/wp-content/uploads/23/2023/06/Week-3-Additional-Best-Practices.pdf

/wp-content/uploads/23/2023/06/Week-3-Endpoint-Security.pdf

/wp-content/uploads/23/2023/06/Week-3-Online-Privacy-1.pdf

/wp-content/uploads/23/2023/06/Week-3-Secure-Communications.pdf

/wp-content/uploads/23/2023/06/Week-3-Understanding-Encryption-1.pdf

/wp-content/uploads/23/2023/06/Week3_Resource_List.pdf

PART IV

CYBERSECURITY CONCERNS IN EMERGING EDUCATIONAL TECHNOLOGIES

Introduction to Emerging Technologies

One or more interactive elements has been excluded from this version of the text. You can view them online here: https://opentextbooks.colvee.org/advancedcybersecuritytrainingteachers/?p=123#oembed-1

Emerging Technologies

This module aims to enlighten you about the cybersecurity concerns in emerging technologies. You will learn about various emerging educational technologies like virtual and remote laboratories, mobile learning, smart boards, virtual reality, automation, cloud computing, the Internet of Things, and 3D printing. More so, you will learn about the benefits of these technologies as well as the cybersecurity concerns around them and their countermeasures.

Emerging Educational Technologies

Learning institutions are experiencing the power of technology more than ever before. Educational technology tools, which were once thought of as nice-to-have, are now needed to continue teaching students without disruption in the current era. Emerging technologies for teaching and learning are making a significant impact on the ways teachers prepare their content and students

consume course material. Additionally, schools are being pushed to adapt to new educational technologies to stay competitive.

Initially, one of the biggest challenges in incorporating emerging technologies in the classroom is the fear of how to implement them effectively. Not every educator is tech-savvy or understands the full potential of current educational technologies to drive the success of the students. Embracing these technologies improves both the teacher's and learner's experience and addresses some of the limitations of face-to-face learning such as those imposed by the COVID-19 pandemic.

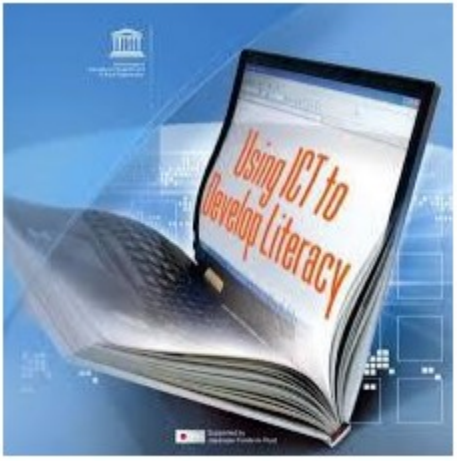


Figure 1: Using ICT to Develop Literacy From UNESDOC

Specific Examples of Emerging Educational Technologies

From online learning to 3D printing, a variety of technologies are making the biggest impact on student learning today. These technologies also allow educators to account for the shortened

attention spans and on-demand expectations of many of today's students. These technologies include:

1. **Video and online classes:** With the undeniable growth of usage in Zoom, Microsoft Teams, and additional web conferencing tools, due to the novel coronavirus, many schools are continuing to see the benefits of offering more coursework online and remote student learning. The growth of online courses and video materials is only expected to continue and adapt to allow for more personalized student learning.

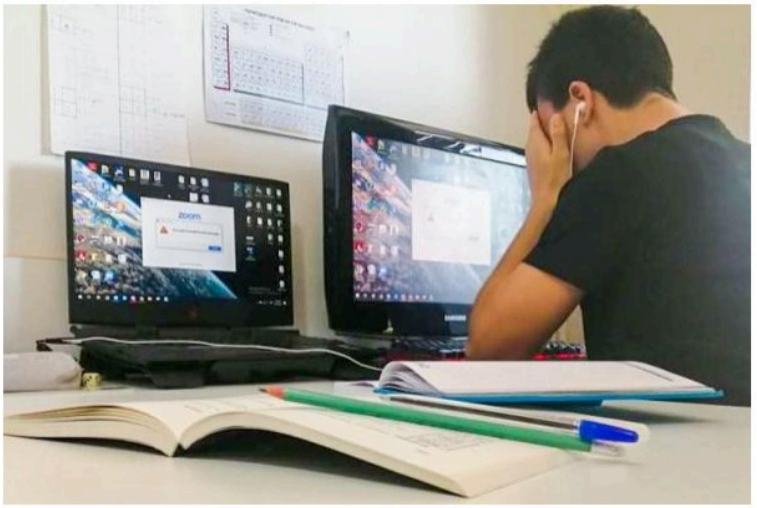


Figure 2: Image of a student learning while from unicef

2. **Mobile Learning:** Students are now using tablets or mobile phones loaded with educational apps and e-textbooks to access information, receive instruction, conduct research, and submit their assignments. The mobile devices have provided opportunities for both educators and students with little to no training to create, store, and share their own.

3. **Gamification:** Many educators are utilizing gamification as an educational approach to motivate students. Essentially, this method

allows them to learn by utilizing video game design and game elements in the learning environment. Gamification allows schools to create enjoyable and engaging experiences for students by inspiring them to approach education through games, contests, and more.

Figure 3: Gamification for learning from openPR

4. **MOOCs:** Educators across the globe are doing some amazing things with MOOCs. They have managed to strike a balance between automating the assessment process while delivering personalized, authentic learning opportunities.

5. **Artificial Intelligence:** Artificial Intelligence-based tools continue to showcase how they can help an array of students participate in online and offline course settings. For example, schools can embed AI-powered captions onto their videos and offer interactive transcription to students who may not be able to participate live otherwise, such as those who are deaf or hard of hearing. Additionally, these tools help to serve as learning features for all students and are proven to drive academic success with additional ways to engage with materials more effectively.

Figure 4: Artificial Intelligence from Forbes

6. **3D printing and virtual reality:** These emerging trends for teaching and learning are reinventing the student experience and their capacity to become proficient in their field with more visual methods that wouldn't be feasible prior. Virtual and remote labs offer flexibility, as students can run experiments as many times as they like, both in and out of school. Because these labs are designed to allow for easy repetition of experiments, students feel less pressure to execute perfectly the first time. In the controlled environments of these labs, students are safe, even if they make an error.

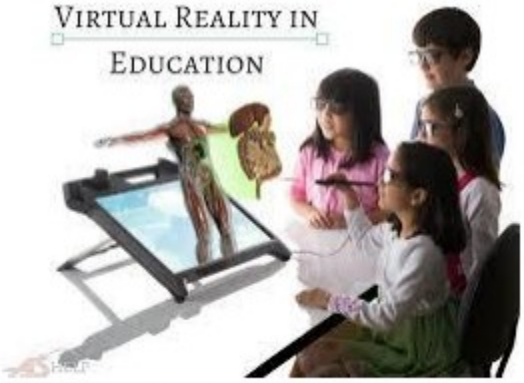


Figure 5: Virtual reality in learning from myassignement

While 3D printing is four to five years away from widespread adoption in schools, it is easy to pinpoint the practical applications that will take hold. Geology and anthropology students, for instance, can make and interact with models of fossils and other artifacts, and organic chemistry students can print out models of complex proteins and other molecules through rapid prototyping and production tools. Even more compelling are institutions that are using 3D technology to develop brand new tools.

Trends in educational technology and the growing usage of ed-tech tools only show the power and potential these additional materials and methods of teaching provide to today's students. Education is about sharing knowledge and technology allows for seamless knowledge sharing and collaboration with faculty, students, and professionals around the world.

Click on the link below to explore the country by country reports of how education is evolving across the globe: https://edu.google.com/latest-news/future-of-the-classroom/emerging-technologies/

Benefits of Emerging Technologies

Technology has greatly impacted the everyday learning experience. It has greatly expanded access to education. In medieval times, for example, only the elite had access to educational opportunities and books. Individuals had to travel to centers of learning to receive an education. Today, everything is available online and on-demand. Technology has also enabled teaching to occur in a variety of formats, both formal and informal, including MOOCs, podcasts, and standard online degree programs. Regardless of the specific learning method, opportunities to collaborate and hear from professionals and thought leaders directly have greatly expanded with access to technologies. Below is an outline of the benefits of emerging educational technologies:

1. Improves engagement

When technology is integrated into lessons, students are expected to be more interested in the subjects they are studying. Technology provides different opportunities to make learning more fun and enjoyable as the same things are taught in new ways e.g. delivering teaching through gamification, taking students on virtual field trips, and using other online learning resources. Furthermore, technology can encourage more active participation in the learning process which can be hard to achieve through a traditional lecture environment.

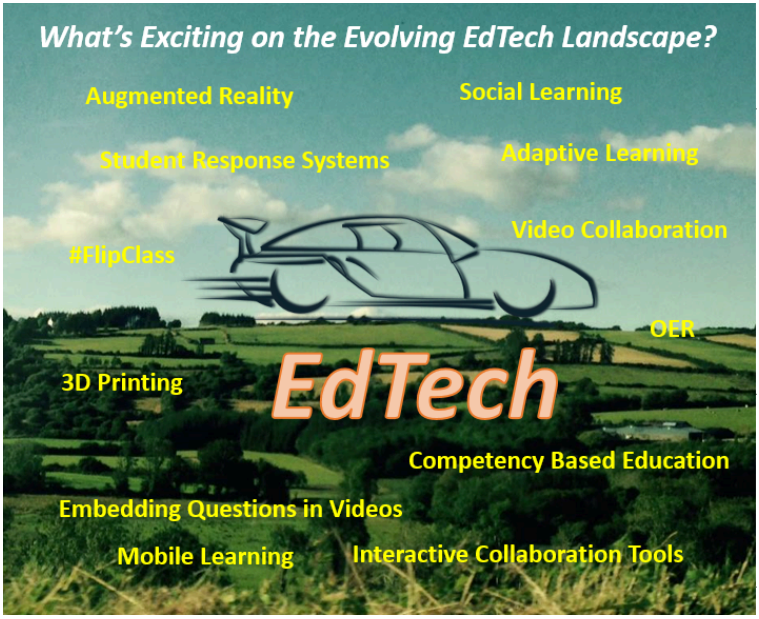


Figure 1: Benefits of educational technologies from Emerging EdTech

2. Improves knowledge retention

Students who are engaged and interested in things they are studying, are expected to have better knowledge retention. As mentioned before, technology can help to encourage active participation in the classroom which is a very important factor for increased knowledge retention. Different forms of technology are experimented with to learn what works best for students in retaining knowledge.

3. Encourages individual learning

No one learns in the same way because of different learning styles and abilities. Technology provides great opportunities for making learning more effective for everyone. For example, students can learn at their speed, review difficult concepts, or skip ahead if they need to. Additionally, technology can provide more opportunities for struggling or disabled students. Access to the Internet gives students access to a broad range of resources to research in different ways, which in turn increases engagement.

Figure 2: A student learning alone at home from WeForum

4. Encourages collaboration

Students can practice collaboration skills by getting involved in different online activities. For instance, working on different projects by collaborating with others on forums or by sharing documents in their virtual learning environments. Technology can encourage collaboration with students in the same classroom, same school, and even with other classrooms around the world.

Figure 3: Students working collaboratively from Pan World Education

5. Students can learn useful life skills through technology

By using technology in the classroom, both teachers and students can develop skills essential for the 21st century. Students can gain the skills they will need to be successful in the future. Modern learning is about collaborating with others, solving complex problems, critical thinking, developing different forms of communication and leadership skills, and improving motivation and productivity. Furthermore, technology can help develop many practical skills, including creating presentations, learning to differentiate reliable from unreliable sources on the Internet, maintaining proper online etiquette, and writing emails. These are very important skills that can be developed in the classroom.

6. Benefits for teachers

With countless online resources, technology can help improve

teaching. Teachers can use different apps or trusted online resources to enhance the traditional ways of teaching and to keep students more engaged. Virtual lesson plans, grading software, and online assessments can help teachers save a lot of time that can be used for working with students who are struggling. Furthermore, having virtual learning environments in schools enhances collaboration and knowledge sharing between teachers. Highlighting the benefits of emerging technologies encourages schools to think differently about technology and its role in teaching. Students are also challenged to investigate new ways of learning. Besides, hands-on time allows faculty and students to explore and use new technology as they think about ways it can help them solve instructional problems

Cybersecurity Risk Preparedness for Emerging Technologies

Cybersecurity risk preparedness is the practice of identifying potential risks and vulnerabilities, assessing the impacts and likelihood of those risks, and mitigating the consequences if the risks become reality. With today's dynamic emerging educational technologies, the security landscape demands that every learning institution, no matter its size, develops and implements a cybersecurity risk preparedness plan. Investing time and resources in creating a cybersecurity risk preparedness plan illustrates that the institution recognizes that no one is immune to falling victim to a cyber-attack. A cybersecurity preparedness plan for emerging technologies requires that the school carries out a cybersecurity assessment and then develops a cybersecurity guideline that covers its needs comprehensively.

Cybersecurity assessments

1. **Take stock of the school's most valuable digital assets:** The first thing to do is to identify the various assets that could be targeted by cybercriminals. These assets might include computers, systems, networks, or data. You will want to understand which of these assets criminals might want to target, which are most at risk of being targeted, and which might not be secure. If the thought of it being breached keeps you up at night, put it on your list.

Figure 1: Cybersecurity assessment (audit) from Pradeepagrawal

2. **Identify the risks, past and present:** Once you have identified the assets you need to protect, you will need to identify the risks that could affect those assets. You will probably look at the risks associated with every threat that can affect your school, from unintentional ones like losing your mobile device to Ransomware attacks. Every potential threat, including new and emerging risks, should be identified.

   You may also want to do a historical analysis of past cyber risks, attacks, and breaches, which will give you a window into your current risks. Any attack you have experienced in the past can offer you valuable information. In addition to giving you information about how attackers accessed your systems in the past, it will also shed light on the ways your team responded to those breaches at the time.
3. **Plan for an attack:** If a teacher or a student clicks a link and your school's data is held to ransom, how will your institution respond? Part of mitigating risk is having a well-thought-out plan in advance. If you have to respond to an attack on the fly, you may not make the best decisions.
4. **Review your controls**: You may already have controls in place to prevent the risks you have identified or to respond to attacks if they occur. Review the controls you have in place to make sure they adequately cover your current risks. Continuous monitoring is important because the risk landscape is constantly changing

and your controls should change to effectively protect your assets.

Creating a Cybersecurity Preparedness Plan

A cybersecurity preparedness plan is a series of events defining the best practices an organization follows to manage its cybersecurity risk. Such a plan reduces the company's exposure to vulnerabilities. Every day, learning institutions of all sizes face the challenge of ensuring the security of their critical systems and data. To help address these challenges, a school needs a strategic, well-thought cybersecurity plan to protect its critical infrastructure and information systems.

Figure 2: Cybersecurity Frameworks from Twitter

There are several cybersecurity plans like the National Institute of Standards and Technology (NIST) and, ISO 27002. When applied properly, a cybersecurity plan enables IT, administrators, to manage their institution's cyber risks more intelligently. A school can adapt an existing cybersecurity plan to meet its own needs or develop one internally.

Core components of a cybersecurity plan

Every cybersecurity plan is different. Thus, each describes core components in its own way. That said, they're all built on similar principles, and they are used to achieve similar cybersecurity goals. While a specific cybersecurity plan goes into far greater detail in how it is constructed and designed, it loosely revolves around a continuous life-cycle process consisting of the following four key stages.

Figure 3: Core components of a cybersecurity plan from controleng

1. **Identify and document cybersecurity goals.** This component is used to identify the cybersecurity goals an educational institution wants to achieve. Identified goals will be different for each school. They are mostly dependent on the business's level of cybersecurity competency, overall business intent, and whether the school must meet specific goals due to regulatory requirements.

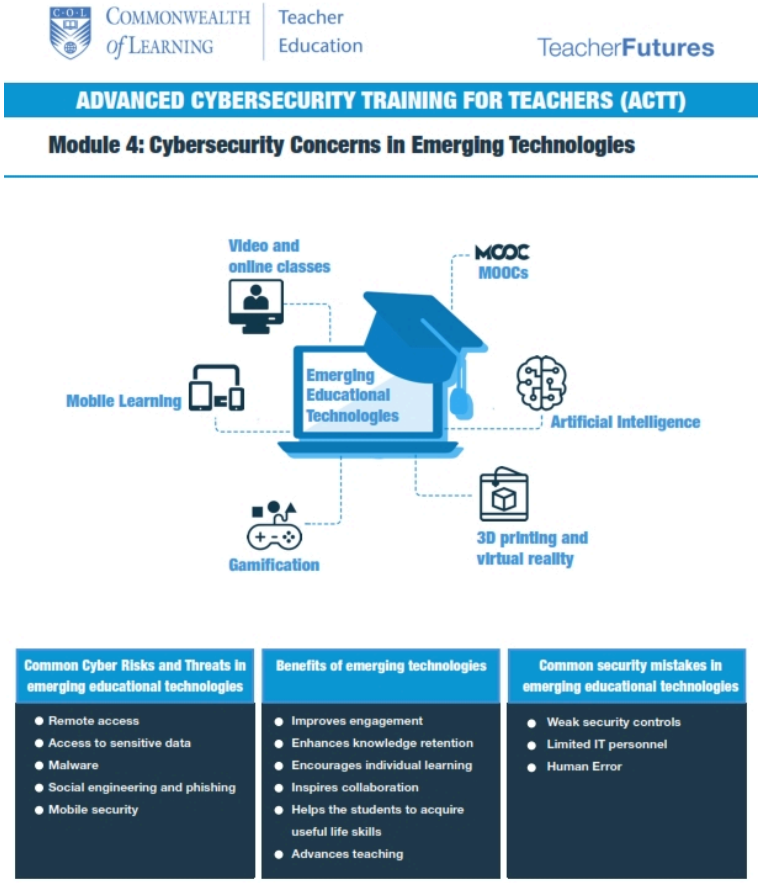
2. **Set guidelines designed to achieve cybersecurity goals**. In this stage of a cybersecurity plan, a detailed list of functions, processes, and actions are created that serve to achieve the goals outlined in the identification stage. This stage should also contain steps

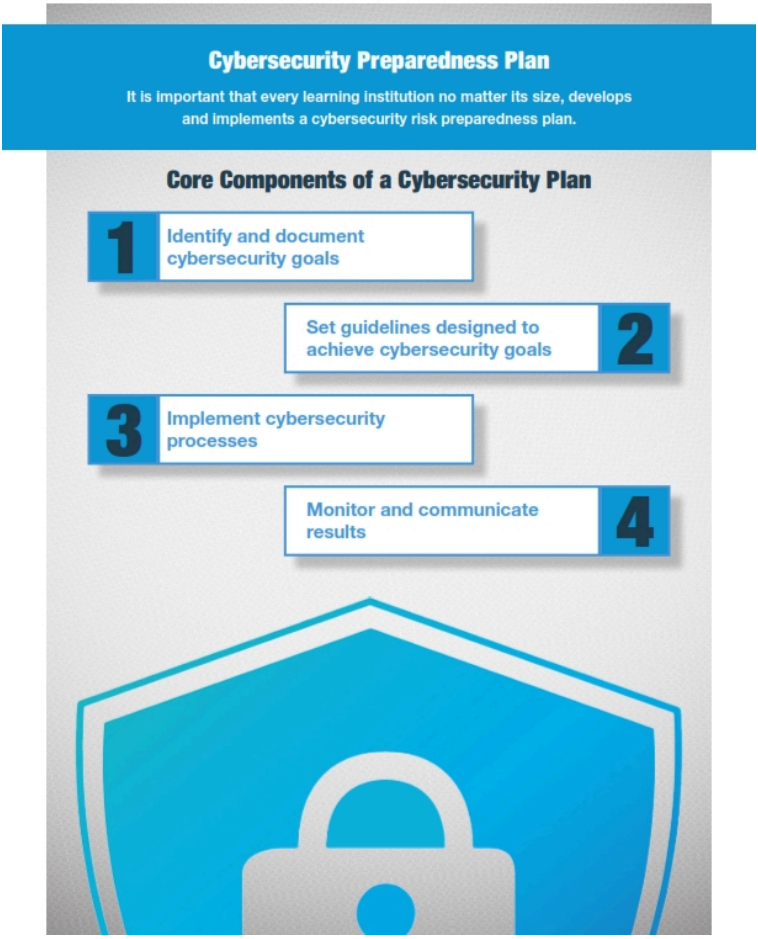
to prioritize goals and define roles and responsibilities for each defined objective.

3. **Implement cybersecurity processes.** This is the action stage of the plan, where each goal is implemented within the school infrastructure. Communication is crucial in this stage as applied cybersecurity processes often involve multiple areas or departments.

4. **Monitor and communicate results.** Lastly, the implemented objectives are monitored, documented, and reviewed to ensure the cybersecurity plan processes are effective. Results are appropriately communicated to the school, and steps are taken to continuously improve existing processes and objectives.

Module 4 Summary Infographic




Cybersecurity Preparedness Plan
It is important that every learning institution no matter its size, develops and implements a cybersecurity risk preparedness plan.
Core Components of a Cybersecurity Plan
1
Identify and document cybersecurity goals
Set guidelines designed to achieve cybersecurity goals
2
3
Implement cybersecurity processes
Monitor and communicate results
4

Module 4 Files and Resources

/wp-content/uploads/23/2023/06/Week-4-Benefits-of-Emerging-Thechnologies.pdf

/wp-content/uploads/23/2023/06/Week-4-Cybersecurity-Risk-Preparedness-for-Emerging-Technologies.pdf

/wp-content/uploads/23/2023/06/Week-4-Cybersecurity-Risks-in-Emerging-Technologies.pdf

/wp-content/uploads/23/2023/06/Week-4-What-Are-Emerging-Technologies.pdf