



NATIONAL CYBERSECURITY CHALLENGE

CONTENT FOR SCHOOLS – 2024

Contents

MODULE 1 - GENERAL IT & CYBERSECURITY KNOWLEDGE	5
Popular Cybersecurity Vulnerabilities (OWASP Top Ten)	5
Common Ports and Services	5
General Knowledge	6
Terminologies.....	7
MODULE 2 - CAREER OPPORTUNITIES IN CYBERSECURITY	10
Governance Risk and Compliance (GRC)	10
Cybersecurity Threat Intelligence	11
Security Architecture	11
User Education	12
Security Operation	13
Application Security	14
Enterprise Risk Management (ERM)	15
Descriptions of some common cybersecurity job roles	16
MODULE 3- Online Activities and Associated risk	21
Background.....	21
The Online Risk Landscape	21
Types of threat actor	23
Online Privacy issues	24
TOP REPORTED INCIDENTS	25
Online Shopping Scams	26
Mobile Payment Services Fraud	27
Courier Service Scams	27
Romance Scams	27
Shopping Fraud	27
Phishing Scams	27
Lottery and Prize Scams	27
Charity Scam	27
Recommendations	27
WhatsApp Account Takeover	28
Sextortion (Sexual Extortion).....	28
Preventive & Mitigation Measures	29

Countering Account Takeovers: Enable 'Two-Step Verification'	29
Avoiding Sexual Extortion Schemes.....	29
Recommendations	29
MODULE 4-INTERNET AND ONLINE SAFETY	30
Introduction	30
2. Staying Safe from Online Predators	32
3. Cybersecurity Cybercrime Incident Reporting Points of Contact	33
4.0 Cyberbullying and Cyber harassment	33
5. Using social media Safely.	34
Privacy Settings for some Social Media Accounts	35
MODULE 5- MOBILE DEVICE SAFETY	40
Introduction and Overview	41
Kinds of Sensitive Data Stored on Mobile Devices	42
Threats to Mobile Devices	42
Securing Mobile Devices	43
Measures that parents can take to protect their children's mobile devices	44
Mobile Security Hacking and Terminologies	45
MODULES 6- SOCIAL ENGINEERING	47
1. What is Social Engineering?	47
The Objective of Social Engineering Attackers	47
Traits of Social Engineering Attacks	47
Types of Social Engineering Attack	47
Stages of Social Engineering	51
How to Spot Social Engineering Attacks	51
How to Prevent Social Engineering Attacks	52
MODULE 8- COP LEGAL	54
1. Indecent image or photograph of a child	54
2. Penalty for indecent image or photograph of a child	54
3. Meaning of publication of indecent image or photograph of a child	54
4. Includes a material image, visual recording, video, drawing or text that depicts: .54	
5. Dealing with a child for purposes of sexual abuse	55
6. Penalty for dealing with a child for purposes of sexual abuse	55
7. Aiding and abetting of child dealing for purposes of sexual abuse	55

8. Cyberstalking of a child.....	56
9. Sexual extortion	56
10. Meaning of Intimate Image.....	56
11. Penalty	56
12. Objective of CRC General Comment 25.....	57
13. General principles	57
14. Right to Non-Discrimination	57
15. Ways in which children can be discriminated.	57
16. Best interest of the child.....	58
17. Right to life, survival, and development	58
18. Respect for the views of the child	58
19. Civil rights and freedoms.....	58
20. Access to information	58
23. Right to privacy.....	59
24. Violence against children.....	59
25. Right to education.....	60

Module 1

MODULE 1- GENERAL IT & CYBERSECURITY KNOWLEDGE

MODULE 1 – BASIC CONCEPTS IN CYBERSECURITY

INTRODUCTION TO CYBERSECURITY

What is Cybersecurity?

Cybersecurity refers to the practice of protecting systems, networks, and programmes from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

Cybersecurity comprises people, technologies, and processes working together to protect networks, computers, programmes, and data from attack, damage, or unauthorised access. Cybersecurity is also the protection of internet-connected systems, including hardware, software, and data, from cyberattacks. It is made up of two words: cyber and security.



Figure 1: Describes what cybersecurity is – securing all devices and systems connected to the internet or networks (Laptops, the cloud, workstations, mobile devices, tablets, servers etc.)

Terminology

- Cyber: Refers to the technology encompassing systems, networks, and programmes or data.
- Security Pertains to the protection of these systems, networks, and programmes from cyber threats.
- Cyberspace: The environment where communication over computer networks occurs. It includes all online digital spaces where information is stored and exchanged.

Key Components of Cybersecurity

Cybersecurity is a complex ecosystem that requires a multi-layered approach to effectively protect information systems, networks, and data. Here's a breakdown of the three essential components and how they work together:

1. People (The Human Element)

People play a crucial role in both strengthening and weakening cybersecurity. Here's how

the human factor comes into play:

- **User Behaviour:** Individual actions significantly impact cybersecurity. This includes creating strong passwords, being cautious about email attachments and links, and reporting suspicious activity. For example, you receive an email claiming you have won a prize from your favourite online game, but it asks your login details. You avoid clicking the link, show the email to your parent, verify if it is a scam, and report the email to the online game platform, this is a user behaviour to protect your account.
- **Cybersecurity Professionals:** These specialists possess the knowledge and skills to design, implement, and maintain security measures. They include security analysts, ethical hackers, and incident responders.
- **Training and Awareness Programmes:** Educating users about cybersecurity threats and best practices is essential. Training programmes can help employees recognise phishing attempts, avoid malware, and understand their role in maintaining a secure environment.
- For example, you attend a cybersecurity workshop where you learn about the dangers of phishing scams and how to recognise suspicious emails. A week later, you receive a message claiming to be from your favourite restaurant, asking for personal information. You remember the training, identify it as a phishing attempt, avoid clicking the link, and report it to a teacher.

2. Technologies (The Tools of the Trade)

Technology plays a vital role in protecting your digital assets. Here are some key security technologies:

a. Firewalls:

- **Hardware Firewalls:** Physical devices that filter traffic to protect networks from unauthorised access (e.g., Cisco ASA (Adaptive Security Appliance)).



Figure 2: Cisco ASA

- **Software Firewalls:** Applications installed on devices to monitor and control network traffic (e.g., Windows Firewall).

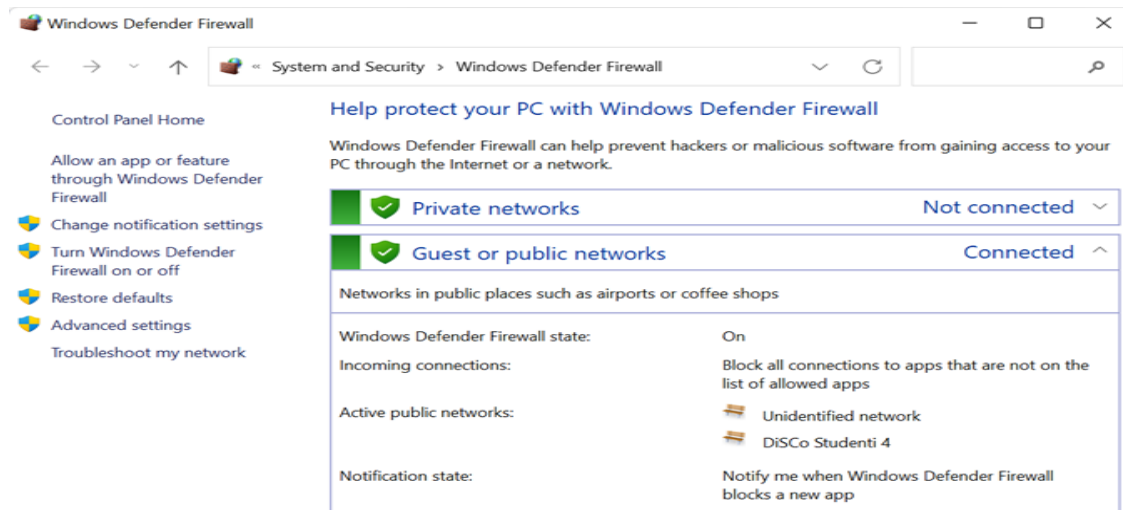


Figure 3: Windows Defender Firewall

b. Intrusion Detection/Prevention Systems (IDS/IPS):

- **Hardware IDS/IPS:** Devices monitoring network traffic to detect and prevent threats (e.g., Cisco Secure IPS).



Figure 4: Cisco Secure IPS – a traditional device powered by Talos.

- **Software IDS/IPS:** Software solutions installed on network infrastructure to identify and block malicious activities (e.g., Snort IDS).

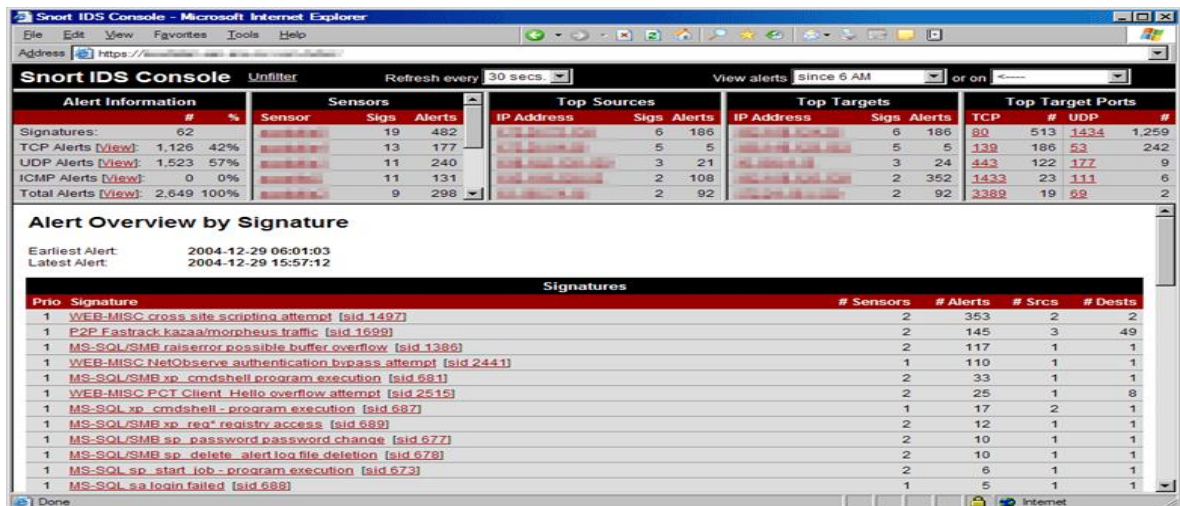


Figure 5: Snort IDS

c. Endpoint Security Solutions:

- **Software Solutions:** Applications protecting end-user devices from malware and unauthorised access (e.g., Symantec Endpoint Protection).
- **Hardware Solutions:** Devices like hardware tokens for multi-factor authentication (e.g., RSA SecurID).

d. Other Software Solutions

- **Antivirus Software:** Protects against malware by scanning files and systems for malicious activity (e.g., McAfee).
- **Encryption Software:** Secures data by converting it into a coded format, ensuring confidentiality and integrity (e.g., VeraCrypt).
- **Security Information and Event Management (SIEM) Systems:** Aggregate and analyse security data to provide a comprehensive view of an organisation's security posture and support real-time threat detection (e.g., Splunk).

3. Processes: The Roadmap for Security

Defined processes ensure consistent application of security practices. Here are some essential cybersecurity processes:

- **Risk Management:** Identifying, analysing, and prioritising potential threats to your systems and data. This allows for the allocation of resources to address the most critical risks. For instance, to manage the risk of a data breach, the school conducts regular assessments to identify vulnerabilities in its IT systems and infrastructure. Based on these assessments, the school implements measures such as software updates, password policies, and data encryption to mitigate potential risks. Additionally, staff and students receive training on cybersecurity best practices, and the school develops an incident response plan to effectively address and contain any security breaches that may occur, ensuring the safety and integrity of sensitive information.
- **Incident Response:** Having a plan to react to a cyberattack is crucial. This includes procedures for detection, containment, eradication, and recovery. Following the detection of suspicious network activity indicating a potential cyberattack, the school's IT team swiftly

identifies and contains the threat to prevent further damage. They isolate affected systems and initiate measures to eradicate the threat, such as running antivirus scans and applying security patches. Once the threat is neutralised, the team focuses on restoring normal operations using data backups and conducts a thorough review to identify lessons learned and improve future incident response protocols.

- **Vulnerability Management:** Regularly scanning systems and software for vulnerabilities and patching them promptly is essential to prevent attackers from exploiting weaknesses. Vulnerability management involves regularly assessing and addressing weaknesses in network and systems to prevent potential security breaches. For instance, if a critical vulnerability is discovered in the student information system (SIS) software, the IT team swiftly prioritises and applies patches provided by the vendor to mitigate the risk of unauthorised access to sensitive student data. Continuous monitoring and periodic vulnerability assessments help ensure the school's information systems remain secure and resilient against emerging threats.
- **Security Policy Development:** Creating and enforcing clear policies that outline acceptable user behaviour, data handling practices, and access controls are crucial. In developing security policies for a school, the administration collaborates with IT professionals and stakeholders to establish guidelines and procedures for protecting sensitive information and ensuring a secure learning environment. This may include policies on data protection, acceptable use of technology, password management, and incident response protocols. Regular review and updating of these policies in accordance with evolving cybersecurity threats and regulatory requirements are essential to maintaining effective security measures within the school.

Importance of Cybersecurity

In today's digital age, cybersecurity is critically important for several reasons:

- **Protection of Sensitive Data:** With the increasing amount of data being generated and stored online, protecting sensitive information such as personal details, financial records, and intellectual property is crucial. Cybersecurity measures help prevent unauthorised access, data breaches, and theft, thereby safeguarding individuals' privacy and organisations' valuable information.
- **Maintaining Business Continuity:** Cyberattacks can disrupt business operations, leading to significant downtime and financial losses. By implementing robust cybersecurity practices, organisations can ensure business continuity, minimise disruptions, and maintain customer trust. Effective cybersecurity also includes disaster recovery and business continuity planning to quickly restore normal operations after an attack.
- **Preventing Financial Loss:** Cyberattacks can result in substantial financial losses due to ransom payments, theft of financial data, and the costs associated with responding to and recovering from breaches. Strong cybersecurity measures help protect against these financial risks by preventing attacks and reducing the impact of any breaches that do occur.
- **Protecting National Security:** Critical infrastructure such as power grids, water supply systems, and transportation networks are increasingly dependent on digital systems. Cyberattacks on these systems can have severe consequences for national security and public safety. Governments and organisations must prioritise cybersecurity to protect these

vital services from potential threats.

- **Compliance with Regulations:** Many industries are subject to regulations that require the protection of sensitive data. Compliance with laws such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), the Data Protection Act, 2012 (Act 843), the Cybersecurity Act, 2020 (Act 1038) and the Directive for the Protection of Critical Information Infrastructure are essential to avoid legal penalties and ensure the protection of data. Implementing robust cybersecurity practices helps organisations meet these regulatory requirements and avoid costly fines.
- **Mitigating Evolving Threats:** Cyber threats are constantly evolving, with cybercriminals developing more sophisticated methods to exploit vulnerabilities. Cybersecurity helps organisations stay ahead of these threats by implementing up-to-date security measures, conducting regular security assessments, and fostering a culture of continuous improvement in security practices.
- **Enhancing Customer Trust:** Consumers are increasingly concerned about the security of their personal information. Organisations that demonstrate a strong commitment to cybersecurity can build trust with their customers, enhancing their reputation and competitive advantage. This trust is crucial for customer retention and the long-term success of the business.
- **Supporting Economic Stability:** Cybersecurity is essential for the stability of the global economy. Cyberattacks can disrupt financial markets, erode consumer confidence, and impact the overall economic health. By protecting digital assets and infrastructures, cybersecurity contributes to the stability and resilience of the economy.

Overview of the Cybersecurity Threat Landscape

The cybersecurity threat landscape is constantly evolving, posing significant challenges to individuals, businesses, and governments. It encompasses a wide range of threats, from malware and phishing attacks to advanced persistent threats and insider risks. Cybercriminals are employing increasingly sophisticated techniques, exploiting vulnerabilities in systems, and leveraging social engineering to achieve their malicious goals.

Understanding the diverse nature of these threats is crucial for developing effective cybersecurity strategies. Each type of threat requires specific defensive measures and awareness to mitigate risks.

Further exploration of these threats, including detailed descriptions and defense mechanisms, will be provided in subsequent modules.



Figure 6: A capture of what the cyber threat landscape looks like – Facilitators can show students a live threat map (<https://cybermap.kaspersky.com/>)

CYBERSECURITY PRINCIPLES

1. Confidentiality, Integrity, and Availability (CIA Triad)

The CIA Triad is the foundational model for understanding and implementing cybersecurity measures. It provides a simple and complete checklist for evaluating an organisation's security. An effective IT security system consists of three parts: confidentiality, integrity, and availability, hence the name "CIA triad."

- The CIA triad provides a high-level framework for cybersecurity professionals to consider when auditing, implementing, and improving systems, tools, and programmes for organisations. It is a powerful way to identify weak points and form solutions to strengthen policies and programmes.



Figure 7: CIA Triad

- Confidentiality:** Confidentiality ensures that sensitive information is accessible only to

those authorised to view it. It involves protecting sensitive data, private and safe from unauthorised access. This includes protecting information from bad actors with malicious intent, as well as limiting access to only authorised individuals within an organisation. Think of confidentiality as privacy. Ensuring confidentiality includes implementing data encryption, two-factor authentication, biometric verification, and security tokens. Imagine your diary is like a secret vault where you keep your thoughts, dreams, and feelings safe. Just like you wouldn't want anyone peeking into your diary without permission, confidentiality means keeping certain information private and only sharing it with trusted people. In school, confidentiality might mean keeping your personal details, like your grades or medical information, between you, your teachers, and your parents, ensuring that your privacy is respected, and your secrets are kept safe.

- **Integrity:** Integrity involves maintaining the accuracy and consistency of data over its lifecycle. It involves ensuring that data is accurate and not altered by unauthorised users. Data accessed internally and externally must maintain integrity so that stakeholders (customers, employees, etc.) can trust the organisation. A system with integrity keeps data safe from unnecessary changes, whether malicious or accidental. Cybersecurity professionals implement access levels, enable tracking when making changes, and protect data when transferring or storing it. Ensuring integrity includes implementing cryptographic checksums, file permissions, uninterrupted power supplies, and data backups. For instance, think of your favourite video game where you earn points by completing tasks and challenges. Integrity is like ensuring that those points are earned fairly and are not tampered with by cheats or hacks. In school, cybersecurity integrity means making sure that your online accounts and grades are accurate and secure, so you can trust that your hard work and achievements are protected from unauthorised changes or manipulation.
- **Availability:** Availability ensures that information and resources are accessible to authorised users when needed. It also refers to the idea that people who need access to data can get it without affecting its confidentiality or integrity. Ensuring availability in data systems can be tricky because it may compete with the other factors in the triad. One of the best ways to protect data is to limit access to it. If you have an information security role, you may experience pushback from customers or coworkers about information availability. Ensuring availability includes implementing data backups, firewalls, backup power supplies, and data redundancy. For instance, imagine you need to access your online homework, but the website is down, and you cannot access it. Availability means making sure that important websites and online resources are always accessible when you need them. In school, this ensures that you and your classmates can reliably access study materials, submit assignments, and participate in online classes without interruptions.

2. Authentication, Authorisation, and Accountability (AAA)

The AAA framework is critical for managing and securing access to network resources and services:

- **Authentication:** Authentication is the process of verifying the identity of a user or device. For example, a company might use multi-factor authentication (MFA) for its employees, requiring them to provide a password, a fingerprint scan, and a one-time code sent to their mobile phone to access the company's internal systems.

For example, to access your school's online learning portal, students and teachers must log in using their unique usernames and passwords. To enhance security, the school

implements Two-Factor Authentication (2FA). After entering your password, you receive a verification code on your mobile phone, which you must enter to complete the login process. This additional step ensures that only authorised individuals can access the portal, protecting sensitive educational materials and personal information.

Imagine entering a secret study group that only you and your friends can access. To get in, you might need to say a special password that only members know. In the same way, when you log into your school email or online classes, you use a username and password to prove you are who you say you are, ensuring that only you can access your personal information and schoolwork.

- **Authorisation:** Authorisation determines what an authenticated user is allowed to do. For instance, in an online banking system, once a customer is authenticated, they may be authorised to view their account balance but not authorised to access the bank's administrative functions. Role-Based Access Control (RBAC) is commonly used to assign specific permissions to users based on their roles within the organisation.

For example, in your school's online grading system, teachers have different levels of access based on their roles and responsibilities. Administrators can create and delete accounts, while teachers can only view and update grades for their assigned classes. Students, on the other hand, can only view their own grades. This system ensures that each user is granted appropriate access privileges, preventing unauthorised individuals from altering sensitive academic data. Imagine your school library has different sections: one for everyone, one for teachers, and one for librarians. You can only enter the sections you are allowed to visit. Similarly, authorisation means that once you log into a system, you can only access the parts you are permitted to see or use. For instance, students can access their own grades and assignments, while teachers can access the entire class's information.

- **Accountability:** Accountability ensures that actions taken by users can be traced back to them. For example, an organisation implements logging and monitoring systems that record user activities on the network, providing an audit trail that can be reviewed in case of a security incident. This helps in detecting and investigating unauthorised activities and ensuring compliance with security policies.

For example, in a school, each teacher is responsible for maintaining accurate attendance records for their classes. To ensure accountability, the school implements a system where teachers electronically record attendance at the beginning of each class. Additionally, the system logs the timestamp and the teacher's username for each entry. If there are discrepancies or questions about attendance, administrators can review the electronic records to identify who took attendance and when, promoting transparency and accountability in the school's operations. Imagine you borrowed a book from the library, and your name is recorded so everyone knows who has it. Accountability is similar; it means that actions taken on a computer or online system are tracked and linked to specific users. In school, this could mean that if someone changes a grade or deletes a file, the system keeps a record of who did it, ensuring that everyone is responsible for their actions and can be held accountable if something goes wrong.

3. Least Privilege Principle

The Principle of Least Privilege (PoLP) dictates that users and systems should have the minimum level of access necessary to perform their functions. Here's how it's implemented:

- **Role-Based Access Control (RBAC):** In an organisation, different roles such as 'employee,' 'manager,' and 'administrator' are created, each with specific access permissions. For example, an employee might only have access to their own work files, while a manager can access the files of their team members, and an administrator can manage system-wide settings.

For example, the IT administrator holds the highest level of access, with permissions to manage user accounts and network infrastructure. Teachers are granted access to the school's learning management system (LMS), enabling them to create course materials and assess student progress, while students have limited access to their own course materials and grades. Parents or guardians have a separate portal to monitor their child's academic performance. This way, everyone has just the right amount of access they need to do their job, keeping everything secure and organised.

- **Access Control Lists (ACLs):** ACLs specify which users or systems are granted access to particular resources. For example, a file server might have an ACL that allows read and write access to a specific file for the finance team but restricts access to other departments.

An example, your school has a list of rules for who can enter different areas: students can go to the library, but only teachers can enter the staff room. Access Control Lists (ACLs) work similarly but for computers. For instance, ACLs determine which websites students can visit on school computers or which files they can access on shared drives. This helps keep everyone's digital activities safe and organised, just like the rules at school keep things running smoothly.

- **Periodic Access Reviews:** Regularly reviewing and adjusting access rights ensures they remain appropriate. For instance, an organisation conducts quarterly reviews to ensure that employees who have changed roles or left the company no longer have access to sensitive data and systems.

For instance, your school had a "clean-up day" where everyone checks their lockers and desks to make sure they only have what they need. Periodic Access Reviews are like those clean-up days, but for digital accounts and systems. For example, the school's IT team might regularly review who has access to certain online resources, ensuring that only current students and staff can use them and that no one has access they shouldn't. This helps keep everything organised and secure, just like tidying up your physical space.

4. Defense in Depth

Defense in Depth is a cybersecurity strategy that employs multiple layers of security controls and measures to protect information and systems from a wide range of threats. The core idea is that if one layer of defense is compromised, additional layers will continue to protect the system. This approach mitigates the risk of a single point of failure and enhances the overall security posture of an organisation.

An example of defense in depth used in securing your school. Defense in Depth is exemplified through a multi-layered approach to security to protect against intruders, a fence, strong locks, steel doors and windows, a safe room, security cameras, and motion sensors. The school's perimeter fence serves as the first line of defense, deterring

potential intruders from accessing the property. A security guard on the school's compound. A comprehensive security system with motion sensors and cameras adds another layer of protection by detecting and alerting the security guard of any suspicious activity. Strong locks and steel doors and windows further fortify the interior of the school, making it difficult for intruders to gain entry. Finally, a safe room provides a secure retreat in the event of a security breach, ensuring their safety until help arrives.

For instance, your online accounts might require a password, a security question, and a fingerprint scan, making it much harder for someone to access them without permission. This way, even if one layer of security is breached, there are still others keeping your information safe.

Key Components of Defense in Depth

- **Physical Security:** Measures to prevent physical access to critical infrastructure, such as security guards, locked doors, biometric access controls, and surveillance cameras.
- **Network Security:** Controls to protect the integrity, confidentiality, and availability of network data. Examples include firewalls, intrusion detection and prevention systems (IDS/IPS), and virtual private networks (VPNs).
- **Endpoint Security:** Protections for devices that connect to the network, such as computers, smartphones, and IoT devices. This includes antivirus software, endpoint detection and response (EDR) tools, and regular software updates and patches.
- **Application Security:** Ensuring that applications are secure against attacks. This involves secure coding practices, regular vulnerability assessments, and application firewalls.
- **Data Security:** Safeguards to protect data at rest and in transit through encryption, access controls, and data masking.
- **User Education and Awareness:** Training programmes to educate users about security best practices, phishing, social engineering, and other common threats.
- **Administrative Controls:** Policies and procedures that govern security practices, including incident response plans, access management policies, and compliance with regulations and standards.

Examples of Defense in Depth

Consider an online retail company implementing defense in depth to secure its e-commerce platform:

- **Physical Security:** The company secures its data centres with biometric access controls, surveillance cameras, and security personnel. Only authorised personnel can access the server rooms.
- **Network Security:** The company deploys firewalls to filter incoming and outgoing traffic, ensuring only legitimate traffic passes through. Intrusion detection and prevention systems (IDS/IPS) monitor network activities for signs of malicious behaviour.
- **Endpoint Security:** All employee computers and servers have antivirus software installed and are regularly updated with security patches. Endpoint detection and response (EDR) tools monitor for suspicious activity and respond to threats in real time.
- **Application Security:** The company's development team follows secure coding practices to minimise vulnerabilities in their software. Regular code reviews, penetration testing, and the use of web application firewalls (WAFs) help protect against application-level attacks.

- **Data Security:** Customer data is encrypted both at rest and in transit. Access to sensitive data is restricted based on Role-Based Access Control (RBAC), ensuring only authorised employees can view or modify the data.
- **User Education and Awareness:** Employees undergo regular training to recognise phishing attempts and understand the importance of strong passwords and other security practices. Simulated phishing attacks help reinforce this training.
- **Administrative Controls:** The company has a comprehensive incident response plan in place, detailing the steps to take in the event of a security breach. Regular audits ensure compliance with industry regulations such as the Directive for the Protection of Critical Information Infrastructure, Data Protection Act, 2012, or Payment Card Industry Data Security Standard (PCI DSS).

CYBERCRIME

Definition of Cybercrime

Computer crime, or cybercrime, is any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may have been the target. Cybercrime could be internal or external to an organisation. Cybercrime is categorised into two types:

- **Insider Attack:** is an attack to the network or computer system by some person (employee, third party personnel, etc.) with authorised system access. It is generally performed by dissatisfied or unhappy inside employees or contractors for revenge or greed.

For example, a student shared their password with a friend, who then logged into their account and changed their grades without permission. This would be an insider attack, where someone who should have access to the system misuses it for their own gain. Similarly, an insider attack occurs when someone with authorised access, like a student or staff member, intentionally or unintentionally abuses their privileges to harm the school's digital systems or steal information.

- **External Attack:** This attack originates from outside the organisation by scanning or gathering information about the organisation. The attacker is either hired by an insider or an external entity.

For example, someone from another school trying to break into your school's computer system to change grades or steal personal information. This would be an external attack, where someone outside the school tries to harm its digital systems. Just like how you lock your front door to keep strangers out of your house, cybersecurity measures are put in place to prevent external attacks and keep your school's digital information safe from outside threats.

Cyberattacks can also be classified as structured attacks or unstructured attacks based on the level of maturity of the attacker.

- **Structured Attacks:** These types of attacks are performed by highly skilled and experienced people, and the motives for these attacks are clear. They have access to sophisticated tools and technologies that allow them to gain access to other networks without being detected.

For instance, a group of students working together to sneak into the school library after

hours by planning out every detail, like distracting the librarian and sneaking past security cameras. This would be a structured attack, where the students carefully plan and execute their actions to achieve their goal. Similarly, a structured attack occurs when hackers meticulously plan and coordinate their efforts to breach a computer system, exploiting vulnerabilities and using sophisticated techniques to gain unauthorised access or steal sensitive information.

- **Unstructured Attacks:** These attacks are generally performed by amateurs who do not have any predefined motives to perform the cyberattack. Usually, these amateurs try to test a tool readily available over the internet on the network of a random company.

For instance, someone randomly trying different passwords to break into your online accounts without any specific plan or strategy. This would be an unstructured attack, where the attacker acts impulsively without careful planning. Similarly, an unstructured attack occurs when hackers use simple and opportunistic methods, like phishing emails or malware, to exploit vulnerabilities in computer systems without a detailed plan, posing a threat to the security of digital information.

.

Cyberwarfare

Cyberspace has become another important dimension of warfare, where nations can carry out conflicts without the clashes of traditional troops and machines. This allows countries with minimal military presence to be as strong as other nations in cyberspace.

Cyberwarfare is an Internet-based conflict that involves the penetration of computer systems and networks of other nations. These attackers have the resources and expertise to launch massive Internet-based attacks against other nations to cause damage or disrupt services, such as shutting down a power grid.

For instance, two rival schools (nations) competing in a big sports event. Now, imagine if instead of playing fair, one school secretly sent spies to sabotage the other team's practices and steal their playbook. This would be like cyber warfare, where countries or groups use digital weapons like malware or hacking to disrupt or spy on each other's computer systems, aiming to gain an advantage or cause harm without direct physical conflict. Just like in sports, cyber warfare involves strategic planning, tactics, and sometimes even espionage to outsmart the opponent.

Key aspects of cyber warfare include:

- **Espionage:** Stealing confidential information and intelligence from government agencies, military organisations, or private enterprises. For example, the infamous Stuxnet worm, believed to be developed by the United States and Israel, was used to sabotage Iran's nuclear programme by targeting its industrial control systems.
- **Sabotage:** Disrupting critical infrastructure such as power grids, water supply systems, and communication networks. For instance, the 2015 cyberattack on Ukraine's power grid caused widespread power outages and highlighted the potential for cyber warfare to impact national infrastructure.

- **Propaganda and Psychological Operations:** Spreading misinformation/disinformation or propaganda to influence public opinion or destabilize societies. The use of social media platforms to spread fake news and manipulate election outcomes is a prominent example of this tactic.

Cost of Cybercrimes to Businesses and Nations

The financial and economic impact of cybercrime is substantial, affecting businesses, individuals, and nations on a global scale. The costs associated with cybercrime include direct financial losses, recovery expenses, legal liabilities, and reputational damage.

For Businesses:

- **Financial Losses:** Cyberattacks can lead to significant financial losses due to theft of funds, data breaches, and operational disruptions. Apparently, in 2023, cyber fraud activities led to direct financial losses of (GH¢59.7m) in Ghana, according to Business Insider Africa, quoting the Director-General of Ghana's Cyber Security Authority (CSA), Dr. Albert Antwi-Boasiako.
- **Recovery and Remediation:** Expenses related to incident response, system repairs, and recovery efforts can be substantial. Businesses may need to invest in new security measures, hire cybersecurity experts, and conduct extensive audits to prevent future attacks.
- **Legal and Regulatory Penalties:** Companies that fail to protect customer data can face severe penalties under data protection regulations such as the General Data Protection Regulation (GDPR) and the Cyber Security Act. For example, British Airways was fined £20 million (GH¢290m) for a data breach that exposed the personal information of over 400,000 customers.
- **Reputational Damage:** Loss of customer trust and damage to brand reputation can have long-term consequences for businesses. Customers are less likely to do business with companies that have suffered high-profile data breaches, leading to loss of revenue and market share.

For Nations:

- **Economic Impact:** Cybercrime can have a significant impact on national economies. A report by McAfee estimated that the global cost of cybercrime reached \$600 billion annually in 2018. This includes losses from intellectual property theft, financial crime, and damage to business operations.
- **National Security:** Cyberattacks on critical infrastructure such as power grids, transportation systems, and communication networks can compromise national security and public safety. Governments must invest heavily in cybersecurity measures to protect against such threats.
- **Costs of Cyber Defense:** Nations must allocate substantial resources to cybersecurity initiatives, including the development of advanced defense systems, cybersecurity training programmes, and international collaboration to combat cyber threats. For instance, the U.S. government's cybersecurity budget for 2020 was over \$17 billion, reflecting the growing importance of defending against cyber threats.
- **Political and Social Impact:** Cybercrime can also have political and social ramifications, such as undermining public confidence in governmental institutions and electoral processes. The interference in the 2016 U.S. presidential election through cyber means is a notable example of the potential political impact of cybercrime.

Popular Cybersecurity Vulnerabilities (OWASP Top Ten)

- a. **Broken Access Control:** This vulnerability occurs when an application does not properly restrict user access to sensitive information or functionality. Attackers can exploit this vulnerability to gain access to unauthorized features or data.
- b. **Cryptographic Failures:** This vulnerability occurs when an application fails to properly implement cryptographic algorithms such as DES, AES, integrity checkers (MD5), Browser Standard like TLS 1.3 or use them in an insecure manner, leading to sensitive data being exposed or becoming vulnerable to attack.
- c. **Injection:** This vulnerability occurs when an application does not properly sanitize user input, allowing an attacker to inject malicious code or commands into the application's backend systems.
- d. **Insecure Design:** This vulnerability occurs when an application is designed in a way that leaves it open to attack. It can be caused by poor coding practices, weak security controls, or lack of proper security testing.
- e. **Security Misconfigurations:** This vulnerability occurs when an application or its components are configured improperly, making them vulnerable to attack. Examples include weak passwords, default accounts, and unnecessary services running on servers.
- f. **Vulnerable and Outdated Components:** This vulnerability occurs when an application uses outdated or vulnerable third-party components, which can be exploited by attackers to gain access to sensitive data or systems.
- g. **Identification and Authentication Failures:** This vulnerability occurs when an application does not properly authenticate users or identify them before granting access to sensitive data or functionality.
- h. **Software and Data Integrity Failures:** This vulnerability occurs when an application does not properly validate user input or ensure the integrity of its data, allowing attackers to manipulate or tamper with it.
- i. **Security Logging & Monitoring Failures:** This vulnerability occurs when an application does not properly log or monitor security events, making it difficult to detect and respond to attacks or security incidents.
- j. **Server-Side Request Forgery:** This vulnerability occurs when an attacker is able to trick an application into making requests to other internal or external systems, potentially allowing them to access sensitive information or execute unauthorized actions.

Common Ports and Services

- a. **HTTP (80):** Hypertext Transfer Protocol, used for accessing web pages.

- b. **HTTPS (443)**: Secure version of HTTP, used for secure web browsing and online transactions.
- c. **FTP (20, 21)**: File Transfer Protocol, used for uploading and downloading files.
- d. **SSH (22)**: Secure Shell, used for secure remote access and file transfers.
- e. **Telnet (23)**: Remote login service, used for accessing servers and network devices.
- f. **SMTP (25)**: Simple Mail Transfer Protocol, used for sending email messages.
- g. **DNS (53)**: Domain Name System, used for translating domain names into IP addresses.
- h. **DHCP (67, 68)**: Dynamic Host Configuration Protocol, used for assigning IP addresses to devices.
- i. **POP3 (110)**: Post Office Protocol, used for retrieving email messages.
- j. **IMAP (143)**: Internet Message Access Protocol, used for retrieving email messages.
- k. **SNMP (161, 162)**: Simple Network Management Protocol, used for monitoring and managing network devices.
- l. **MySQL (3306)**: Open-source relational database management system.
- m. **SMTP (587)**: Used for email message submission. It is an alternative to port 25, which is used for SMTP (Simple Mail Transfer Protocol) email delivery.

General Knowledge

Ghana Emergency Numbers

- a. Police – 191/18555
- b. Fire – 192
- c. Ambulance – 193
- d. Universal Emergency Hotline - 112
- e. Cyber Security Authority – 292
- f. National Security – 999

Ghana Short Codes

- a. Check status of SIM card registration - *400# (All networks)
- b. Check number of SIMs registered to a Ghana card - *402*1# (All networks)
- c. Check services that SIM is subscribed to- *175# (MTN), *463# (Vodafone), *100# (AirtelTigo)
- d. Deactivate call divert - ##21# (All networks)
- e. Deactivate call forwarding - ##61# (All networks)
- f. Report mobile money fraud – Send text message to 1515 (MTN), 100 (AirtelTigo), Call 100 or 0505555111 (Vodafone)

Terminologies

- b. **Artificial Intelligence:** refers to the development and deployment of computer systems or machines that can perform tasks that typically require human intelligence.
- c. **Architecture:** It is a term used for designing houses. In computer/IT terms, it can refer to the overall design and structure of a system or a software application. It encompasses the organization, components, relationships, and principles that define how the system operates, interacts, and fulfils its intended purpose.
- d. **Bitcoin:** Bitcoin is a decentralized digital currency that operates on a peer-to-peer network known as the blockchain. It was created in 2009 by an anonymous person or group of people using the pseudonym Satoshi Nakamoto. On June 7, 2021, the Department of Justice announced that it had seized approximately \$2.3 million worth of cryptocurrency.
- e. **Botnet:** A botnet is a network of compromised computers or devices that are under the control of a malicious actor or a botmaster. The term "botnet" is a combination of the words "robot" and "network," referring to the automated nature of the compromised devices
- f. **Common Vulnerability Scoring System (CVSS):** Is an industry standard for getting a numerical score to show users how secure (or not) a computer system, application or service is.
- g. **Distributed (Distributed Denial of service):** It is a type of cyber-attack aimed at overwhelming a target system, network, or website with a flood of malicious traffic from multiple sources. The goal of a DDoS attack is to disrupt the availability of the targeted service by exhausting its resources or causing it to become unresponsive to legitimate users. The first "D" stands for a common cybercrime known as a DDoS attack.
- h. **Data Loss Prevention:** The name given to technical security controls/mechanism a company can use to protect sensitive or vulnerable data from being leaked (either by accident or on purpose), disclosed or lost by users.
- i. **Eavesdropping or wiretapping or interception:** Is a term that is used in relation to be listening to something that one should not hear (such as a password). Cybercriminals may be able to do this to users who use unprotected networks to transmit confidential information.

- j. **Kernel:** is term used for the most basic level or core of an operating system, responsible for resource allocation, file management and security. In a different context, this word can also mean the seed and hard husk of a cereal.
- k. **McAfee:** is a computer security company founded by namesake John in 1987 before being acquired by Intel in 2011, is well known for its anti-virus software that is available to individual consumers.
- l. **MFA:** is known as Multi-Factor Authentication.
- m. **OTP:** Is a One-time password. It is a temporary authentication code used for verifying a user's identity during a specific session or transaction. It is a security measure designed to enhance the security of online accounts, systems, or applications by providing an additional layer of authentication beyond traditional username and password combinations. It can only be used once.
- n. **Plaintext:** refers to the original, unencrypted form of data or information. It is the readable and understandable version of the message before any cryptographic transformations or operations have been applied to it.
- o. **PIN:** The secret password strictly limited to numeric character is known as Personal Identification Number.
- p. **Phishing:** The most common cyberattack on the internet that comes in the form of an email pretending to be from your bank or a trusted organisation and asking for your password and other login information.
- q. **Sandbox:** Is a controlled and isolated environment where software applications or processes can run without affecting the underlying system or other applications. It is often used for testing, development, or running potentially untrusted or risky programs in a secure manner. In a different context, this term refers to safe playing area for children.
- r. **SIGINT:** Signals intelligence (SIGINT) is the process of intercepting signals during electronic warfare such as radio communications, telecommunications signals and digital communications to determine if they contain any important security information, for intelligence purposes.
- s. **Social Engineering** This refers to the manipulation of individuals or groups to gain unauthorized access to sensitive information, systems, or resources. It is known as a malicious actor's trick used to trick people into revealing sensitive information. An

example of this is when a scammer poses as tech support to gain access to someone's computer.

- t. **Sniffing or Traffic monitoring:** This refers to the act of watching or capturing and inspecting network traffic to gather information about the data being transmitted over a network.
- u. **Data at Rest:** This describes the state of data. It typically refers to stored digital data. It is said to be "at" as opposed to being "in motion" when moving across a network.
- v. **Kernel:** is term used for the most basic level or core of an operating system, responsible for resource allocation, file management and security. In a different context, this word can also mean the seed and hard husk of a cereal.
- w. **WannaCry:** A global ransomware attack on Windows computers that occurred in May 2017 due to vulnerabilities in a popular Windows service called Service Message Block (SMB).

Module 2

MODULE 2- CAREER OPPORTUNITIES IN CYBERSECURITY

MODULE 2 - CAREER OPPORTUNITIES IN CYBERSECURITY

Governance Risk and Compliance (GRC)

The GRC domain refers to the framework that organizations use to manage and monitor their governance, risk management, and compliance activities related to information security. The governance component of the GRC domain involves establishing policies and procedures for information security management, including defining roles and responsibilities for individuals involved in managing cybersecurity risks. The risk management component involves identifying and assessing cybersecurity risks, implementing appropriate controls to mitigate risks, and monitoring and reporting on the effectiveness of risk management activities. The compliance component involves ensuring compliance with relevant cybersecurity laws, regulations, and standards. This includes identifying and tracking cybersecurity-related regulations, developing and maintaining cybersecurity compliance policies and procedures, and implementing mechanisms for monitoring and reporting compliance.

Common Roles

- Compliance Officer
- Risk Manager
- Governance Analyst
- Internal Auditor
- Information Security Officer
- Documentation Review

Skills & Attributes

- Excellent analytical and critical thinking skills to identify and assess risks, and to develop effective risk management strategies.
- Strong communication skills to effectively communicate complex information to different stakeholders, including executives, employees, and external auditors.
- Strong project management skills to manage multiple initiatives and prioritize tasks effectively.
- Attention to detail to ensure accuracy and completeness of risk assessments, compliance reports, and other documentation.

Cybersecurity Threat Intelligence

Cybersecurity threat intelligence is the collection, analysis, and dissemination of information related to potential cybersecurity threats and attacks. This information is used to inform strategic and tactical cybersecurity planning and is gathered from a variety of sources including open-source intelligence and commercial threat intelligence feeds.

Common Roles

- Threat Intelligence Analyst
- Cyber Threat Hunter
- Cybersecurity Incident Responder
- Information Security Manager
- Cybersecurity Consultant

Skills & Attributes

- Strong analytical skills to collect, analyse, and interpret data from various sources to identify potential cybersecurity threats.
- Knowledge of cyber threat landscape, including threat actors, attack methods, and malware.
- Familiarity with security tools and techniques, such as SIEM, threat intelligence platforms, and data visualization tools.
- Strong communication skills to effectively communicate threat intelligence information to stakeholders in a clear and concise manner.
- Attention to detail to ensure accuracy and completeness of threat intelligence reports and other documentation.

Security Architecture

The security architecture domain of cybersecurity refers to the design and implementation of a secure computing environment that ensures the confidentiality, integrity, and availability of an organization's information assets. This domain focuses on developing a security infrastructure that incorporates a range of technologies, processes, and policies to prevent and mitigate cybersecurity threats.

Security architecture jobs combine hardware and software knowledge with programming, research, and policy development. Security architects anticipate potential threats and design systems to pre-empt them.

Common Roles

- Cloud Security Engineer

- Security Engineer
- Network Security
- Access Control Manager
- Cryptographer

Skills & Attributes

- Technical expertise: A strong understanding of cybersecurity principles, technologies, and practices is essential for designing and implementing effective security architectures.
- Risk management: Security architects must be able to assess and analyse risks to an organization's information assets and develop strategies to mitigate those risks.
- Communication skills: Effective communication skills are essential for security architects, as they must be able to communicate complex technical information to a variety of stakeholders, including business leaders, IT staff, and other security professionals.
- Project management: Security architects often work on large-scale projects that require coordination with multiple stakeholders, including other security professionals, IT staff, and business leaders. Strong project management skills are essential to ensure that projects are completed on time, within budget, and with the desired outcome.
- Compliance: Security architects must have a strong understanding of regulatory requirements and compliance standards related to cybersecurity, such as GDPR, HIPAA, and PCI-DSS. They must be able to design security architectures that meet these requirements while still providing effective protection against cyber threats.

User Education

User education is a critical aspect of cybersecurity. It refers to the process of educating users within an organization about safe computing practices and how to protect sensitive information from cyber threats. The goal of user education is to reduce the likelihood of security incidents caused by human error, such as falling for phishing scams or using weak passwords.

Common Roles

- Security Awareness Training Specialist
- Technical Trainer

- Learning and Development Manager
- Cybersecurity Education Program Manager

Skills & Attributes

- Strong communication skills: The ability to communicate complex cybersecurity concepts to non-technical users in a clear and concise manner is essential for user education.
- Knowledge of cybersecurity best practices: A deep understanding of cybersecurity threats and the best practices for protecting against them is crucial for a user education professional.
- Creativity and innovation: User education often involves developing creative and innovative strategies for engaging users and making cybersecurity training more effective.
- Adaptability: User education professionals must be able to adapt to changing technologies and evolving threats to ensure that training remains relevant and effective.
- Patience and persistence: Educating users about cybersecurity can be challenging and requires patience and persistence to ensure that users are properly trained and follow best practices.

Security Operation

The Security Operation (SecOps) is a domain in cybersecurity that focuses on managing and responding to security incidents and threats. It involves the implementation and management of security technologies, processes, and procedures that are designed to prevent, detect, and respond to cybersecurity incidents. The SecOps team is responsible for monitoring the organization's systems, networks, and applications to identify potential security threats and incidents. They use a range of security tools, such as firewalls, intrusion detection and prevention systems (IDS/IPS), and security information and event management (SIEM) solutions, to monitor and analyse security logs and events.

COMMON ROLES

- Security Operations Center (SOC) Manager
- Penetration Tester
- Security Analyst

Skills & Attributes

- Analytical and problem-solving skills: The ability to analyse complex security events and incidents, identify potential threats, and develop effective solutions is critical for SecOps professionals. They should be able to think critically, creatively, and systematically to solve security problems.
- Communication skills: Effective communication is essential in SecOps, as it involves working with different teams, stakeholders, and vendors to manage security incidents. SecOps professionals should be able to communicate clearly and effectively, both orally and in writing.
- Attention to detail: SecOps involves monitoring and analysing large volumes of security logs and events and requires attention to detail to identify potential security incidents. A small detail can be the key to uncovering a security threat.
- Ability to work under pressure: Security incidents can occur at any time and require quick action to contain and remediate the threat. SecOps professionals should be able to work effectively under pressure and prioritize tasks to manage incidents in a timely manner. They should be able to handle high-stress situations with calmness and focus on the task at hand.

Application Security

The application security domain of cybersecurity involves the protection of software applications from potential cyber threats. It focuses on identifying and addressing vulnerabilities in software applications that can be exploited by attackers to gain unauthorized access or steal sensitive data. Application security involves a range of activities, including secure software design, coding, testing, and deployment. It also includes ongoing monitoring and maintenance of applications to ensure that they are secure and free from vulnerabilities.

Common Roles.

- DevSecOps Engineer
- Application Security Analyst
- Application Security Engineer
- Security code auditor

Skills & Attributes

- Strong knowledge of software development: Application security professionals should have a strong understanding of the software development process, including knowledge of programming languages, frameworks, and development methodologies.
- Knowledge of security standards and best practices: Application security professionals should have a strong understanding of security standards and best practices, including OWASP Top 10, CWE Top 25, and NIST guidelines.
- Analytical skills: Application security professionals should have strong analytical skills, including the ability to analyse security logs and identify potential security incidents.
- Communication skills: Application security professionals should have strong communication skills, including the ability to communicate complex technical information to non-technical stakeholders.
- Problem-solving skills: Application security professionals should have strong problem-solving skills, including the ability to identify and address potential security risks in software applications.

Enterprise Risk Management (ERM)

The Enterprise Risk Management (ERM) domain of cybersecurity is concerned with identifying, assessing, and managing risks to an organization's information assets. This includes risks associated with cyber threats, such as data breaches, cyber-attacks, and other forms of cybercrime. ERM involves a comprehensive approach to risk management that encompasses all aspects of an organization's operations, including its people, processes, and technology. This approach helps organizations to better understand their risk posture and to develop effective risk management strategies that address both existing and emerging threats.

Common roles

- Chief Information Security Officer (CISO)
- Risk Manager
- Compliance Manager

Skills & Attributes

- Risk Management Expertise: A strong understanding of risk management principles and methodologies is essential for a person working in cybersecurity ERM.
- Analytical Thinking: The ability to analyse complex data sets, identify trends, and draw insights is important in cybersecurity ERM.

- **Communication Skills:** Effective communication skills are important for a person working in cybersecurity ERM, as they need to be able to explain complex security concepts to non-technical stakeholders.
- **Business Acumen:** A strong understanding of an organization's business objectives and operations is important for a person working in cybersecurity ERM. **Collaboration:** Cybersecurity ERM often involves working with stakeholders from different departments and business units.

Descriptions of some common cybersecurity job roles



Job role	Description
Compliance Officer	Ensures that the organization complies with laws, regulations, and internal policies and procedures.
Risk Manager	Identifies, analyses, and manages risks to the organization and its assets.
Information Security Officer	Ensures that information assets are protected against unauthorized access, use, disclosure, disruption, modification, or destruction.
Governance Analyst	Helps to establish and maintain policies and procedures related to governance activities.
Internal Auditor	Evaluates the effectiveness of internal controls, risk management processes, and compliance with laws and regulations.
Threat Intelligence Analyst	Responsible for collecting, analysing, and disseminating intelligence related to potential cybersecurity threats and attacks.
Cyber Threat Hunter	Conducts proactive hunting for potential cyber threats, using various tools and techniques to detect and prevent attacks
Cybersecurity Incident Responder	Responds to and manages cybersecurity incidents, including analysing and containing security breaches, and recovering from cyber-attacks.
Cybersecurity Consultant	Provides expertise and guidance to organizations on threat intelligence and cybersecurity best practices and helps to implement effective cybersecurity strategies.

Information Security Manager	Oversees the overall security posture of the organization, including threat intelligence and incident response activities.
Security Analyst	A security analyst is responsible for monitoring and analysing security events and alerts from various sources to identify potential security incidents. They also investigate security incidents, conduct forensic analysis, and recommend measures to prevent future incidents.
Security Operations Center (SOC) Manager	A SOC manager oversees the daily operations of a security operations center, which is responsible for monitoring and responding to cybersecurity incidents. They manage the SOC team, ensure that security incidents are effectively managed and resolved, and continuously improve the SOC's effectiveness and efficiency.
Penetration Tester	A penetration tester is responsible for identifying vulnerabilities in an organization's systems, networks, and applications by simulating real-world cyber-attacks. They use a range of techniques and tools to test the organization's defenses and identify potential weaknesses that can be exploited by attackers. These skills may also be used for hunting bugs in applications for profit (bug bounty).
Cloud Security Engineer	
Security Engineer	A security engineer is a cybersecurity professional who designs, implements, and maintains security controls to protect an organization's systems, networks, and data from cyber threats.
Network Security Engineer	A network engineer is a professional who designs, implements, and maintains computer networks for organizations. They are responsible for ensuring the smooth and efficient

	operation of network infrastructure, including local area networks (LANs), wide area networks (WANs), and wireless networks.
Access Control Manager	An access control manager is a cybersecurity professional who is responsible for managing access to an organization's systems, networks, and data. They are responsible for creating and enforcing access policies, ensuring compliance with security regulations, and monitoring access logs for any suspicious activity.
Cryptographer	A cryptographer is a cybersecurity professional who specializes in creating and breaking codes and ciphers to secure or gain access to information. They use advanced mathematical and computational techniques to design and analyse encryption algorithms, and are employed in various industries, including government, military, and technology.
DevSecOps Engineer	A DevSecOps engineer is responsible for integrating security into the software development lifecycle. They work closely with developers and operations teams to ensure that security is integrated into all stages of the development process, from design to deployment.
Application Security Analyst	An application security analyst is responsible for monitoring and analysing security logs and events from software applications to detect potential security incidents.
Application Security Engineer	An application security engineer is responsible for designing, developing, and implementing secure software applications. They work closely with software development teams to ensure that applications are designed and developed with security in mind.

Security code auditor	A code auditor is a cyber security professional who reviews source code in applications to find any glitches or bugs that might affect functionality or security. The code auditor needs to be aware of the latest technologies and methods in use by hackers and may need to simulate a cyber-attack to test the code
Chief Information Security Officer (CISO)	The CISO is responsible for overseeing an organization's overall security strategy, including risk management. This includes identifying and prioritizing risks, developing risk management strategies, and monitoring the effectiveness of security controls.
Security Awareness Training Specialist	This role is responsible for developing and delivering security awareness training programs to educate employees on cybersecurity best practices.
Technical Trainer	This role involves creating and delivering training programs on the use of specific cybersecurity tools or technologies
Learning and Development Manager	This role is responsible for developing and implementing a comprehensive training and development program for employees across all areas of the organization, including cybersecurity.
Cybersecurity Education Program Manager	This role involves managing the development and delivery of a comprehensive cybersecurity education program for employees, which includes training, awareness campaigns, and ongoing support and guidance.

Module 3

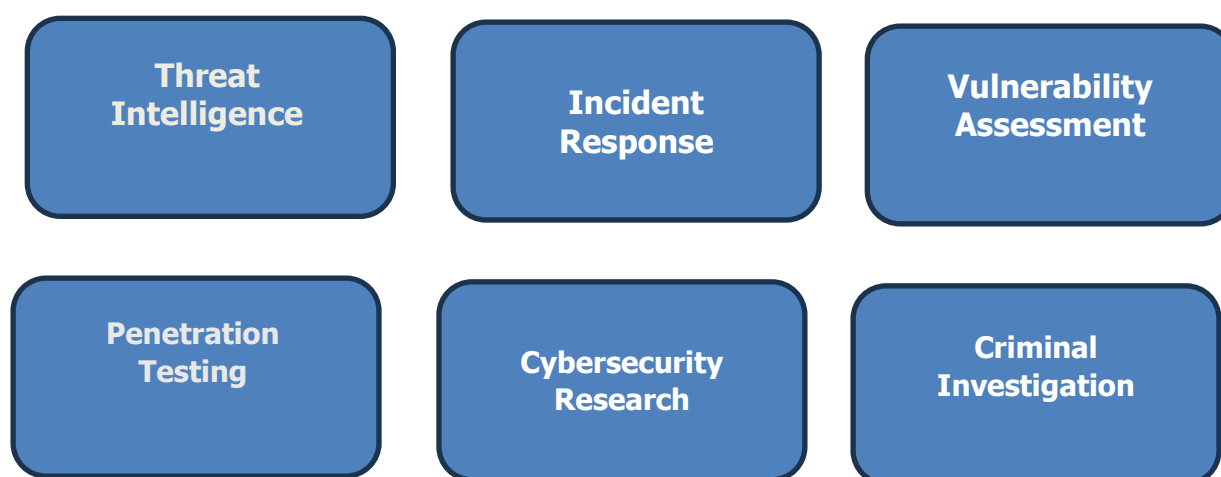
MODULE 3- OPEN-SOURCE INTELLIGENCE

OPEN-SOURCE INTELLIGENCE MODULE

Introduction to OSINT

OSINT (Open-Source Intelligence) refers to the collection and analysis of information from publicly available sources. This includes social media, online forums, public databases, search engines, and online publications. OSINT is a crucial aspect of cybersecurity, as it helps identify potential threats and vulnerabilities. By leveraging OSINT, security professionals can stay ahead of threats and make informed decisions to protect their organizations.

What is OSINT Used For?



Types of OSINT Sources

- **Social media:** Social media platforms like Twitter, Facebook, and LinkedIn can provide valuable insights into potential threats and vulnerabilities.
- **Online Forums and Discussion Boards:** Online communities like Reddit, Stack Overflow, and GitHub can offer valuable information on security-related topics.
- **Public Databases and Archives:** Public databases like WHOIS and DNS records can provide information on domain ownership and network infrastructure.
- **Search Engines and Meta-Search Engines:** Search engines like Google and Bing can be used to gather information on specific topics or targets.
- **Online Publications and News Articles:** News articles and online publications can provide valuable insights into emerging threats and trends.

OSINT Collection Methods

- **Web Scraping:** Web scraping involves using software to extract data from websites and web pages.
- **API Calls:** API calls can be used to gather data from social media platforms, search engines, and other online sources.
- **Human Intelligence (HUMINT):** HUMINT involves gathering information through human interactions, such as interviews and surveys.

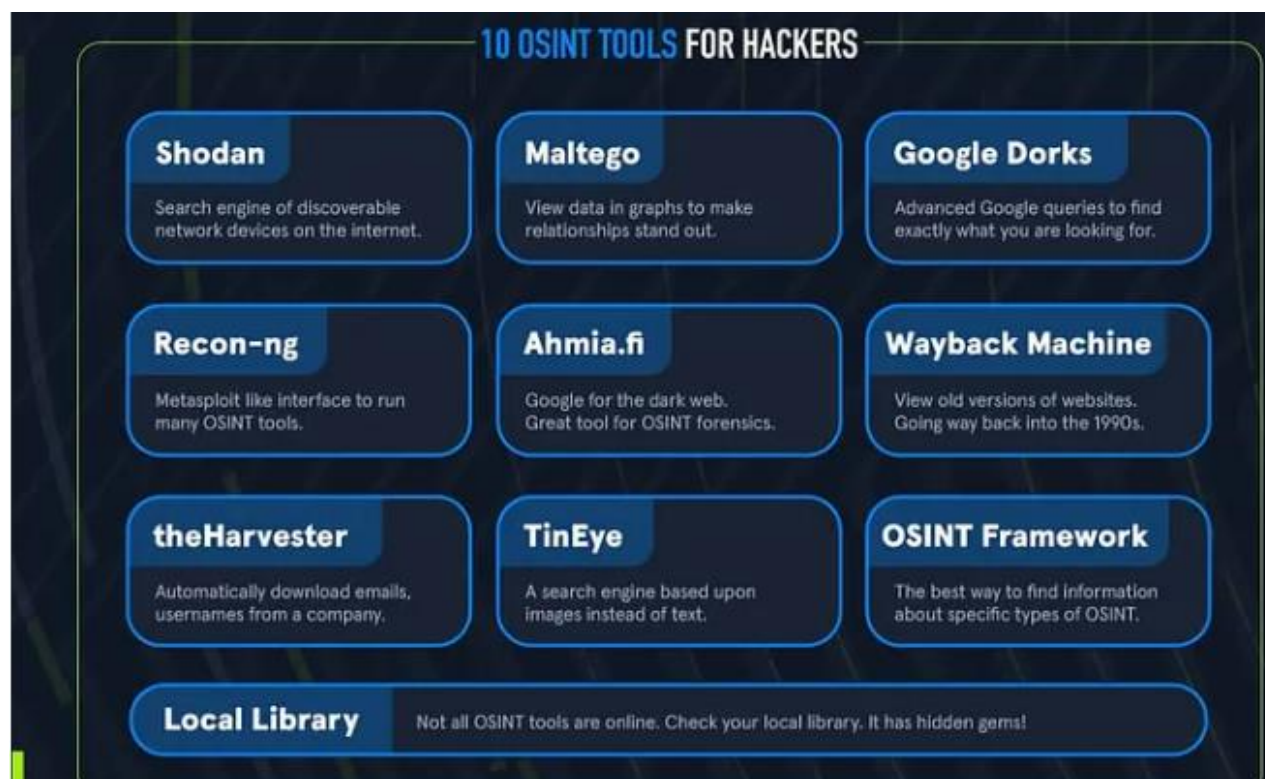
- **Crowdsourcing:** Crowdsourcing involves gathering information from a large group of people, often through online platforms.
- **OSINT Tools:** Various tools like Maltego, Shodan, and Recon-ng can be used for OSINT collection and analysis.



OSINT Analysis Techniques

- **Network Analysis:** Network analysis involves studying relationships between entities and identifying patterns and anomalies.
- **Geospatial Analysis:** Geospatial analysis involves studying geographic locations and mapping data to identify trends and patterns.
- **Sentiment Analysis:** Sentiment analysis involves studying text data to identify emotions and opinions.
- **Entity Recognition:** Entity recognition involves identifying and extracting specific entities like names, locations, and organizations.
- **Data Visualization:** Data visualization involves using visual representations to understand and communicate complex data.

OSINT Tools and Resources



Case Study: Using OSINT to Enhance School Safety and Security Scenario

Sunshine High School, a mid-sized public school, noticed a rise in cyberbullying incidents and unauthorized access attempts to its online systems. Concerned about student safety and the integrity of its digital infrastructure, the school administration decided to employ OSINT techniques to identify and mitigate these threats.

OSINT Activities

Step 1: Monitoring Social Media

The school's IT team started by monitoring social media platforms like Twitter, Instagram, and Facebook for any posts mentioning Sunshine High School. They used specific keywords related to the school, such as "SunshineHS," "Sunshine High School," and "SunshineBullying."

- **Findings:** They discovered several posts from students discussing bullying incidents. Some posts included derogatory comments and threats directed at specific students.

Step 2: Analyzing Online Forums and Groups

The team also explored online forums and groups where students might discuss school-related issues. They paid close attention to popular platforms like Reddit and local community message boards.

- **Findings:** They found a thread on Reddit where students were sharing tips on bypassing the school's internet security to access restricted websites. This posed a significant risk to the school's digital safety.

Step 3: Checking Public Databases

The IT team accessed public databases and archives to verify the security of the school's digital assets. They looked into domain registration details and checked for any reported vulnerabilities associated with the school's online systems.

- **Findings:** They discovered that the school's website domain had some outdated security certificates, making it vulnerable to potential attacks.

Step 4: Using OSINT Tools

The team utilized various OSINT tools like Maltego and Shodan to gather more detailed information about the school's digital footprint. These tools helped them map out the network infrastructure and identify potential weak points.

- **Findings:** They identified several unsecured network devices within the school's IT infrastructure that needed immediate attention.

Step 5: Conducting Sentiment Analysis

Sentiment analysis was performed on the collected social media posts and online forum discussions to gauge the overall mood and identify any alarming trends.

- **Findings:** The analysis revealed a high level of anxiety and distress among students, particularly related to cyberbullying incidents.

Mitigation Measures

Based on the OSINT findings, Sunshine High School took several steps to enhance security and safety:

1. Enhanced Cyberbullying Prevention:

- The school launched a campaign to raise awareness about cyberbullying and its consequences.
- They set up a dedicated hotline and email address for students to report bullying incidents anonymously.

2. Improved Network Security:

- The IT team updated all security certificates and patched vulnerabilities in the school's digital infrastructure.
- They installed advanced firewall and intrusion detection systems to prevent unauthorized access.

3. Student and Staff Training:

- Regular training sessions were conducted for students and staff on the importance of cybersecurity and safe online behavior.
- They introduced workshops on recognizing and reporting cyber threats.

4. Monitoring and Response:

- The school established a continuous monitoring system to keep track of social media and online forums for any new threats or incidents.

- They created an incident response team to address any security issues promptly.

5. **Collaboration with Authorities:**

- The school collaborated with local law enforcement and cybersecurity experts to enhance their security measures and respond to serious threats.

By effectively using OSINT techniques, Sunshine High School was able to identify and mitigate various security threats, ensuring a safer environment for its students and staff. This proactive approach not only addressed immediate concerns but also established a robust framework for future security measures.

Key Takeaways for Students

- **Awareness:** Understand the importance of cybersecurity and safe online practices.
- **Reporting:** Know how and where to report cyberbullying or any suspicious online activity.
- **Collaboration:** Work together with peers, teachers, and parents to maintain a secure and supportive school environment.
- **Continuous Learning:** Stay informed about the latest trends in cybersecurity and adapt to new challenges.

Module 4

MODULE 4- ONLINE ACTIVITIES AND ASSOCIATED RISK

Background

1. Online gaming
2. Social networking
3. Video and audio streaming
4. Betting
5. E-learning
6. Online shopping
7. Software downloads
8. Sexting



According to Cybersecurity Ventures, the rising cost of damages resulting from cybercrime, is expected to reach \$10.5 trillion by 2025. Each year there are at least 378 million and 12,000 victims of cybercrime in the United States and Ghana respectively. Indeed, the Internet has also brought with it several unintended, unforeseen, and unwanted risks. Some of these are of particular concern to the health and safety of children and young people. Many fraudsters like to specifically target children, as young people often don't have the experience and knowledge to distinguish legitimate requests from fraudulent ones. Fraudsters can use knowledge gained from children online to steal,



blackmail, terrorize, or even kidnap.

Some common online risks include the following:

Online Risk	Definition	Exposure Factors
Information disclosure (self-disclosure)	This occurs when we share personal information about ourselves online, on our profiles and with our online friends. It is normal to share information about ourselves but when it includes personally identifiable information (i.e. passport details, Ghana Card number, home address, phone number), it makes it possible for malicious persons to use this information to profile you, to stalk you or harass you online and offline.	Social networking, Online gaming
Online fraud	This occurs when we meet people online or opportunities that are not what they claim to be. This includes fake online shops, social media profiles, scholarships, investments, and fake online companies.	Online shopping, social networking
Recruitment fraud	This is a form of online fraud where a fake profile or businesses offers non-existent jobs to individuals who visit their page. They may be pretending to be recruiters who want to employ people into hospitals, ministries, the army or even into schools.	Online job searches
Scholarship fraud	Fraudsters are actively deceiving students with the lure of foreign scholarships on social media. In addition, fake websites related to scholarships are being created, and their links spread on social media platforms. When students input their personal information on these websites, scammers use it for various purposes. These cybercriminals adopt new methods every day to defraud people, offering fake scholarships for free studies at universities abroad, collecting documents, and demanding upfront payments for application processing. Often, students are duped into paying multiple times for different processing steps, only to be blocked later, losing their money.	Social networking
Cyberbullying	This is the use of technology to harass persons online by exposing embarrassing information about them or making them receive a flood of unkind messages from online users.	Social networking

Fake news	Fake news is any news item that is not true or intentionally misrepresents the facts of an issue. Often this is done to confuse readers as part of a misinformation campaign.	Searching for news online, social networking
Inappropriate content	Inappropriate content includes any audio, picture or video which is not good for people, especially children, to see or use. Usually, this used to refer to pornography or material with excessive violence.	Social networking and online streaming, sexting
Cyber grooming	Cyber grooming occurs when an adult builds an emotional relationship with a young person online, with the intention of sexual abuse or exploitation. This can extend offline where the adult sends gifts and money to make the young person feel special/indebted.	Social networking, online gaming
Sextortion	This is a form of blackmail which occurs when one person demands sexual favours from another individual in order to prevent the blackmailer from disclosing sensitive information about him/her. For example, a student may be blackmailed because they sent their naked pictures to another person. This is one of the biggest risks of forming intimate online relationships.	Social networking, sextortion
Romance Scams	Malicious actors create fake online profiles to deceive victims into believing they are engaging in a trusting romantic relationship. They use the relationship to persuade the victims to send money, provide sensitive personal and financial information, or purchase items for them.	Social networking
Cyberstalking	Cyberstalking is the use of technology and online platforms to closely follow the activities of another person, for the purpose of harassment, or abuse. This can be used by a malicious person to gain enough information to intimidate you since he/she has gained access to sensitive information about you.	Social networking, online gaming
Malware	Malware refers to the many different types of malicious software which infect our computers and destroy our data. This software comes from various sources, but the most common source is online downloads. Examples include spyware, trojan, ransomware, botnet and rootkit.	Software downloads, online gaming, sexting

Flaming	Flaming, also known as roasting, is the act of posting insults, often including profanity or other offensive language, on the internet.	Social networking, Online gaming
---------	---	-------------------------------------

Types of threat actor

The internet is a powerful tool and while these online activities are not harmful, the use of computers and the internet comes along with some risks to anyone who uses them. This is mainly because there are malicious people who use the internet as a tool to harm others. Other times, the risk is present because innocent people make innocent mistakes without realizing the possibility of danger.



This makes it important to know the various types of malicious persons online and how they operate, since this is one of first ways to prevent us from falling victim (know thy enemy, know thyself).

A threat actor is a malicious person, group or government that launches attacks on other users and their systems. There are different types and each one usually has a specific goal. The two main goals are financial gain and destruction of data. Some types of threat actors include:

Threat Actor Type	Definition	Chief Goal	Typical Targets
Cyber terrorists	These are terrorist groups which launch cyberattacks as way to promote their extremist ideology or spread fear through their attacks.	Cause violence, harm or destroy critical services to spread their cause.	Businesses, Critical services, and State/Public infrastructure
State-sponsored actors	These are groups of very technical experts who are funded, directed, or sponsored by nations to launch cyberattack against other nations or businesses	Espionage, theft of intellectual property & Sensitive information, theft of funds (huge sums)	Businesses, and Government organizations

Cybercriminals/Organized crime	These are individuals and groups who want to steal sensitive data, money, and personal information, and launch attacks on a variety of systems.	Financial gain	Businesses and Organizations. Especially, those that might use a lot of personal data or have a lot of money
Hacktivists	These are hackers who focus on bringing awareness to social issues or their ideology.	Exposing secrets, and disrupting organizations and services seen as evil.	Not limited to any specific type. Any organization can be a victim
Script kiddies	These are low-level hackers who use tools developed by others to launch cyberattacks. They aren't skilled enough to design tools on their own.	Gain satisfaction from being able to attack systems, and inflicting damage through online vandalism	Vulnerable systems which may be easy to penetrate.
Insiders	These are individuals working within their own organization who use their level of access to either support or carry out cyberattacks on their own organization.	Work from within an organization to bypass security and launch cyberattack	Not limited to any specific type. Any organization can be a victim

Online Privacy issues

There is a popular saying that “the internet never forgets”. This is because the computers, databases and other systems that support the internet are designed to be available all the time. The saying also means that the information we upload or share

online stays there forever and is never truly deleted, even when we click the delete button.

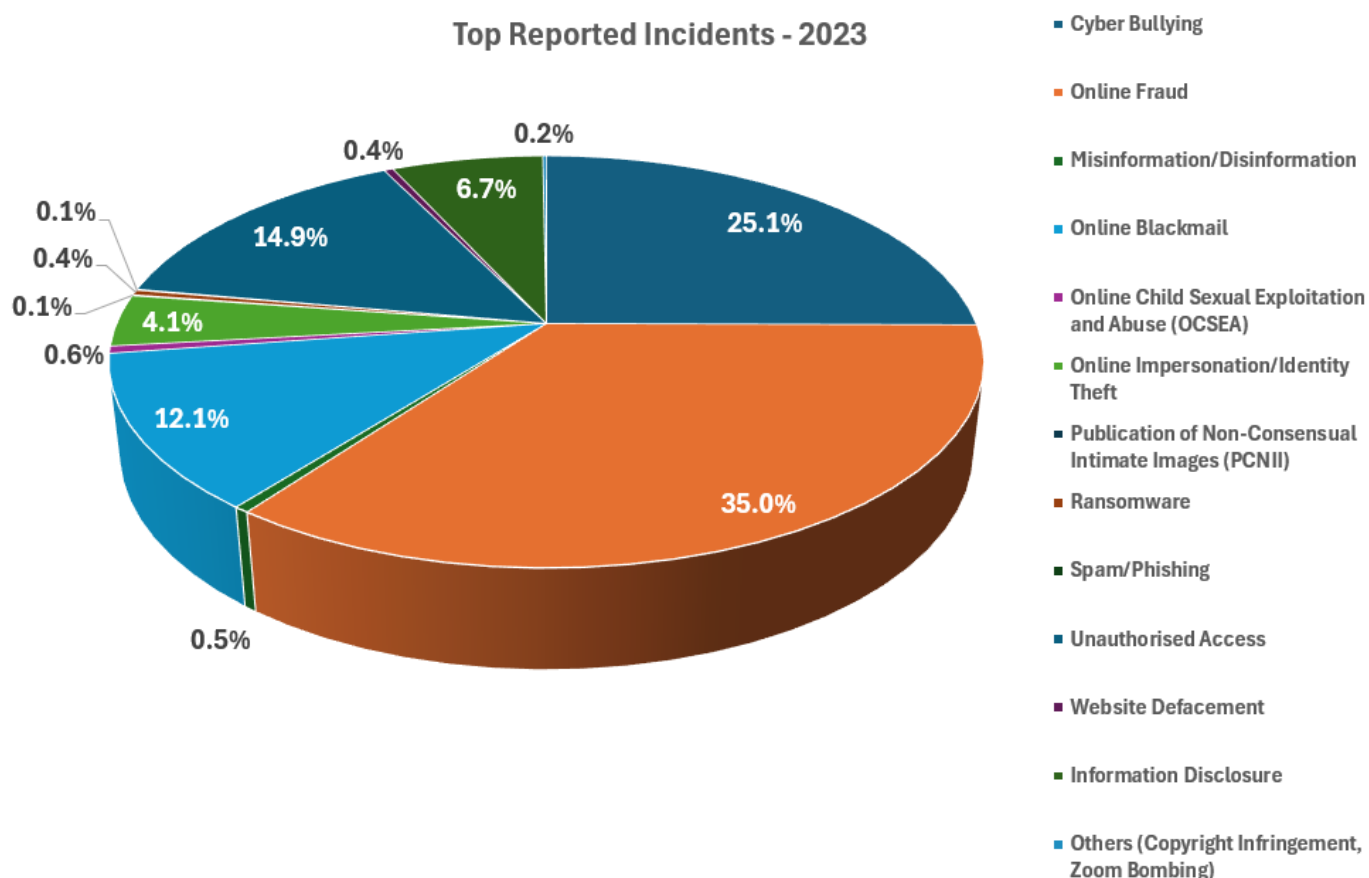
This is what is referred to as Digital Footprint. In other words, a digital footprint is a trail that exists online which is left to show that we have been online. Generally, this includes websites we visit, photos we upload, messages we send, items we buy, and any other action we take online.



For example, the Internet Archive (archive.org) contains the largest collection of the internet's history available to mankind. It contains numerous books, music, videos, websites, and even social media posts which the original owners may have deleted.

This is very useful for research; however, the same Internet Archive can be used by different entities for different purposes. Online marketing companies may use your digital footprint to build a profile, track users and recommend products to them; cybercriminals use digital footprint to conduct cyberstalking on individuals or companies and subsequently attack them; the government can use digital footprint to analyse the population so that they can understand their demographic, interests, and behaviour to provide new social amenities; the police and law enforcement can also use our digital footprint to locate us if we are kidnapped or to track and arrest cybercriminals and other lawbreakers.

TOP REPORTED INCIDENTS



1. Online Fraud (Investment Fraud, Romance Scams, Recruitment Scams) – **35%**
2. Cyber Bullying – **25%**
3. Unauthorised Access (Account Takeover, Phishing etc) – **14.9%**
4. Online Blackmail (Sextortion, Extortion) – **12.1%**
5. Information Disclosure – **6.7%**
6. Online Impersonation / Identity Theft – **4.1%**
7. Online Child Sexual Exploitation and Abuse (OCSEA) – **0.6%**
8. Misinformation / Disinformation – **0.5%**
9. Ransomware – **0.4%**
10. Website Defacement – **0.4%**
11. Publication of Non-Consensual Intimate Images – **0.1%**
12. Spam / Phishing – **0.1%**
13. Others (Copyright infringement, Zoom bombing) – **0.2%.**



Online Shopping Scams:

Malicious actors create fake online shops or impersonate existing businesses on social media pages, offering heavily discounted goods. Victims are enticed to send money for these deals but never receive the items.

Mobile Payment Services Fraud:

Malicious actors trick unsuspecting victims into sharing their mobile money wallet PIN. The scammers then proceed to make unauthorised payments or transfers from the victim's wallet.

Courier Service Scams:

Malicious actors impersonate workers of a legitimate courier service and lure unsuspecting victims to believe they have a package that needs to be delivered for a certain fee. No delivery is made after the victims make the payment.

Romance Scams:

Malicious actors create fake online profiles to deceive victims into believing they are engaging in a trusting relationship. They use the relationship to persuade the victims to send money, provide personal and financial information, or purchase items for them.



Shopping Fraud:

Malicious actors create fake websites or online shops or impersonate existing businesses on social media pages, offering heavily discounted packages and items. Victims are enticed to send money for these deals but never receive the promised packages/items.

Phishing Scams:

Malicious actors send unsolicited emails or messages claiming to be from a romantic partner, or from a company offering deals. These messages contain links or attachments that when clicked, install malicious software (malware), or steal personal information.

Lottery and Prize Scams:

Malicious actors contact victims and claim that they have won a prize or lottery for a gift but need to pay a fee or provide personal information to claim the prize.

Charity Scam:

Malicious actors may contact victims and claim to be a charity organization. They may ask for donations for gifts for needy children and other related causes.

Recommendations

- Be wary of unsolicited messages or emails claiming to be from a romantic partner.
- Be cautious of "too good to be true" deals on packages or gifts.
- Do not share personal information such as your Ghana card number, credit card information, or bank account details with anyone, especially if you do not know them well.
- Be cautious of online romantic partners who make requests for money or other sensitive information.
- DO NOT share your personal information such as your credit/debit card information or bank account details with anyone, especially if you do not know them well.
- Use only reputable online marketplaces or retailers when purchasing items or gifts. Look for reviews and customer feedback and always insist on payment AFTER delivery.
- Do not pay any delivery fees for goods you did not order.

WhatsApp Account Takeover

A potential victim would either receive a call from an unknown number, or a message from a friend (whose social media account may have been compromised) requesting the victim to share a one-time password (OTP) (usually a 6-digit verification code) sent to the victim's number as a text message.



The scammers apply social engineering, typically creating a sense of emergency and request for the OTP which was sent to the victim. The victim would thereafter lose access to the account after providing the scammers with the verification code.

The scammers, after gaining access to the victim's account then target persons and groups on the victim's contact list as the next potential victims. Through this, the scammers would impersonate the victim's friends and promote other fraudulent activities or solicit funds. The scammers' request would be on the pretext of helping them to join online groups such as work or school groups or sign up and claim prizes for fake lucky draws allegedly conducted or joined.

Preventive & Mitigation Measures

Countering Account Takeovers: Enable 'Two-Step Verification'

- Open WhatsApp Settings
- Tap Account > Two-step verification > Enable.
- Enter a six-digit PIN of your choice and confirm it.
- Provide a valid email address you have access to or tap Skip.

Note: Providing the email address is recommended. Otherwise, if you forget your PIN, you will have to wait 7 days before you can reset it. Tap Next

Confirm the email address and tap Save or Done

Sextortion (Sexual Extortion)

A potential victim would typically make a new friend on a social media platform e.g., Facebook. Eventually the two parties exchange WhatsApp numbers and the chats continue over there, establishing a level of trust and familiarity. After some time, a video call is initiated over which the victim ends up being persuaded to go nude. Unknown to them, the session is recorded by the other party.

Some days afterwards, the other party (or an associate) will contact the victim indicating that they have these videos and will threaten to release them in public unless they receive a specified payment. In some cases, the criminals will go ahead to share it online, provide a link (URL) to where it is and indicate it would only be taken down when they are paid. The demands typically do not end once the first payment is made.



Avoiding Sexual Extortion Schemes

- Avoid initiating and/or participating in video calls of an intimate nature i.e. where nudity is displayed, sexually explicit acts are performed etc.
- If you receive a ransom demand, do not make payment. Instead, report it immediately to the CSA's Cybersecurity/Cybercrime Incident Reporting Point of Contact for guidance.

RECOMMENDATIONS



The following measures are recommended to prevent online scams:

- Never share your social media application account verification codes with anyone. Protect all your social media application accounts by enabling the 'Two-Step Verification' or 'Two-Factor authentication (2FA)' feature.
- Be aware of who has physical access to your phone. If someone has physical access to your phone, they can use your account without your permission. Do NOT be impulsive - Beware of unusual requests from strangers or even your social media contacts.
- Do NOT believe - Be wary of claims that you have won a prize, especially if you have not participated in any campaign or lucky draw. Check official websites to determine whether the lucky draw offers are legitimate. Always verify the authenticity of the request by contacting your friend, but do not do so through the social media platform as the account might have been taken over by scammers.
- Do NOT give - Do not transfer money or give out your personal information, bank account or credit/debit card details, and One-Time Password (OTP) to anyone, including family and friends.
- If you are contacted by anyone claiming to have images and/or videos of you of an intimate nature requesting a payment in exchange for not releasing them to the public, report it immediately to the CSA's Cybersecurity/Cybercrime Incident Reporting Point of Contact for guidance. Do NOT make any payments.

Module 5

MODULE 5- MISINFORMATION, DISINFORMATION AND FAKE NEWS

Misinformation, Disinformation and Fake News

Exploring the Definitions, Impacts and Solutions



Presentation Overview

Misinformation, Disinformation, and Fake News

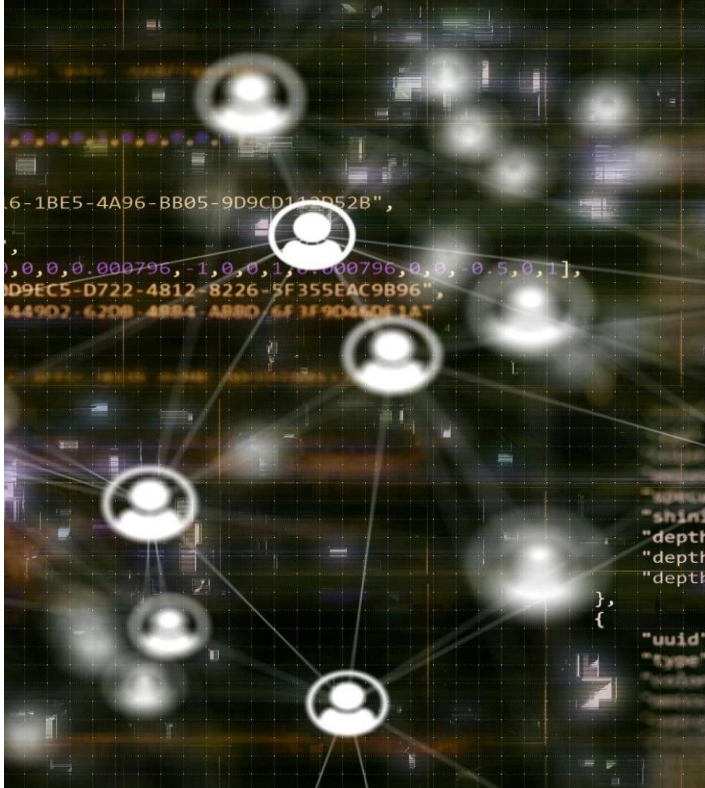
The presentation will begin by defining and providing examples of misinformation, disinformation, and fake news.

Impact on Society

We will discuss the impact of misinformation, disinformation, and fake news on society, including their effects on politics, public opinion, and media.

Combatting Misinformation

Finally, we will cover ways to combat misinformation, disinformation, and fake news, including fact-checking tools and media literacy education.



Definitions and Examples

Misinformation

Misinformation is false or inaccurate information that is spread unintentionally through various mediums such as social media, news outlets, or word of mouth.

Disinformation

Disinformation is false or inaccurate information that is spread intentionally to mislead people or influence public opinion on a particular topic.

Fake News

Fake news is a type of disinformation that is designed to look like legitimate news but contains false or misleading information that is spread through various mediums.



Definitions of Misinformation, Disinformation, and Fake News

Misinformation

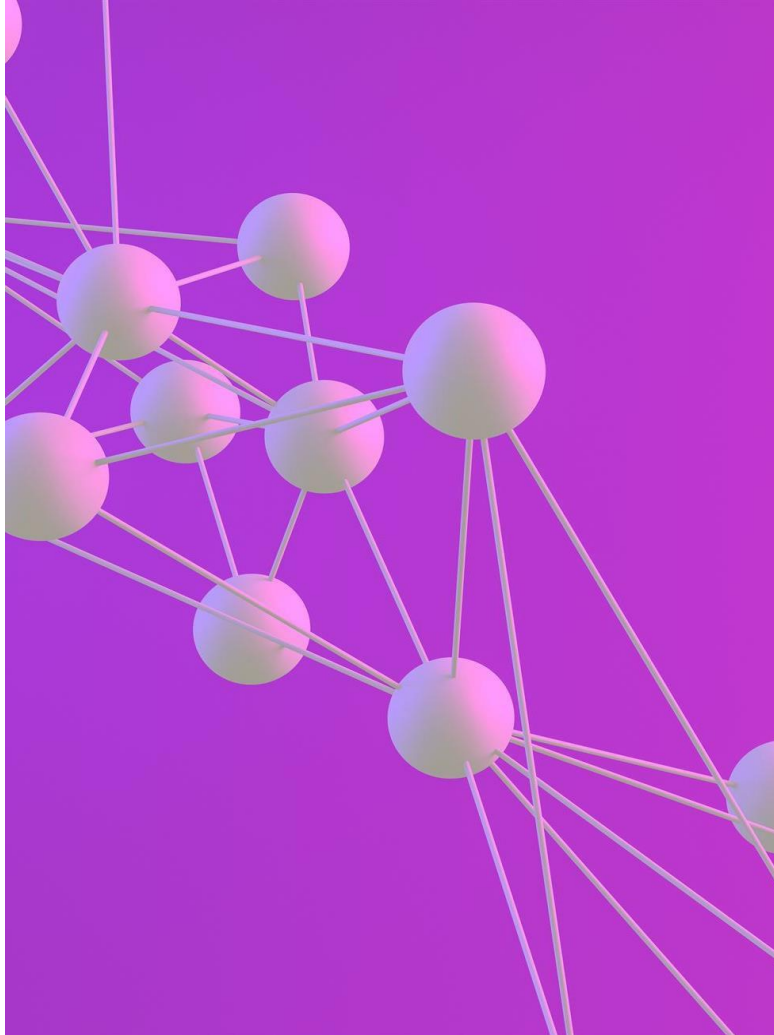
Misinformation is inaccurate information that is spread unintentionally, often due to lack of knowledge or awareness.

Disinformation

Disinformation is intentionally misleading information that is spread to deceive or manipulate others, often with the goal of achieving a political or social agenda.

Fake News

Fake news is a type of disinformation that is spread through traditional or social media, often with the purpose of generating clicks or views for profit.



Examples of Misinformation, Disinformation, and Fake News

Misinformation

Misinformation is inaccurate or incomplete information that is spread widely through social media or other channels, leading to confusion or misunderstanding among the public.

Disinformation

Disinformation is false information or propaganda that is spread through news outlets or social media to influence public opinion or sow confusion.

Fake News

Fake news is fabricated stories or hoaxes that are spread through social media or other outlets to generate clicks or attention, often with the intent of influencing public opinion.

Impact on Society

Political Polarization

Misinformation, disinformation, and fake news can cause political polarization and divisions in society. It can lead to mistrust and hostility among people with differing views, making it difficult to find common ground for important issues.

Health Consequences

Misinformation, disinformation, and fake news can have serious health consequences. It can lead to the spread of false medical advice, treatment, or cures, causing harm to individuals and society as a whole.



Political Polarization



Misinformation and Disinformation

Misinformation and disinformation are major contributors to political polarization, as they promote extreme views and reduce trust in institutions.

Social Unrest

Political polarization can lead to increased social unrest, as people become more divided and less willing to compromise.

Decreased Civic Engagement

Political polarization can lead to decreased civic engagement, as people become less interested in participating in the political process.

Breakdown of Democratic Values

Political polarization can lead to a breakdown of democratic values, as people become more focused on winning at all costs rather than working together for the common good.

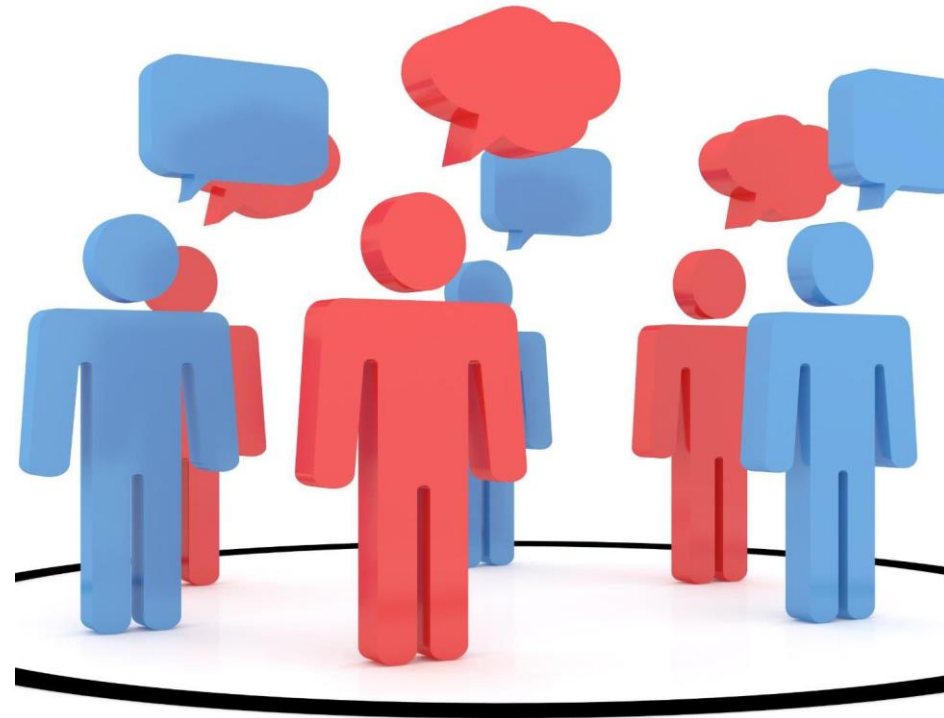
Health Consequences

Misinformation and Health

Misinformation, disinformation, and fake news can have serious health consequences during public health crises, leading to dangerous behaviors and further spread of disease.

False Information about Treatments and Cures

False information about treatments, cures, and prevention strategies during public health crises can be dangerous and lead to harmful behaviors.



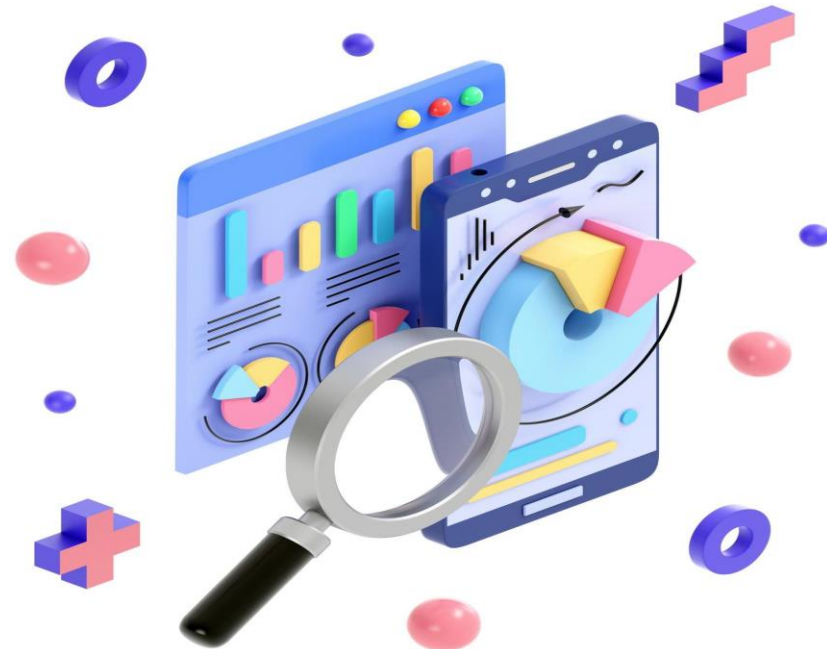
Combating Misinformation, Disinformation and Fake News

Fact-Checking Tools

Fact-checking tools are an effective strategy for combating misinformation and fake news. They use various methods, such as crowdsourcing, to verify the accuracy of news articles and social media posts.

Media Literacy Education

Media literacy education is an important strategy for combating misinformation and fake news. It teaches people how to critically analyze news articles and social media posts, and how to identify bias, misinformation, and propaganda.





Fact - Checking Tools

Fact-checking is crucial in verifying the accuracy of information provided by individuals and organizations. Fact-checking tools help to minimize the spread of false information and promote informed decisions.

Media Literacy Education

Understanding Sources of Information

Media literacy education can help individuals understand the sources of information and the reliability of these sources, enabling them to make informed decisions.

Author's Intentions

Media literacy education can help individuals identify the author's intentions, enabling them to better understand the message and the potential biases involved.





Conclusion

Misinformation, disinformation, and fake news are complex issues that can be solved by taking a multifaceted approach, including understanding the definitions, impact, and ways to combat these issues.



[Click here for the training. Enroll on 16-18year olds](#) (Guide below)

STEP 1

Click on “Enroll here”

Training Modules

In partnership with the National Cybersecurity Authority of the Kingdom of Saudi Arabia, ITU and partners are launching a set of online self-paced trainings on child online protection, geared towards the following target groups: parents, educators, policy-makers, ICT industry, and children themselves (aged 9-12, and 13-15 and 16-18).

Online training for children aged 9 to 12 years old is out! [ENROLL HERE](#)
Online training for children aged 13 to 15 years old is out [ENROLL HERE](#)
Online training for children aged 16 to 18 years old is out [ENROLL HERE](#)

[Click here](#) to discover more about the trainings and our new releases:
Our app and game for children

Online training on Children's Rights and Business in the digital environment is out! [Click here for more details](#).

The trainings for parents, carers, educators and policymakers are accessible on the ITU Academy [here](#).

[Click here](#) to discover more about the new language versions of the trainings.

Stay tuned looking out for new trainings coming soon!



NEW!

NEW!

STEP 2

Click on “Next”

Training on Child Online Protection for 16 to 18 year olds

Hello!

Welcome to the training on Child Online Protection for 16 to 18 year olds.

To earn your badge, complete all three modules of the course.

Get Started!

Next

STEP 3

Fill the form



Please fill the form to access the course

*Are you 16-18 years old?



Yes



No

*Which Country are you from?

*Do you live in:

☐ Choose one of the following answers

☐ A big city

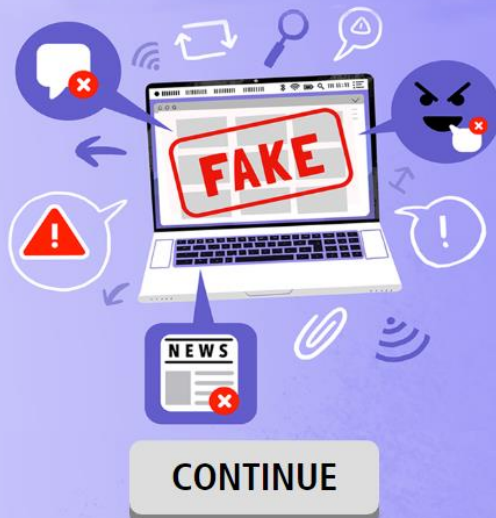
STEP 4

Training material provided

NB: Focus on module 3 however,
you can learn module1&2

Module 3: Online Safety Lessons Fake News and Mis/Disinformation

Click the button below to continue.



Module 6

MODULE 6- INTERNET AND ONLINE SAFETY

MODULE 4-INTERNET AND ONLINE SAFETY

Introduction

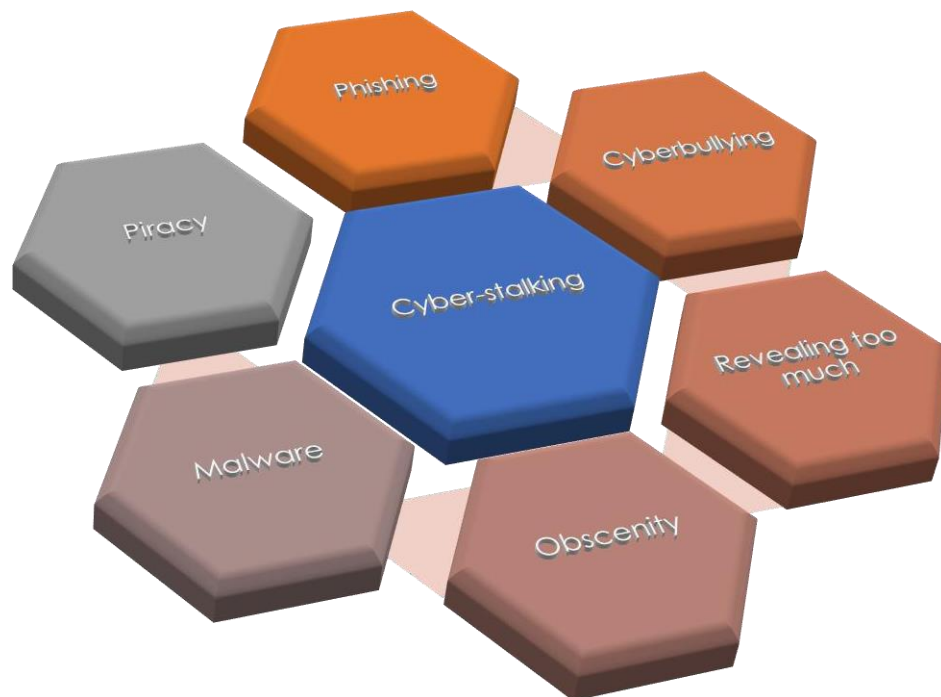
The Internet can be a wonderful place to learn, shop, play games, and talk to your friends. Unfortunately, there are also predators, identity thieves, and others online who may try to harm you. In order to be safe online, it's important for you and your kids to be aware of the dangers. Many children are confident that they know how to be safe online. However, there are a few reasons children are often more at risk. They may not always think about the consequences of their actions, which can cause them to share too much information about themselves. Children also are sometimes specifically targeted by cyberbullies or predators. If you're a parent or guardian, you can help to keep your children safe by **talking to them about their Internet use, teaching them about online dangers, and learning everything you can about the Internet** so you can make informed decisions. In order to keep your children safe, you'll need to know about the **different types of online dangers** that exist. For example, children and teens may find inappropriate content on the Internet, such as pornography or obscene language. There is also a possibility of cyberbullying or cyber harassment from others online. This does not mean your child will encounter all of these threats. However, knowing about the dangers can help you and your children make smart decisions online.

Importance of Limiting Children's Internet Use

- a. Whenever someone uses a computer, there is a risk of **eye strain, wrist strain, and other injuries**. You can help prevent this by limiting the amount of time your children spend on computers and mobile devices.
- b. There's also another reason to limit your children's Internet use: Because people are spending more and more time online, **Internet addiction** is becoming a more

significant problem. Internet use can be a good thing, but if it becomes an addiction, it can affect a person's offline life.

- c. It's important for children to be careful whenever they're connected to the Internet because online dangers are not just limited to **bad websites**. Chat rooms, computer games, and even social networking sites can be risky. If your children have mobile phones, they'll also need to be careful when texting or when accessing the Internet on their phones.



1. Figure 1: A figure showing some dangers children can encounter online.

Places where Children can be at Risk.

- a. Children may encounter threats in the following places:
- b. Instant Messaging (IM) & Chat
- c. Computer Games which have built-in chat
- d. Texting
- e. Email
- f. Software Downloads
- g. Social Networking Sites (Example: Facebook)

h. File Sharing Networks (also called peer-to-peer networks or P2P)

2. Staying Safe from Online Predators

The Internet is much more anonymous than the real world. People can hide their identities or even pretend to be someone they're not. This can sometimes present a real danger to children and teens who are online. Online predators may try to lure children and teens into sexual conversations or even face-to-face meetings. Predators will sometimes send obscene material or request that kids send pictures of themselves. Therefore, it's important to **teach your children to be on their guard** whenever they're online.

Teens are generally more at risk from predators. Because they are curious and want to be accepted, they **may talk to a predator willingly**, even if they know it's dangerous. Sometimes teens may believe they are in love with someone online, making them more likely to agree to a face-to-face meeting.

Guidelines to help Children Stay Safe from Online Predators

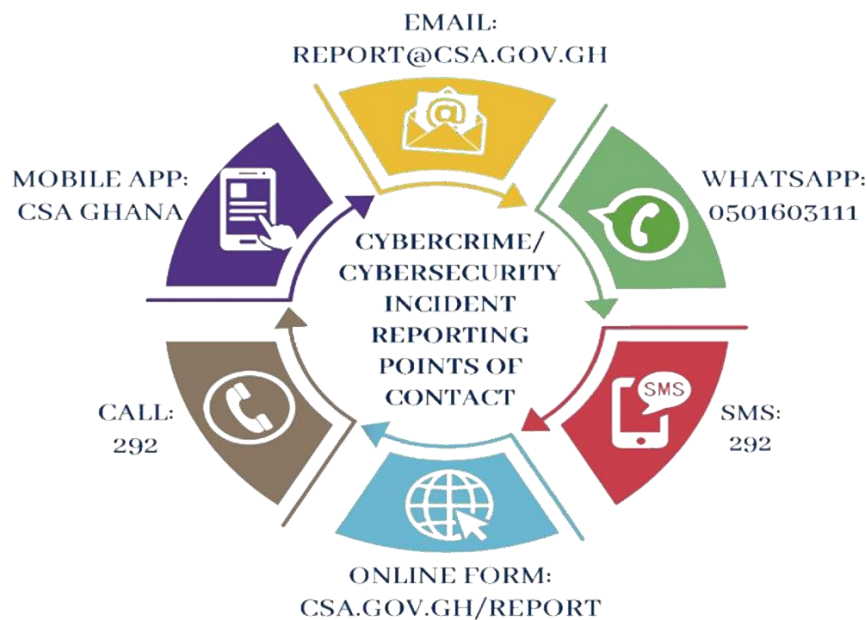
- **Avoid using suggestive screen names or photos.** These can result in unwanted attention from online predators.
- **If someone is flattering you online, you should be wary.** Although many people online are genuinely nice, predators may use flattery to try to start a relationship with a teen. This doesn't mean you need to be suspicious of everyone, but you should be careful.
- **Don't talk to anyone who wants to get too personal.** If they want to talk about things that are sexual or personal, you should end the conversation. Once you get pulled into a conversation (or a relationship), it may be more difficult to stop.
- **Keep in mind that people are not always who they say they are.** Predators may pretend to be children or teenagers to talk to kids online. They may use a fake profile picture and add other profile details to appear more convincing.
- **Never arrange to meet with someone you met online.** Predators may try to arrange a face-to-face meeting with a child or teen. Even if the person seems nice, this can be dangerous.
- **Tell a parent or trusted adult if you encounter a problem.** If anyone makes you feel uncomfortable online, you should tell a parent or trusted adult

immediately. You should also save any emails or other communication because they may be needed as evidence.

3. Cybersecurity Cybercrime Incident Reporting Points of Contact

- Cyber Security Authority

Report cybersecurity incidents or seek further guidance from the Cyber Security Authority (CSA) through the following channels.



- Call the Police where necessary.

4.0 Cyberbullying and Cyber harassment

Cyberbullying is bullying that occurs online, often through instant messaging, text messages, emails, and social networks. Cyberbullies may be the same age as the victims, or they may be older. If the perpetrator is an adult, it is generally called **cyber-stalking** or **cyber harassment**.

Cyberbullying can be just as hurtful as other types of bullying, and in some ways it can be worse. Cyberbullying is not limited to the playground; it can occur anytime children are online, even if they're at home. Also, the bully can sometimes remain anonymous, which can make the bullying more difficult to stop.

4.1 Examples of Cyberbullying

- Writing hurtful things through instant messaging, text messaging, or online games

- Posting derogatory messages on social networking sites
- Posting or sharing embarrassing photos or videos
- Creating a fake profile in order to humiliate someone.

4.2 Responding to Cyberbullying

- **Don't reply to the bully.** Bullies often want to get a reaction from their victims. If you ignore them, they may lose interest.
- **If possible, block messages from the bully.** If the bullying is happening in chat, email, or on a social networking site, you can usually block all messages from the bully.
- **Keep all emails and other messages that the bully sends.** You may need to use these as evidence at some point.
- **Report the bullying to a parent or trusted adult.** If the bullying continues, tell a parent or trusted adult (such as a teacher) so they can help you deal with the problem.

4.3 Identifying Cyberbullying

Kids can be mean sometimes. Unfortunately, the Internet often makes it easier for people to say hurtful things because it's more impersonal and anonymous than real life. As a result, **many kids participate in cyberbullying even though they don't consider themselves bullies.**

It's important for your children to understand that the comments they make online can hurt just as much as those made face to face. Make sure they know **not to say anything online that they wouldn't say in person.**

It's also possible for kids to face serious consequences for cyberbullying. Many schools now have **zero-tolerance policies** for bullying, which may include cyberbullying that occurs outside of school. In some cases, students have even been suspended from school for cyberbullying.

5. Using social media Safely.

Social networking sites are more popular than ever, and they've changed the way people use the Internet. Some of the most popular sites are Facebook, Instagram, and Twitter. These sites allow people to keep in touch with their friends, share links, plan events, and more.

- For many teens and even younger children, online social networking is an **important part of their lives** because it lets them talk to their friends no matter where they are. Social networks aren't a bad thing, but there are a few risks your kids will need to be aware of.

5.1 Social Media Usage Guidelines



- **Keep your posts private.** On most social networking sites, you can choose to only share things with your friends. It's important to use this setting whenever possible because it makes it more difficult for people you don't know to gain access to your information.
- **Check your privacy settings frequently.** Facebook sometimes reorganizes its privacy and account settings, which can cause your information to be shared with more people than you want. With Facebook or any other social networking site, you should review your privacy settings to make sure they are set the way you want them to be.

Privacy Settings for some Social Media Accounts

1. Instagram

Note: If you are under 16 when you sign up for an Instagram account, you'll have the option to choose between a public or private account, but **Private** is selected by default. If you're over 16, your Instagram account is public by default, and you can choose to make your account private at any time. Learn more about how to make your account private below.

To make your account private:

- Click  **More** in the bottom left, then click **Settings** .
- Click **Who can see your content**.
- Below **Account Privacy**, click to check the box next to **Private Account**.
- Click **Switch to private** to confirm.
- Keep in mind that business profiles aren't able to make their accounts private. If you want to make your business account private, first switch back to a personal account.

2. LinkedIn

The Privacy tab covers all privacy and security settings related to what can be seen about you, how information can be used, and downloading your data.

To access your LinkedIn privacy settings:

- Click the Me icon at the top of your LinkedIn homepage.

- b. Select **Settings & Privacy** from the dropdown.
- c. Click the **Data Privacy** on the left rail.
- d. You'll find the following sub-sections in the Data privacy section:

How LinkedIn uses your data:

- a. Manage the ways your data is used on LinkedIn.
- b. **Who can reach you:** Manage invitations and messages.
- c. **Messaging experience:** Choose how you would like LinkedIn to customize your experience. This includes read receipts, typing indicators, and reply to suggestions.
- d. **Job seeking preferences:** Set your preferences regarding job seeking, including letting recruiters know you're open to opportunities.
- e. **Other applications:** Control how associated accounts can use your data.

3. Facebook

- a. Review and update your privacy settings for your profile.
- b. Limit who can see your past posts.
- c. Go to your Activity Log to review your posts and things you've been tagged in.
- d. Visit your Profile and Tagging settings to manage things like who can see what other people post on your profile and review who can see content you're tagged in.
- e. Edit basic info on your Facebook profile and choose who can see it.
- f. Learn more about who can see your posts in groups or on a Page, and how to choose who can see your story.
- g. Let's give you a way to share with a specific audience. You can use the audience selector to choose the list you want to share a post with.
 - From the top of your Feed, click **What's on your mind, [name]?**
 - Click the audience selector.
 - Click the name of the list you want to share with.
 - Click **Post**.

You can use the audience selector to change who can see things (example: posts and photos) you share on your timeline after you share it. Keep in mind, when you share something on someone else's timeline, they control the audience for the post.

- **Be careful what you share.** Even if you're keeping posts private, it doesn't guarantee that other people won't be able to see it. For example, if you share a photo with your friends, they can easily save it to their computers and post it to

another website. You shouldn't post something online unless you're comfortable with everyone in the world seeing it.

- **Don't add strangers to your friends list.** Although it may be tempting to have thousands of "friends" online, this increases the chances that your photos and personal information will be shared with the world.
- **Keep in mind that things you post online may stay there for years.** Even if something doesn't seem embarrassing, it may damage your reputation years later when you're looking for a job or applying to college. Employers and colleges often check social networking sites for information on candidates, so a photo or other post could lower their impression of you.
- **Use good netiquette.** Netiquette is a set of guidelines for communicating online. Using good netiquette helps to ensure that the things you say aren't misinterpreted. Example: In forums, chats, social networks, or WhatsApp groups, express your opinion with respect and never attack others.

Recommendations for Setting up a social networking profile.

- **Screen name**

Should you use your full name, first name only, or a pseudonym (fictitious name)? It may be okay to use your full name on sites like Facebook and LinkedIn where you can limit your sharing to the people you know. On a message board or chat room, you should not use your full name, since you are interacting with people you don't know. Instead, you can just use your first name or a pseudonym.

- **Profile picture**

Many sites allow you to choose a profile picture. This can either be a photo or an avatar, which is a graphical image that represents you. On Facebook, most people use photos of themselves. However, on a more public site (such as a discussion board), you may want to use an avatar, as it allows you to remain more anonymous.

Keep in mind that many different people will be able to see your profile picture. Therefore, it's important to choose a picture that won't reflect negatively on you. It's possible for a photo to get you into trouble at school or damage your reputation.

- **Profile information**

You should be careful about what personal information you share. If you have the option of making your info private to just you and your friends, you should choose this option. You should never make your birthday or home address publicly viewable.

- **Contact information.**

Generally speaking, you do not want to include any contact information other than your email address. Do not use home phone numbers or addresses. If you must include a phone number, use a mobile phone number.

It may also be a good idea to create a separate email address for social networking connections in order to protect your normal account from getting cluttered with spam and phishing emails.

- **Image and persona**

Many sites allow you to customize your profile with wallpaper, personal interests, likes and other types of information like relationship status. Always keep in mind what type of public image you want to project as you choose how to customize your profile and what types of information to include.

Your online image will become more important when you begin applying for jobs or to college. Anything that is inappropriate may lower someone's impression of you. Even if you're not worried about it now, don't post anything that's going to come back to haunt you in a few years.

Understanding File-Sharing Networks

File-sharing networks became popular in the late 1990s when Napster was first created. Napster used a kind of technology called peer to peer (or P2P), which allowed people to share music with others around the world.

Napster was shut down due to legal reasons, but since then many more P2P programs have appeared. Unlike Napster, these programs not only let people share music but also TV shows, movies, and software. Unfortunately, there are many risks associated with these programs, which range from viruses to legal trouble, so to be safe it's best to keep your kids away from them.

Basic Legal Issues of File Sharing

In theory, you can use a file-sharing network to download and share files that aren't copyrighted. The problem is that most software, music, TV shows, and movies **are copyrighted**, and there can be stiff penalties if you're caught downloading or sharing them. For example, in 2006 Jammie Thomas was sued by several record labels for sharing music on the Kazaa file-sharing network. She was ordered to pay \$1.5 million in damages, which was later reduced to \$54,000.

Keep in mind that some songs and TV episodes can be downloaded for free from the **iTunes Store** and other places, and a lot of software is also free. So, if your kids have downloaded something without paying for it, it doesn't necessarily mean they've done anything wrong.

File Sharing Safety

Downloading a file through a P2P network is generally riskier than downloading it from a website. Many files on P2P networks carry viruses or other malware. Also, when sharing files, you are giving other people access to the files on your computer. Although most people try to only share specific folders, it's possible to accidentally share the entire contents of your computer.

There is also a risk of your kids encountering pornography or other inappropriate content through file-sharing networks. Even if you have parental controls set up on your computer, they may not catch these files.

Examples of File-Sharing Programs

There are countless file-sharing programs out there, so it would be impossible to list all of them. Here are a few of the most common ones:

- BitTorrent
- uTorrent
- FrostWire
- BitComet
- Ares Galaxy

Recommended Guidelines for Keeping Children Safe Online

It can be difficult to keep your kids completely safe online. Even if you set up parental controls on your home computer, your kids will use many other computers that don't have parental controls. To keep your kids safe, you'll need to teach them to make good decisions online—even when you're not around.

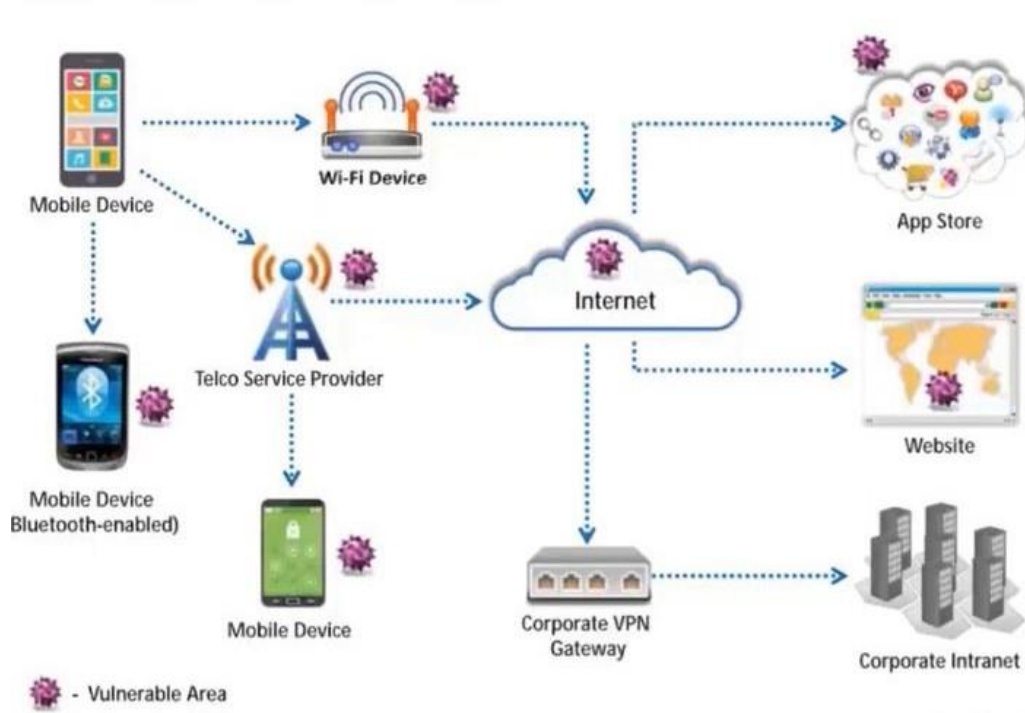
Below are some general tips you can use when teaching your kids about online safety:

- **Learn everything you can about the Internet.** Being familiar with the Internet will not only help you understand the risks, but it will also help you talk to your kids.
- **Set standards for what your kids can and cannot do online.** It's important to make rules for your kids so they know what's expected of them. Don't wait until something bad happens to start creating guidelines.
- **Teach your kids to keep personal information private.** It's usually a bad idea to post personal information online such as phone numbers, addresses, and credit cards. If criminals gain access to this information, they can use it to harm you or your family.
- **Teach your kids to use social networking sites safely.** Sites like Facebook allow kids—and adults—to share photos and videos of themselves, as well as have conversations with friends and strangers. If your kids share something with friends, it's still possible for it to get into the wrong hands. Generally, they should only post something online if they're comfortable with everyone in the world seeing it.
- **Encourage your kids to come to you if they encounter a problem.** If your child gets into trouble online, you'll want him or her to come to you instead of hiding it. Keep in mind that your kids could accidentally encounter a bad site, even if they're doing everything right.
- **Talk to your kids about Internet use.** Talk to your kids regularly about how they use the Internet. If they're in the habit of talking to you about the Internet, they'll be more willing to come to you if there's a problem.

Module 7

MODULE 7- MOBILE DEVICE SAFETY

1. Mobile security guidelines and tools.



Introduction and Overview

Mobile Device Security refers to the measures designed to protect sensitive information stored on and transmitted by laptops, smartphones, tablets, wearables, and other portable devices. At the root of mobile device security is the goal of keeping unauthorized users from accessing the enterprise network.

Mobile devices have become an integral part of our daily lives, with more people relying on them for tasks such as communication, online banking, and e-commerce. However, this increased reliance on mobile devices has also made them a prime target for cybercriminals who seek to exploit vulnerabilities in the mobile device ecosystem. In this context, mobile security refers to the measures that are taken to protect mobile devices and the data they contain from cyber threats.

Examples of Mobile Devices include, tablets, laptops, wearable devices such as smart watches and fitness trackers, handheld game consoles, smart phones.

Kinds of Sensitive Data Stored on Mobile Devices

Mobile devices can store various kinds of sensitive data that could be of interest to cyber criminals:

- a. **Personal Information:** Personal information, such as names, addresses, phone numbers, and email addresses, is often stored on mobile devices in contact lists, email clients, and messaging apps.
- b. **Financial Data:** Mobile devices can store financial data, such as credit card/VISA information, bank account information, and payment app credentials including mobile money pins/passwords.
- c. **Health Information:** Mobile devices can store health information, such as medical records, prescriptions, and health monitoring data.
- d. **Location Data:** Mobile devices can store location data, such as GPS coordinates and location histories, which can reveal information about a user's activities and habits.
- e. **Passwords and Login Credentials:** Passwords and login credentials for various accounts, such as email, social media, and banking, are often stored on mobile devices for easy access.
- f. **Business Information:** Mobile devices used for work purposes can store business information, such as confidential documents, client information, and trade secrets.
- g. **Personal Media:** Personal media, such as photos, videos, and audio recordings, can also be sensitive and may need to be protected from unauthorized access.

It is important to protect these sensitive data on mobile devices from unauthorized access, theft, or loss. In the wrong hands, this data can be used to commit various types of crime including identity theft, payment fraud, among others.

Threats to Mobile Devices

Threats to mobile devices can be categorized into four (4) main sections.

a. Web-based Threats

- **Malicious Websites:** Malicious websites can infect mobile devices with malware, spyware, or viruses, often through drive-by downloads or social engineering tactics.
- **Phishing:** Phishing attacks can target mobile device users through fake emails, text messages, or social media accounts, tricking users into revealing sensitive information or installing malware.
- **Drive-By Downloads:** Drive-by downloads occur when malware is automatically downloaded and installed on a mobile device when visiting a malicious website or clicking on a malicious link.

- **Man-in-the-Middle (MitM) Attacks:** MitM attacks can intercept mobile device traffic and steal sensitive information, such as login credentials or financial data when surfing the web on an unsecured network.

b. App-based Threats

- **Rogue Apps:** Rogue apps are malicious apps that masquerade as legitimate apps on app stores, but actually perform malicious activities, such as stealing data or displaying unwanted ads. They can also be downloaded from third-party app stores or other sources.
- **Unpatched Vulnerabilities:** Unpatched vulnerabilities in mobile apps can be exploited by attackers to gain access to sensitive information or perform other malicious activities.

c. Network-based threats

- **Man-in-the-Middle (MitM) Attacks:** Public Wi-Fi networks and other unsecured networks can be used by cybercriminals to intercept and steal sensitive information through MitM attacks.
- **Unattended Network Connection:** Wireless networks and communications protocols (Bluetooth, Wi-Fi and location services) when turned on and not attended to can open up a mobile device to various forms of attacks by cybercriminals.

d. Physical Threats

- **Theft:** Mobile devices are often targeted by thieves due to their high value and portability, and the theft of a mobile device can result in the loss of sensitive information or data.
- **Loss:** Losing a mobile device can also result in the loss of sensitive information or data, especially if the device is not password-protected or encrypted.
- **Shoulder Surfing:** Shoulder surfing is a type of physical threat to mobile device security that involves an attacker looking over the shoulder of a mobile device user to obtain sensitive information, such as login credentials or personal data. Shoulder surfing can occur in public places, such as coffee shops, airports, or trains, where mobile device users may be using their devices near others.

Securing Mobile Devices

To protect mobile devices from these threats, users should follow best practices highlighted below.

- **Passwords and Biometric Authentication:** Use strong passwords or biometric authentication, such as fingerprints or facial recognition, to prevent unauthorized access to your device.

- **Keep Software and Apps Up to date:** Install the latest software and app updates, which often contain important security fixes and patches.
- **Install Security Software:** Install reputable security software, such as antivirus and anti-malware, to protect your device from malicious software.
- **Avoid Public Wi-Fi:** Avoid using public Wi-Fi, which is often unsecured and can expose devices to security risks.
- **Disable wireless connections:** Disable Bluetooth, near field communication (NFC), Wi-Fi and location services when you are not using them, as they can be vulnerable to attacks.
- **Be Careful with Downloads:** Only download apps and files from reputable sources, such as the official app store, and be wary of suspicious links or attachments.
- **Backup Your Data:** Regularly backup your data to prevent data loss in case of theft, damage, or other incidents.
- **Enable Remote Wiping:** Enable remote wiping, which allows you to erase all data from your device if it is lost or stolen.
- **Enable Multi/two-factor authentication:** Multi/two-factor authentication adds an extra layer of security to the device by requiring users to enter a second authentication factor, such as a fingerprint or a code sent to their mobile phone.
- **Avoid jailbreaking/rooting:** Avoid jailbreaking/rooting the device as it can remove important security features.

By implementing these countermeasures, users can enhance the security of their mobile devices and protect their sensitive data from cyber threats.

Measures that parents can take to protect their children's mobile devices:

1. **Use parental controls:** Most mobile devices have built-in parental control features that can help parents restrict access to certain apps or content, set time limits, and monitor their child's online activity.
2. **Limit access to sensitive information:** Parents/guardians should ensure that their child's mobile device does not contain sensitive information, such as credit card numbers, social security numbers, or other personal information.
3. **Install security software:** Parents/guardians should install antivirus software on their child's mobile device to protect against malware and other security threats.
4. **Check age rating for online accounts and app:** Parents/guardians need to check the age rating of apps and ensure to sign up with the right ages of the child. This helps the app administrators to filter contents and protect children.
5. **Teach safe online behaviour:** Parents/guardians should educate their children about safe online behaviour, such as not sharing personal information, not accepting friend requests from strangers, and avoiding inappropriate content.

6. **Monitor online activity:** Parents/guardians should monitor their child's online activity and review their browsing history and social media activity to ensure that they are not accessing inappropriate content or communicating with strangers.
7. **Use privacy settings:** Parents/guardians should adjust privacy settings on their child's mobile device and social media accounts to limit who can see their child's posts and information.
8. **Use strong passwords:** Parents/guardians should ensure that their child's mobile device is protected by a strong password or PIN code to prevent unauthorized access.
9. **Keep software updated:** Parents/guardians should ensure that their child's mobile device is always running the latest software updates to ensure that any security vulnerabilities are addressed.
10. **Use secure networks:** Parents/guardians should ensure that their child's mobile device is only connected to secure and trusted networks, such as their home Wi-Fi network.

Overall, by implementing these measures, parents can help protect their child's mobile device and ensure that they are using it safely and responsibly.

Mobile Security Hacking and Terminologies

Mobile platform hacking refers to the process of exploiting vulnerabilities in the software or hardware of a mobile device's operating system to gain unauthorized access or control over the device.

- a. **Rooting or jailbreaking:** This involves removing the software restrictions imposed by the mobile operating system, which can enable the attacker to gain access to sensitive information, install malicious software or perform other unauthorized actions.
- b. **Network attacks:** Attackers can exploit vulnerabilities in the mobile network to intercept traffic and gain access to sensitive data.
- c. **Social engineering:** This involves manipulating users into providing sensitive information such as login credentials or personal information through techniques such as phishing emails, fake websites, or social media scams.
- d. **Code injection:** Attackers can exploit vulnerabilities in mobile applications by injecting malicious code into legitimate apps, allowing them to take control of the device or steal data.
- e. **Outdated software:** refers to software applications or systems that are running on older versions or releases that have not been updated with the latest security patches, bug fixes, or feature enhancements provided by the software vendor.

Outdated software is a common vulnerability in Android devices, as many users do not update their devices regularly.

- f. **Open-source vulnerabilities:** Android is built on open-source software, which can sometimes contain vulnerabilities that can be exploited by attackers.
- g. **Exploit:** an exploit is a piece of software, code, or technique that takes advantage of a vulnerability or weakness in a computer system, software application, or network to gain unauthorized access or perform malicious actions.
- h. **Phishing:** Phishing is a social engineering attack in which attackers trick users into giving away sensitive information such as usernames and passwords.
- i. **Encryption:** Encryption is the process of encoding data to prevent unauthorized access to it. Mobile devices can use encryption to protect sensitive data such as passwords, credit card numbers, and other personal information.
- j. **VPN:** A Virtual Private Network (VPN) is a secure connection between a mobile device and a remote server. A VPN can be used to encrypt traffic and protect a user's privacy while using public Wi-Fi networks.
- k. **Brute-Force Attack:** A brute-force attack is a hacking technique in which an attacker uses automated software to try every possible combination of characters to guess a user's password.
- l. **Backdoor:** A backdoor is a hidden entry point into a mobile device's operating system that can be used to bypass security measures and gain unauthorized access to the device.

Module 8

MODULE 8- SOCIAL ENGINEERING

MODULES 8- SOCIAL ENGINEERING

1. What is Social Engineering?

Social Engineering is the manipulation technique that exploits human error to gain private information, access, or valuable.

Social Engineering is the term used to describe any cyberattack where a human (rather than a computer) is the target; for this reason, it is sometimes referred to as "People Hacking".

Attacks can occur online, in-person, and via other interactions.

The Objective of Social Engineering Attackers

- a. **Sabotage** - Disrupting or corrupting data to cause harm or inconvenience.
- b. **Theft** - Obtaining valuables like information, access, or money.

Traits of Social Engineering Attacks

- c. **Heightened emotions** – Emotional manipulation gives the attacker the upper hand in any interaction. Victims are more likely to take irrational or risky actions when in an enhanced emotional state. Fear, excitement, curiosity, anger, guilt, and sadness are types of emotions used in equal measure to convince victims.
- d. **Urgency** – Time- sensitive opportunities or requests are another reliable tool used by social engineering attackers. Victims may be motivated to compromise themselves under the guise of a serious problem that needs immediate attention.
- e. **Trust** – Confidence used by the attacker to craft a narrative that the victim can easily believe and is unlikely to rouse suspicion. Believability is invaluable and essential to a social engineering attack.

Types of Social Engineering Attack

S/N	Types of Social Engineering	Definition
1	Phishing	<p>Phishing is a social engineering technique in which an attacker pretends to be a trusted institution or individual in an attempt to persuade the victim to expose personal data or other valuable information.</p> <p>Attacks using phishing are targeted in one of two ways:</p> <ol style="list-style-type: none"> 1. Spam phishing or mass phishing is a widespread attack aimed at many users. These attacks are non-personalized and try to catch any unsuspecting person. 2. Spear phishing or whaling is the use of personalized information to target users. Whaling attacks specifically aim at high-profile individuals like celebrities, political leaders, and heads of institutions. <p>Types of Phishing</p> <ul style="list-style-type: none"> • Email phishing is the email means of phishing to urge the victim to reply or follow-up on an email request via web links, phone numbers, or malware attachments. • Angler Phishing takes place on social media, where an attacker imitates a trusted company customer service team. The attacker intercept communication between a customer and an institution to hijack and divert conversation in private messages to advance attacks. • Search engine phishing attempts to place links to fake websites at the top of search results. • User Resource Locator (URL) phishing links tempt victims to click on phishing websites. URL links are usually delivered in emails, text messages, social media messages and online advertisements. • In-session phishing appears as an interruption to your normal web browsing. • Vishing (short for Voice phishing) occurs when a fraudster attempts to trick a victim into discussing sensitive information or giving them access to the victim's computer over the telephone. One popular vishing scheme involves the attacker calling victims and pretending to be from a telecommunication company.

		<ul style="list-style-type: none"> Smishing (short for Voice phishing or SMS phishing) occurs when a fraudster attempts to trick a victim into discussing sensitive information or giving them access to the victim's computer through SMS or text messaging.
2	Pretexting	<p>Pretexting is a type of social engineering where the attacker creates a scenario where the victim feels compelled to comply under false pretenses. Typically, the attacker will impersonate someone in a powerful position to persuade the victim to follow their orders.</p> <p>Pretexting uses a deceptive identity as the "pretext" for establishing trust, such as directly impersonating a vendor or a facility employee. This approach requires the attacker to interact with you more proactively. The exploit follows once the attacker have convinced the victim that they are legitimate.</p>
3	Baiting	<p>Baiting puts something enticing or curious in front of the victim to lure them into the social engineering trap.</p> <p>Baiting abuses the victim's natural curiosity to coax them into exposing valuable information to the attacker.</p> <p>Methods of Baiting can include:</p> <p>Use of USB drives left in public spaces like libraries and parking lots.</p> <p>Email attachments including details on a free offer or fraudulent free software.</p>
4	Quid Pro Quo Attacks	<p>Quid pro quo is a term which means "a favor for a favor", an exchange of personal information for some reward or other compensation. The exploit comes from getting the victim excited for something valuable that comes with a low investment from the victim. However, the attacker simply takes the victim's data with no reward or compensation for the victim.</p>
6	Tailgating	<p>Tailgating is a social engineering attack used to gain physical access to an unauthorized location. Tailgating is achieved by closely following an authorized user into the area without being noticed by the authorized user.</p>
7	Piggybacking	<p>Piggybacking is a social engineering attack used to gain physical access to an unauthorized location by following an authorized person who has legitimate access.</p>

8	Shoulder surfing	Shoulder surfing is a social engineering technique used by attackers to obtain sensitive information, such as passwords or credit card numbers, by looking over someone's shoulder as they enter or access the information.
---	------------------	---

Stages of Social Engineering

1. **Prepare** by gathering background information on you or a larger group you are a part of.
2. **Infiltrate** by establishing a relationship or initiating an interaction, starting by building trust.
3. **Exploit** the victim once trust and weakness are established to advance the attack.
4. **Disengage** once the user has taken the desired action.

How to Spot Social Engineering Attacks

Defending against social engineering requires you to practice self-awareness. Always slow down and think before doing anything or responding.

Attackers expect you to take action before considering the risks, which means you should do the opposite. To prevent being a victim of social engineering attacks, look out for these questions:

- **Are my emotions heightened?** When you're especially curious, fearful, or excited, you're less likely to evaluate the consequences of your actions. In fact, you probably will not consider the legitimacy of the situation presented to you. Consider this a red flag if your emotional state is elevated.
- **Did this message come from a legitimate sender?** Inspect email addresses and social media profiles carefully when getting a suspect message. There may be characters that mimic others, such as "torn@example.com" instead of "tom@example.com." Fake social media profiles that duplicate your friend's picture and other details are also common.
- **Did my friend actually send this message to me?** It's always good to ask the sender if they were the true sender of the message in question. Whether it was a co-worker or another person in your life, ask them in-person or via a phone call if possible. They may be hacked and not know, or someone may be impersonating their accounts.
- **Does the website I'm on have odd details?** Irregularities in the URL, poor image quality, old or incorrect company logos, and webpage typos can all be red flags of a fraudulent website. If you enter a spoofed website, be sure to leave immediately.
- **Does this offer sound too good to be true?** In the case of giveaways or other targeting methods, offers are a strong motivation to drive a social engineering attack forward. You should consider why someone is offering you something of value for little gain on their end. Be wary at all times because even basic data like your email address can be harvested and sold to unsavory advertisers.

- **Are attachments or links suspicious?** If a link or file name appears vague or odd in a message, reconsider the authenticity of the whole communication. Also, consider if the message itself was sent in an odd context, or time, or raises any other red flags.
- **Can this person prove their identity?** If you cannot get this person to verify their identity with the organization, they claim to be a part of, do not allow them the access they are asking for. This applies both in-person and online, as physical breaches require that you overlook the attacker's identity.

How to Prevent Social Engineering Attacks

Beyond spotting an attack, you can also be proactive about your privacy and security. Knowing how to prevent social engineering attacks is incredibly important for all mobile and computer users. Here are some important ways to protect against all types of cyberattacks:

- **Never click on links in any emails or messages.** You'll want to always manually type a URL into your address bar, regardless of the sender. However, take the extra step of investigating to find an official version of the URL in question. Never engage with any URL you have not verified as official or legitimate.
- **Avoid sharing names of your schools, pets, place of birth, or other personal details.** You could be unknowingly exposing answers to your security questions or parts of your password. If you set up your security questions to be memorable but inaccurate, you'll make it harder for a criminal to crack your account. If your first car was a "Toyota," writing a lie like "clown car" instead could completely throw off any prying hackers.
- **Be very cautious of building online-only friendships.** While the internet can be a great way to connect with people worldwide, this is a common method for social engineering attacks. Watch for tells and red flags that indicate manipulation or a clear abuse of trust.
- To protect against shoulder surfing, individuals should be cautious about entering sensitive information in public or semi-public areas and try to position themselves so that others cannot easily see their screens.
- Protection against social engineering starts with education. If all users are aware of the threats, our safety as a collective society will improve. Be sure to increase

awareness of these risks by sharing what you've learned with your coworkers, family, and friends.

Module 9

MODULE 9- COP LEGAL

MODULE 9- COP LEGAL

The Cybersecurity Act, 2020, (1038) established the Cyber Security Authority (CSA) to regulate Cybersecurity activities and promote the development of Cybersecurity in the country. Pursuant to section 4(j) of the Cybersecurity Act, 2020 (Act 1038), the CSA is mandated to promote the protection of children online.

There are provisions in the act that protect children, that is section 62-68.

1. Indecent image or photograph of a child

Section 62 (1) – A person shall not

- (a) take or permit to be taken an indecent image or photograph of a child.
- (b) produce or procure an indecent image or photograph of a child for the purpose of the publication of the indecent image or photograph through a computer system.
- (c) publish, stream, including live stream, an indecent image or photograph of a child through a computer or an electronic device; or
- (d) possess an indecent image or photograph of a child in a computer system or on a computer or electronic record storage medium.

2. Penalty for indecent image or photograph of a child

- 2) A person who does any of the above commits an offence and is liable on summary conviction:
 - to a fine of not less than two thousand five hundred penalty units and not more than five thousand penalty units or
 - to a term of imprisonment of not less than five years and not more than ten years or to both.
- 1 penalty unit = 12 cedis

3. Meaning of publication of indecent image or photograph of a child

A person publishes an indecent photograph, image or visual recording if that person:

- parts with possession of the indecent photograph, image or recording to another person; or
- exposes or offers the indecent photograph, image or recording for acquisition by another person.

4. Includes a material image, visual recording, video, drawing or text that depicts:

- a child engaged in sexually explicit or suggestive conduct.

- a person who appears to be a child engaged in sexually explicit or suggestive conduct.
- images representing a child engaged in sexually explicit or suggestive conduct.
- sexually explicit images of children.
- any written material, visual representation or audio recording that promotes sexual activity with children that would be an offence under any law in Ghana.
- any written material of sexual activity with a child that would be an offence under any law in Ghana; or
- any audio recording of sexual activity with a child that would be an offence under any law in Ghana.
- any written material, visual representation or audio recording that promotes sexual activity with children that would be an offence under any law in Ghana.
- any written material of sexual activity with a child that would be an offence under any law in Ghana; or
- any audio recording of sexual activity with a child that would be an offence under any law in Ghana.

5. Dealing with a child for purposes of sexual abuse

- 63. (1) A person shall not use
 - a computer online service,
 - an internet service,
 - a local bulletin board service, or
 - any other device capable of electronic data storage or transmission
- to seduce, solicit, lure, groom or entice, or **attempt to** seduce, solicit, lure, groom or entice, a child or another person believed by the person to be a child, for the purpose of facilitating, encouraging, offering, or soliciting unlawful sexual conduct of or with any child, or the visual depiction of such conduct.

6. Penalty for dealing with a child for purposes of sexual abuse.

A person who deals with a child for purposes of sexual abuse commits an offence and is liable on summary conviction to a term of imprisonment of not less than five years and not more than fifteen years.

7. Aiding and abetting of child dealing for purposes of sexual abuse

- Section 64 (1) - An owner or operator of a computer on-line service, weblog, internet service, or internet bulletin board service shall not:
 - aid and abet another person for the purpose of facilitating or encouraging the on-line solicitation of a child; or
 - permit any person to use the service of that person for the purpose of facilitating,

encouraging, offering, or soliciting unlawful sexual conduct of or with a child, or the visual depiction of such conduct.

- (2) the penalty for this offence upon summary conviction is a term of five years to fifteen years imprisonment.

8. Cyberstalking of a child

- 65. (1) A person shall not use a computer online service, an internet service, or a local internet bulletin board service or any other electronic device to compile, transmit, publish, reproduce, buy, sell, receive, exchange, or disseminate the name, telephone number, electronic mail address, residence address, picture, physical description, characteristics, or any other identifying information on a child in furtherance of an effort to arrange a meeting with the child for the purpose of engaging in sexual intercourse, sexually explicit conduct, or unlawful sexual activity
- (2) A person who cyberstalks a child commits an offence and is liable on summary conviction to a term of five to fifteen years imprisonment.

9. Sexual extortion

- Section 66. (1) - A person shall not threaten to distribute by post, email, text, or transmit, by electronic means or otherwise, a private image or moving images of the other person engaged in sexually explicit conduct, with the specific intent to:
 - harass, threaten, coerce, intimidate, or exert any undue influence on the person, especially to extort money or other consideration or to compel the victim to engage in unwanted sexual activity; or
 - extort money or other consideration or compel the victim to engage in unwanted sexual activity.
- 2) A person shall not threaten to distribute by post, email, text, or transmit, by electronic means or otherwise, an intimate image of a child engaged in sexually explicit conduct, with the specific intent to:
 - harass, threaten, coerce, or intimidate the person, especially with intent to extort money or other consideration or to compel the victim to engage in unwanted sexual activity; or
 - extort money or other consideration or compel the victim to engage in unwanted sexual activity.

10. Meaning of Intimate Image

An intimate image may include a depiction in a way that the genital or anal region of another person is bare or covered only by underwear; or the breasts below the top of the areola, that is either uncovered or clearly visible through clothing.

11. Penalty

- A person who is convicted of sextortion commits an offence and is liable on summary conviction to a term of ten to twenty-five years imprisonment.

- Convention on the Rights of the Child (CRC)
- The United Nations Convention on the Rights of the Child is an international human rights treaty which sets out the civil, political, economic, social, health and cultural rights of children.
- This treaty was adopted by United Nations Member States on 20th November 1989. **Ghana signed the Convention of the Rights of the Child on 29th January 1990** and one week later, on 5th February 1990, Ghana became the first country in the world to ratify the treaty – committing to adopt it into national law.

12. Objective of CRC General Comment 25

This general comment requires countries to implement the Convention in relation to the digital environment and provide guidance on relevant legislative, policy and other measures to ensure full compliance with their obligations under the Convention and its Optional Protocols in the light of the opportunities, risks and challenges in promoting, respecting, protecting and fulfilling all children's rights in the digital environment.

13. General principles

The following four principles provide a lens through which the implementation of all other rights under the Convention should be viewed. They should serve as a guide for determining the measures needed to guarantee the realization of children's rights in relation to the digital environment.

- Non-discrimination.
- Best interests of the child.
- Right to life, survival, and development.
- Respect for the views of the child.

14. Right to Non-Discrimination

The right to non-discrimination requires that all children have equal and effective access to the digital environment in ways that are meaningful for them and overcome digital exclusion.

15. Ways in which children can be discriminated.

- By being excluded from using digital technologies and services or
- by receiving hateful communications or unfair treatment through use of those technologies.
- When automated processes that result in information filtering, profiling or decision-making are based on biased, partial, or unfairly obtained data concerning a child.
- Lack of access to digital literacy, privacy, and online safety.
- The digital environment can include gender-stereotyped, discriminatory, racist,

violent, pornographic, and exploitative information, as well as false narratives, misinformation and disinformation and information encouraging children to engage in unlawful or harmful activities.

16. Best interest of the child

- In considering the best interests of the child, regard should be given to children's rights, including their rights to:
- seek, receive, and impart information,
- be protected from harm and have their views given due weight, and
- ensure transparency in the assessment of the best interests of the child and the criteria that have been applied.

17. Right to life, survival, and development

- Children should be protected from risks to their right to life, survival, and development. Risks relating to content, contact, conduct, and contract encompass, among other things,
- violent and sexual content,
- cyberaggression and harassment,
- gambling,
- exploitation and abuse, including sexual exploitation and abuse, and
- the promotion of or incitement to suicide or life-threatening activities, including by criminals or armed groups designated as terrorist or violent extremist.

18. Respect for the views of the child

- The use of digital technologies can help to realize children's participation at the local, national, and international levels.
- Countries should promote awareness of, and access to, digital means for children to express their views and offer training and support for children to participate on an equal basis with adults, anonymously where needed, so that they can be effective advocates for their rights, individually and as a group.
- Children should be involved in all consultative processes, including children who lack access to technology or the skills to use it.

19. Civil rights and freedoms

- Access to information
- Freedom of expression
- Freedom of thought, conscience, and religion
- Freedom of association and peaceful assembly
- Right to privacy

20. Access to information

- Ensure that children have access to information in the digital environment restricted only when it is provided by law.
- Provide and support the creation of age-appropriate and empowering digital content for children in accordance with children's evolving capacities.
- Provide diverse, accessible, and beneficial content for children with disabilities and other minority groups.
- Easily find, diverse and good quality information online by ensuring automated search and information filtering.

21. Freedom of Expression

- Children's right to freedom of expression includes:
- The freedom to seek, receive and impart information and ideas of all kinds, using any media of their choice.
- When children express their political or other views and identities in the digital environment, they may attract criticism, hostility, threats, or punishment.
- States parties should protect children from cyberaggression and threats, censorship, data breaches and digital surveillance.

22. Freedom of thought, conscience, and religion

- Countries should respect the right of the child to freedom of thought, conscience, and religion in the digital environment.
- Children should not be penalized for their religion or beliefs or have their future opportunities in any other way restricted, however, the exercise of children's right to manifest their religion or beliefs in the digital environment may be subject only to limitations that are lawful, necessary, and proportionate.

23. Right to privacy

- Privacy is vital to children's agency, dignity, and safety and for the exercise of their rights.
- Threats to children's privacy may arise from data collection and processing by public institutions, businesses, and other organizations, as well as from such criminal activities as identity theft.
- Threats may also arise from children's own activities and from the activities of family members, peers, or others, for example, by parents sharing photographs online or a stranger sharing information about a child.

24. Violence against children

- The digital environment may open up new ways to perpetrate violence against children.
- Forms of digitally facilitated violence and sexual exploitation and abuse may be perpetrated within a child's circle of trust, by family or friends or, for adolescents,

by intimate partners, and may include cyberaggression, including bullying and threats to reputation, the non-consensual creation or sharing of sexualized text or images, such as self-generated content by solicitation and/or coercion, and the promotion of self-harming behaviours, such as cutting, suicidal behaviour or eating disorders.

- The digital environment can open up new ways for non-state groups, including armed groups designated as terrorist or violent extremist, to recruit and exploit children to engage with or participate in violence.

25. Right to education

- The digital environment can greatly enable and enhance children's access to high quality inclusive education, including reliable resources for formal, non-formal, informal, peer-to-peer and self-directed learning.
- Use of digital technologies can also strengthen engagement between the teacher and student and between learners.
- It is of increasing importance that children gain an understanding of the digital environment, and of the possible negative effects of digitalization on societies.