

TOPIC 16

SYSTEM AND DATA SECURITY

Senior Four ICT

By Emmanuel Gidudu

By the end of this topic, you will be able to:

- Identify types of computer security risks and malware
- Describe common security attacks and how attackers gain access
- Explain technologies used to secure computer systems
- Apply security measures both on and off a network
- Understand and draft an ICT Code of Conduct

Connecting to Prior Knowledge

This topic builds on what you already studied. Check what you can recall:

Topics 1 & 7	Awareness of ICT threats — viruses, malware, phishing
Topic 7	Safe internet and online practices
Topic 8	Health, safety, and responsible ICT use
Topics 3 & 15	Managing files, folders, and software

WHY THIS MATTERS:

In Uganda and globally, cyber-attacks are increasing in frequency and sophistication. In today's connected world, computer systems store personal details, financial records, academic data, medical records, and business secrets. Protecting this information is an essential skill for every ICT user.

 *THINK: Name one cyber threat you have personally heard about in Uganda. What damage did it cause?*

16.1 Computer Security Risks — Overview

A computer security risk is any action, event, or vulnerability that could lead to the compromise, loss, or damage of computer systems, networks, or the data they process. Risks can originate from malicious actors, careless users, or even natural disasters, threatening Confidentiality, Integrity, or Availability (the CIA Triad).

Risk Type	Description	Example
Human Error	Mistakes made by users	Accidentally deleting files; sharing passwords; clicking phishing links
Malware	Software designed to damage or gain unauthorised access	Viruses, worms, ransomware, spyware, Trojans
Hacking / Unauthorised Access	Attacker gaining access without permission	Breaking into a bank's database to steal customer records
Physical Threats	Physical damage to hardware causing data loss	Theft of laptop; fire destroying a server room
Natural Disasters	Environmental events damaging hardware or infrastructure	Lightning strikes, floods, earthquakes destroying equipment
Software Vulnerabilities	Security flaws in software attackers can exploit	Unpatched operating system exploited by a worm
Social Engineering	Manipulating people to reveal confidential information	Phishing emails; pretexting calls claiming to be IT support
Insider Threats	Deliberate or accidental breaches by employees	A disgruntled employee leaking confidential data

? QUICK CHECK: What is the difference between an 'insider threat' and 'social engineering'? Give a school-based example of each.

The CIA Triad — Core Security Requirements

All security measures aim to protect three core properties of information:

C — CONFIDENTIALITY

Only authorised users can access the information.

Examples: passwords, encryption, access controls, biometrics.

Threat: A hacker reading your private emails.

I — INTEGRITY

Information is accurate and has not been tampered with.

Examples: digital signatures, checksums, audit logs.
Threat: An attacker modifying marks in a school database.

A — AVAILABILITY

Authorised users can access information when they need it.

Examples: backups, redundant systems, anti-DoS tools.
Threat: A ransomware attack encrypting hospital records.

 **SCENARIO:** A student changes their mark in the school database. Which part of the CIA Triad has been violated? Explain why.

16.2 Types of Malware

Malware (malicious software) is any software intentionally designed to perform unauthorised, harmful actions on a computer system without the owner's consent. Understanding malware types is essential for implementing effective security measures.

Malware Type	Description	How It Spreads
Virus	Attaches to a legitimate file/program and spreads when the infected file is shared or executed.	Email attachments, infected USB drives, downloads
Worm	Self-replicating program that spreads across networks WITHOUT needing a host file.	Network connections, email, instant messaging
Trojan Horse	Disguises itself as legitimate software but contains a malicious payload.	Fake software downloads, pirated games/movies
Ransomware	Encrypts the victim's data and demands a ransom payment to restore access.	Phishing emails, exploit kits, vulnerable software
Spyware	Secretly monitors user activity and sends data (passwords, browsing history) to an attacker.	Bundled with free software, fake browser extensions
Adware	Displays unwanted advertisements and may redirect browser searches.	Bundled with free software, malicious websites
Rootkit	Hides deep in the OS to maintain persistent access and conceal other malware.	Trojans, exploiting OS vulnerabilities
Keylogger	Records every keystroke typed — including passwords and credit card numbers.	Trojans, phishing attacks, physical keyloggers on USB ports

Malware — Stealth Techniques & Uganda Context

Advanced Stealth Techniques

Polymorphism

Changes form with each infection to evade signature-based detection.

Stealth

Actively hides its presence from antivirus software.

Armoring

Wraps itself in protective code that makes analysis difficult.

Fileless Execution

Runs entirely in memory without leaving traces on disk — very hard to detect.

Blended Threats

Modern malware often combines multiple characteristics. A 'blended threat' may first appear as a Trojan, then act as a Worm to spread across the network, and finally deliver a Ransomware payload — making it especially dangerous and difficult to contain.

Uganda Cybersecurity Legal Context

Computer Misuse Act 2011 (amended 2022)

Criminalises hacking, spreading malicious code, and cyber harassment in Uganda.

NITA-U (National IT Authority Uganda)

Government body responsible for ICT security standards and Uganda's digital infrastructure.

AI-Powered Attacks (2026)

Attackers increasingly use AI to accelerate every phase of an attack — from reconnaissance to exploitation (Check Point Research, 2026).

 **QUICK CHECK:** What is the difference between a Worm and a Virus? Why is a Keylogger especially dangerous for banking

16.3 Identifying a Malware-Infected Computer

Recognising the signs of infection early allows quick action to limit damage:

Sign	What It Suggests
Computer extremely slow	Even when running only a few programs.
Frequent crashes / errors	Unexpected error messages or blue screens.
Programs run without user input	Applications open, close, or run on their own.
Unknown programs appear	In the Start Menu, taskbar, or desktop.
Browser homepage changed	Default search engine altered without the user's knowledge.
Constant pop-up advertisements	Even when the browser is not open.
Antivirus disabled or won't update	Malware disabling its own detection.
Files missing, renamed, or encrypted	Or files have changed in size unexpectedly.
High network activity when idle	Computer sending large amounts of data over the network.
Hard drive indicator flashing constantly	Unusual disk activity with no clear cause.

PRACTICAL CHECK: Open Task Manager (Ctrl+Shift+Esc). Check Processes tab for unfamiliar processes using high CPU, RAM, or Network bandwidth. Check Startup tab for suspicious programs set to run at startup.

16.4 Computer Security Attacks

A security attack is any deliberate action that compromises the security of information and/or computer systems — including copying, traffic analysis, modification, or fabrication of data. Attacks violate the CIA Triad (Confidentiality, Integrity, Availability).

Two Main Categories:

PASSIVE ATTACKS

Stealthy — the attacker monitors or eavesdrops WITHOUT altering data or disrupting services. Difficult to detect.

Examples: Eavesdropping, traffic analysis, release of message content, data interception.

Analogy: These are like someone listening at the door without entering the room.

ACTIVE ATTACKS

Direct interference — involves modification, fabrication, or disruption of data. Easier to detect but can cause significant damage.

Examples: Masquerade/spoofing, replay attacks, modification of messages, Denial of Service (DoS).

Analogy: These are like someone breaking down the door and rearranging furniture.

Stages of a Security Attack:

① Reconnaissance
Gather info, find vulnerabilities

② Initial Access
Phishing, malware, or credentials

③ Lateral Movement
Move across systems inside network

④ Privilege Escalation
Gain higher-level access

⑤ Execution
Exfiltrate data, encrypt, destroy

16.4 Specific Attack Types & Prevention

Attack Type	Description	How to Prevent
Phishing	Fake emails, websites, or messages trick users into revealing credentials or clicking malicious links.	Train users; use email filters; verify sender addresses; never click suspicious links.
Man-in-the-Middle (MITM)	Attacker intercepts communication between two parties, reading or altering messages.	Use HTTPS; avoid public Wi-Fi for sensitive transactions; use a VPN.
Denial of Service (DoS)	Overwhelming a server with traffic to make it unavailable to legitimate users.	Use firewalls; DDoS protection services; rate limiting.
Brute Force Attack	Trying millions of password combinations until the correct one is found.	Use strong passwords; enable account lockout policies; use MFA.
SQL Injection	Inserting malicious SQL code into a web form to manipulate a database.	Sanitise all user inputs; use parameterised queries in web code.
Zero-Day Exploit	Exploiting a previously unknown vulnerability in software before a patch is available.	Keep software updated; use intrusion detection systems; apply virtual patches.
Password Attack (Dictionary)	Using a list of common words to guess passwords.	Avoid dictionary words; use complex, unique passwords; use a password manager.

How Attackers Gain Access — Attack Vectors

An attack vector is the method or pathway a threat actor uses to gain access to a network, system, or application.

Attack Vector	Description	Prevalence
External Remote Access	Unauthorised access via compromised credentials for VPNs, RDP, or remote management tools.	59.4% of ransomware cases
External Exploit	Exploitation of known software vulnerabilities (often patchable but unpatched).	33.2% of ransomware cases
Human Risk	User actions including falling for phishing, social engineering, or credential mismanagement.	99.2% of BEC cases

EMERGING THREAT — Fake CAPTCHA / ClickFix Attacks:

Masquerade as anti-bot CAPTCHAs but trick users into copying and executing malicious commands. Accounts for approximately 45% of observed on-premises compromises.

LAYERED SECURITY STRATEGY — Essential Measures:

Strong access controls & MFA	Keep systems patched & updated	Maintain offline backups	Regular security training	Deploy firewalls & anti-malware
------------------------------	--------------------------------	--------------------------	---------------------------	---------------------------------

 *DISCUSS: Why do 59.4% of ransomware attacks start with remote access credentials? What should organisations do to*

16.5 Security Technologies — Passwords

A 'defence in depth' approach uses several overlapping security measures so that if one fails, others are still in place. Passwords are the most fundamental access control mechanism.

Characteristics of a STRONG Password:

Length	At least 12–16 characters long.
Complexity	Contains uppercase, lowercase, numbers, AND special characters (!@#\$%^&*).
No dictionary words	Does not use dictionary words, names, or dates.
Unique	Not used for more than one account.
Changed regularly	Every 3–6 months for sensitive accounts.

STRONG PASSWORD EXAMPLES:

Weak: 'amina2024' → Strong: 'Am!n4_K@mP@L@#8'

PASSPHRASE APPROACH: 'I_Love_Makerere_2024!' — long, memorable, and complex.

Password Exercise — Rate & Improve

Evaluate the following passwords. Rate each Weak, Moderate, or Strong and give a reason. Then rewrite Weak/Moderate ones as Strong passwords:

#	Password	Rating	Reason / Improved Version
(a)	password123	_____	_____
(b)	Nak@to#2024!	_____	_____
(c)	amina	_____	_____
(d)	iLoveUganda77!\$	_____	_____
(e)	qwerty	_____	_____

 EXTENSION: Design a 'School Password Policy' — what rules would you require for all student accounts?

16.5.2 Biometrics

Biometrics uses unique physical or behavioural characteristics to verify identity. Unlike passwords, biometrics cannot easily be stolen or forgotten.

Biometric Type	Description	Common Use
Fingerprint Scanner	Scans the unique pattern of ridges on a finger.	Smartphone unlock, laptop login, ATMs, border control
Facial Recognition	Analyses the geometry and structure of the face.	iPhone Face ID, Windows Hello, surveillance systems
Iris / Retina Scan	Scans the unique pattern of the iris or retina of the eye.	High-security facilities, some national ID systems
Voice Recognition	Analyses the unique characteristics of a person's voice.	Banking phone systems, smart assistants (Siri, Alexa)
Behavioural Biometrics	Analyses typing patterns, mouse movement, and walking gait.	Bank fraud detection, continuous authentication systems

Biometrics vs. Passwords — Key Comparison:

Passwords: Can be forgotten, shared, or stolen. Biometrics: Unique to each person, cannot be forgotten, but also cannot be changed if compromised (e.g., if your fingerprint data is stolen).

16.5.3 Firewalls

A firewall is a security system — hardware, software, or both — that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It creates a barrier between a trusted internal network and untrusted external networks (like the internet).

Analogy: A firewall is like a security guard at a building entrance who checks every person (data packet) entering or leaving — allowing authorised visitors and stopping suspicious ones.

Types of Firewalls:

Packet Filtering Firewall

Examines individual packets and allows or blocks them based on rules (IP address, port number).

Fastest but least intelligent — doesn't understand context.

Stateful Inspection Firewall

Tracks the state of active connections and makes decisions based on context, not just individual packets.

More secure than packet filtering.

Application Layer Firewall (Proxy Firewall)

Inspects traffic at the application level (e.g., HTTP, FTP). Acts as an intermediary between the user and the internet.

Provides the highest level of security.

Next-Generation Firewall (NGFW)

Combines traditional firewall features with deep packet inspection, IDS/IPS, and SSL inspection.

Most advanced — used in enterprise environments.

Examples: Windows Defender Firewall (built-in); pfSense (open-source); Cisco ASA; Fortinet FortiGate.

? *QUICK CHECK: What is the difference between a firewall and antivirus software? Can they replace each other?*

16.5.4 Antivirus Software

Antivirus software detects, prevents, and removes malicious software. It is an essential layer of defence for every computer.

How Antivirus Works — Three Detection Methods:

Signature-Based Detection

Compares files against a database of known malware 'signatures' (unique fingerprints). Fast and reliable for known threats. **WEAKNESS:** Cannot detect new/unknown malware.

Heuristic Analysis

Detects suspicious behaviour that **RESEMBLES** known malware patterns — even if the exact malware is not in the database. Useful for new variants.

Sandboxing

Runs suspicious files in an isolated 'sandbox' environment to observe behaviour **BEFORE** allowing them on the main system. Most thorough but slowest method.

Common Antivirus Examples:

Windows
Defender
(free, built-in)

Kaspersky

Avast

ESET NOD32

Malwarebytes

Bitdefender

Key Practices:

Keep antivirus definitions updated automatically

Run scheduled scans at least weekly

Scan ALL USB drives before opening any files

Do not disable antivirus — not even temporarily

16.5.5 & 16.5.6 Honeypots & Intrusion Detection

16.5.5 Honeypots

A honeypot is a decoy computer system or network resource deliberately set up to attract and trap attackers. It mimics a real system with seemingly valuable data, but any interaction with it is treated as malicious. Honeypots help security professionals learn about attack methods and identify attackers BEFORE they reach the real systems.

Analogy: A honeypot is like leaving a decoy wallet (with no real money but a GPS tracker) visible on a table to catch a thief. The real wallet is safely hidden elsewhere.

16.5.6 Intrusion Detection Systems (IDS) vs. Intrusion Prevention Systems (IPS)

IDS and IPS monitor, detect, and respond to unauthorised or malicious activities within computer networks. They are essential for early detection of intrusions and continuous protection of information systems.

System	Function	Action Type
IDS — Intrusion Detection System	Monitors traffic and logs suspicious events; sends alerts to the administrator.	PASSIVE — alerts but does NOT automatically block.
IPS — Intrusion Prevention System	Monitors traffic and automatically blocks or prevents threats in real time.	ACTIVE — detects AND blocks threats automatically.

Examples: Snort (open-source IDS/IPS), Suricata, Cisco IPS, Zeek (Bro).

16.6.1 Securing a Computer ON the Network

Key security practices when a computer is connected to a network or the internet:

Security Measure	How to Implement
Enable Firewall	Ensure Windows Defender Firewall is active. Go to Settings > Windows Security > Firewall. Configure rules to block suspicious ports.
Install & Update Antivirus	Use a reputable antivirus. Set it to update definitions automatically and run scheduled scans.
Use HTTPS	Only visit websites using HTTPS (padlock icon in browser address bar). Avoid HTTP sites for sensitive activities.
Secure Wi-Fi Connection	Use WPA3 or WPA2 encryption on your router. Use a strong Wi-Fi password. Avoid public Wi-Fi for sensitive activities.
Enable 2-Factor Authentication (2FA)	Add a second verification step (SMS code or authenticator app) to accounts — especially email and banking.
Regularly Update OS & Software	Enable automatic updates (Settings > Windows Update). Updates patch known security vulnerabilities.
Use a VPN	A Virtual Private Network encrypts your internet traffic, making it harder for attackers to intercept.
Configure User Accounts	Create standard user accounts for daily use — NOT Administrator accounts. Use admin only when needed.

16.6.2 Securing a Computer OFF the Network

Protecting standalone systems from physical access, malware via removable media, and unauthorised use:

Security Measure	How to Implement
Physical Security	Lock the computer room. Use cable locks on laptops. Restrict physical access to servers.
Screen Lock / Screensaver	Set computer to lock after 5 minutes of inactivity: Settings > Personalization > Lock screen. Press Windows+L to lock immediately.
Encrypt Hard Drive	Use BitLocker (Windows) or VeraCrypt to encrypt the hard drive so data is unreadable if the device is stolen.
Secure USB Ports	Disable USB ports in BIOS for devices that should not use them — prevents unauthorised data transfer or malware via USB drives.
Regular Data Backup	Back up important data to external drive or cloud storage. Use the 3-2-1 Rule: 3 copies, on 2 different media, 1 stored offsite.
Data Disposal	Before discarding a computer, use data wiping software (DBAN, Eraser) to permanently delete all data. Simply deleting files is NOT enough.
BIOS Password	Set a BIOS/UEFI password to prevent unauthorised users from changing boot settings or booting from external devices.

? What is the 3-2-1 Backup Rule? Why is simply pressing Delete on a file NOT enough to securely dispose of sensitive data?

16.7 Code of Conduct for ICT Use

A Code of Conduct for ICT use is a set of rules and ethical guidelines that govern how individuals should behave when using information and communication technologies. It promotes responsible, legal, and ethical use of digital systems — emphasizing respect for privacy, protection of data, prevention of cybercrime, and appropriate use of internet resources (ITU, 2020).

Sample ICT Code of Conduct — School Computer Lab:

1. Respect Privacy	Do not access other users' files, emails, or accounts without permission. Do not share personal information about others online.
2. Protect Credentials	Never share your password with anyone, including friends. Use strong, unique passwords for all accounts.
3. Use ICT Honestly	Do not plagiarise or copy others' work. Acknowledge all sources used in assignments.
4. Report Security Concerns	If you notice a virus, suspicious activity, or security breach, report it immediately to the ICT teacher.
5. Do Not Introduce Malware	Do not bring infected USB drives to school. Do not download software from untrustworthy sources.
6. Respect Intellectual Property	Do not pirate software, music, or videos. Use only licensed or free/open-source software on school equipment.
7. Responsible Internet Use	Only visit websites relevant to your studies during school hours. Do not engage in cyberbullying or harassment.
8. Protect School Equipment	Handle computers and printers with care. Report any damage or malfunction immediately.
9. Log Out After Use	Always log out of your account when you have finished using a school computer.
10. Respect Others' Online Safety	Do not take or share photos/videos of classmates or teachers online without their permission.

 **ACTIVITY:** In pairs, draft a 5-rule ICT Code of Conduct specifically for your school's computer lab. Present your rules to the

SCENARIO — Kampala Secondary School ICT Lab

The ICT teacher at Kampala Secondary School discovers that several student computers in the lab are behaving strangely. The computers are very slow, pop-up advertisements are appearing constantly, and one computer displays the message:

'Your files have been encrypted. Pay 0.05 Bitcoin to restore your files.'

Students have been bringing personal USB drives to school and using them on school computers. The school's antivirus has not been updated in 8 months.

Discussion Questions:

- | | |
|-----|---|
| (a) | Identify the specific type of malware that has encrypted files. What is this attack called? |
| (b) | What are the most likely ways the malware entered the school network? |
| (c) | What immediate steps should the ICT teacher take to CONTAIN the damage? |
| (d) | Outline a complete security improvement plan for the lab: antivirus, USB policies, passwords, user accounts, and backups. |
| (e) | Should the school pay the ransom to recover the encrypted files? Explain the risks and alternatives. |
| (f) | Create a 5-rule Code of Conduct for the ICT lab that would have PREVENTED this situation. |

Class Exercises — Exercise 4.1

Exercise 1 Security Assessment	Open Windows Defender (Settings > Windows Security). Check: (a) Is antivirus turned on? (b) When were virus definitions last updated? (c) Is the firewall active? Write a short report of your findings.
Exercise 2 Password Rating	Evaluate these passwords — rate each Weak, Moderate, or Strong with a reason: (a) 'password123' (b) 'Nak@to#2024!' (c) 'amina' (d) 'iLoveUganda77!\$' (e) 'qwerty' Then rewrite each Weak/Moderate password as a Strong password.
Exercise 3 Task Manager Investigation	Open Task Manager (Ctrl+Shift+Esc) > Network tab. Observe network activity. Research any unfamiliar processes sending data. Are any suspicious? Report your findings.
Exercise 4 Cyber Threats Poster	In pairs, create a poster (on paper or digitally) showing 'The 5 Most Dangerous Cyber Threats to Students in Uganda' — with an explanation of each threat and one prevention tip.
Exercise 5 Code of Conduct Draft	Draft a 5-rule ICT Code of Conduct for your school's computer lab. Present your rules to the class and discuss the differences between groups.

Topic 16 Summary — What Did We Learn?

16.1 Security Risks Overview

Types: Human Error, Malware, Hacking, Physical Threats, Natural Disasters, Software Vulnerabilities, Social Engineering, Insider Threats. CIA Triad: Confidentiality, Integrity, Availability.

16.3 Identifying Infection

10 warning signs including slow performance, unknown programs, changed browser, constant pop-ups, disabled antivirus. Practical: Task Manager check.

16.5 Security Technologies

Defence-in-depth approach. Passwords (strong characteristics), Biometrics (5 types), Firewalls (4 types), Antivirus (3 detection methods), Honeypots, IDS/IPS.

16.7 Code of Conduct

10 rules for ethical ICT use: Respect Privacy, Protect Credentials, Honesty, Report Concerns, No Malware, Intellectual Property, Responsible Internet, Protect Equipment, Log Out, Respect Others.

16.2 Types of Malware

Virus, Worm, Trojan, Ransomware, Spyware, Adware, Rootkit, Keylogger. Stealth techniques: Polymorphism, Fileless execution. Uganda's Computer Misuse Act 2011.

16.4 Security Attacks

Passive vs. Active attacks. Specific types: Phishing, MITM, DoS, Brute Force, SQL Injection, Zero-Day, Dictionary. 5 stages of an attack. Top attack vectors.

16.6 Securing Systems

ON the network: Firewall, Antivirus, HTTPS, WPA3, 2FA, VPN, Updates, User Accounts. OFF the network: Physical security, Encryption, USB control, 3-2-1 Backups, Data Disposal.

Uganda Context

Computer Misuse Act 2011 (amended 2022), NITA-U role, increasing AI-powered attacks (2026 threat landscape).

Topic 16 Self-Evaluation Checklist

Tick the column that best describes your confidence for each skill:

Skill / Knowledge Area	Not Yet	Partially	Fully
I can define computer security risk and explain the CIA Triad.	☐	☐	☐
I can identify and describe at least 8 types of computer security risks.	☐	☐	☐
I can explain the different types of malware and how each spreads.	☐	☐	☐
I can recognise the signs of a malware-infected computer.	☐	☐	☐
I can distinguish between passive and active security attacks.	☐	☐	☐
I can describe specific attack types (phishing, DoS, MITM, SQL injection) and their prevention.	☐	☐	☐
I can explain the characteristics of a strong password and create one.	☐	☐	☐
I can describe at least 4 types of biometric authentication and their uses.	☐	☐	☐
I can explain how firewalls work and name the 4 types.	☐	☐	☐
I can describe how antivirus software detects malware (3 methods).	☐	☐	☐
I can explain the difference between IDS and IPS.	☐	☐	☐
I can list security measures for a computer on a network.	☐	☐	☐
I can list security measures for a computer off a network.	☐	☐	☐
I can explain the 3-2-1 backup rule.	☐	☐	☐
I can draft an ICT Code of Conduct for a school computer lab.	☐	☐	☐