Introduction to Cyber Security

QCTO Occupational Certificate

Cyber Security Analyst

Learner Guide 1

Module Code

252901001-KM-01

NQF Level 4, Credits 8

MICTSETA
Media, Information And Communication Technologies Sector Education And Training Authority
SHAPING SKILLS, PIONEERING INDUSTRIES, EMPOWERING FUTURES

Developed by The Learning Studio (Pty) Ltd.

Table of Contents

Personal Details Form

Surname	
First name(s)	
ID Number	
Gender	☐ Male ☐ Female
Race Group	
Address	
Cellphone number	
Company name	
Company address	
Company telephone	
List any courses you have passed since you left school.	
What do you do in your job?	
What do you do when you are not at work?	
What do you want to learn in this course?	

Learner Declaration and Copy of ID

I _____*(name)*,

_____ *(ID Number)* declare that all work contained within this Portfolio of Evidence is my own work.

Signature: _____

Date: _____

Place: _____

Witness: _____

Paste/staple certified copy of learner's ID here.

Facilitator Report and Declaration

Facilitator Report on _____ *(learner's name)*

Describe the learner's participation in the course. Include some comments about the learner's attendance and diligence. Mention anything exceptional that the learner has done for the duration of the course. Based on this and on the evidence in the portfolio, make a statement regarding the competency of the learner.

Facilitator Declaration

I declare that as far as I am aware, the **content** of this module is the independent and original work of the learner concerned.

I declare that the **knowledge topics** have been covered and that the learner is suitably competent and has met each of the **internal assessment criteria** listed.

Facilitator: _____

Signature: _____

Contact No. _____

Date: _____

Title

Introduction to Cyber Security

Purpose of the Knowledge Module

The focus of the learning in this knowledge module is to build an understanding of fundamentals of various computer and network security threats such as identity theft, credit card fraud, phishing, virus and backdoors, email hoaxes (fraud), loss of confidential information, hacking attacks, and social engineering.

Module Introduction

Welcome to our exploration of cyber security! In today's digital world, where we rely on computers and the internet for almost everything, it's more important than ever to keep our information safe. Cyber Security is like a shield that protects our digital lives from harm. This module, Introduction to Cyber Security, is designed to equip you with the knowledge to recognise and understand various threats that can compromise your digital safety. We will explore common risks like identity theft, credit card fraud, phishing scams, malware (including viruses and backdoors), email hoaxes, loss of confidential information, hacking attacks, and the deceptive tactics of social engineering.

By the end of this module, you will have a solid foundation in identifying these threats and understanding how they work. You'll also learn practical strategies to protect yourself, your devices, and your organisation from these risks, empowering you to navigate the digital world more confidently and securely.

lesson 1

Building a Strong Cyber Security Foundation

Lesson Objectives

By the end of this lesson, the learner should be able to:

- Explain the importance of securing computer and mobile devices in today's digital world.
- Identify the objectives of computer and mobile device security, such as confidentiality, integrity, and availability.
- Recognise common cyber threats and the potential consequences of compromised devices (data breaches, financial loss).
- Describe various security measures to protect your devices, including strong passwords, firewalls, and encryption.

Topics

KM-01-KT01 Introduction to computer and mobile device security

Topic Elements

KT0101	Governance and legislation
KT0102	Security policy
KT0103	Physical security (e.g. biometric authentication)
KT0104	Web content filters
KT0105	Need for protection of privacy and data

IACW

IAC0101 The importance of computer and mobile device security is justified

IAC0102 Objectives of computer and mobile device security are explained

The weighting is 15%.

Introduction to Computer and Mobile Device Security

Our lives are increasingly intertwined with technology, from personal devices to complex business networks. This reliance on digital systems brings many benefits, but it also creates vulnerabilities that cyber criminals can exploit.

The more we rely on technology in our daily lives, from our phones to the systems businesses use, the more helpful it becomes. But with this convenience comes a risk. Just like any valuable tool, these digital systems can be targeted by criminals who want to steal information or cause trouble.

Throughout this module, we will explore key topics such as:

- What is cyber security and why is it important?
- Common cyber threats and attacks
- The importance of securing computer and mobile devices
- Essential security practices for individuals and organisations
- Understanding the role of cyber security professionals

By the end of this module, you will gain a solid understanding of the importance of cyber security and be equipped with the basic knowledge to protect yourself and your devices online.

What is Cyber Security?

Cyber Security refers to the practices and techniques used to protect information, such as documents, financial information, emails, photos and systems from unauthorised access, use, disclosure, disruption, modification, or destruction. Imagine your computer as a safe filled with valuable treasures (your data, financial information, personal records). Cyber Security safeguards that safe, ensuring only authorised individuals can access its contents and that the safe itself remains secure from external threats.

But what happens if a device is compromised or threatened?

Unfortunately, the digital world is not without its dangers. Cyber criminals constantly develop new ways to exploit vulnerabilities or weaknesses and steal information or disrupt systems. The consequences of a compromised device or a data breach can be severe:

Data breaches and identity theft

If a hacker gains access to your device, they can steal sensitive information like passwords, credit card numbers, and personal details. This stolen information can be used for identity theft, causing financial loss and a significant amount of hassle to recover your identity.

Example

In 2014, a major retail chain experienced a massive data breach due to a (malicious software) malware infection on point-of-sale systems. Millions of customer credit card details were compromised.
(https://krebsonsecurity.com/tag/target-breach/ accessed 05/05/2024)

Financial loss

Malicious software (malware) can target financial information. If your device becomes infected, the cyber attack can lead to identity theft, unauthorised purchases on your accounts, or even fraudulent banking activity.

Disruption and downtime for businesses

Businesses rely heavily on secure devices to conduct operations. A cyber attack on a company's network through a compromised device can lead to data breaches, system outages, and significant downtime, this can result in financial losses and reputational damage.

Example

A hospital network was crippled by ransomware in 2021, forcing them to delay critical surgeries and pay a hefty ransom to regain access to their systems. *(https://www.npr.org/2023/06/25/1184025963/cyber attacks-hospitals-ransomware)*

Social media and reputational damage

Social media influencers and other public figures can also suffer significant losses if their accounts are compromised.

Example

A social media influencer lost access to their account after falling victim to a phishing scam, leading to financial losses and reputational damage.
(https://www.nytimes.com/2020/07/16/business/dealbook/twitter-hack-bitcoin.html)

Safety risks

In critical infrastructure sectors like healthcare or energy, cyber attacks can pose physical safety risks by disrupting essential services.

Loss of privacy

Personal information like emails, photos, or financial documents can be exposed, potentially damaging your reputation or causing emotional distress.

Objectives of Computer and Mobile Device Security

Now that we understand the importance of securing our devices, let's look at specific objectives we aim to achieve:

Confidentiality

Ensures information remains private and accessible only to authorised users, preventing identity theft and protecting sensitive data.

Integrity

Ensures the accuracy and completeness of information and systems, critical for decision-making and preventing financial losses.

Availability

Ensures authorised users can access information and systems when needed, preventing disruptions and ensuring smooth business processes.

By understanding these objectives and implementing proper security measures, we can all play a role in protecting our valuable information in the digital age.

Integrating Security Measures

With the objectives in mind, let's explore how to put them into practice through various security measures for both individuals and organisations:

Governance and Legislation

Organisations must comply with laws and regulations like South Africa's Protection of Personal Information Act (POPIA), which focuses on data confidentiality and user privacy. This ensures responsible data practices and helps safeguard user information.

Security Policy

Policy Development: A well-defined security policy outlines acceptable use of devices, password requirements, and security protocols for employees. This policy serves as a blueprint for an organisation's digital defence strategy, promoting a culture of security and accountability.

A strong security policy promotes a culture of security within an organisation by clearly outlining expectations and making everyone accountable for protecting information.

Physical Security

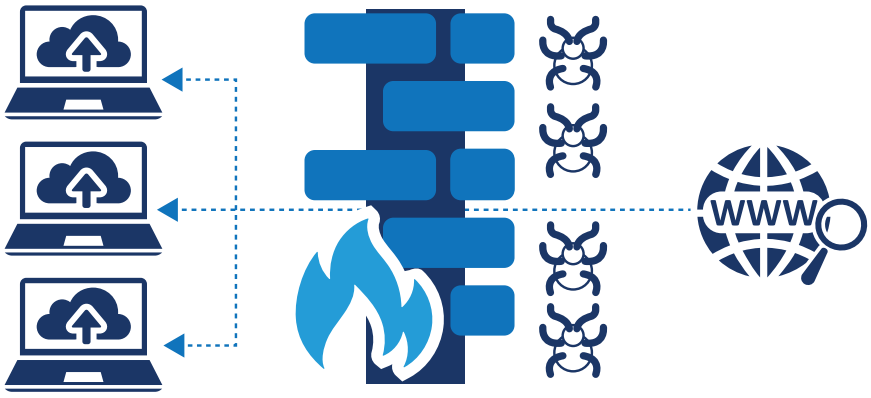
e.g. biometric authentication

Implement physical security steps such as locking devices, using strong passwords, and employing biometric authentication (e.g., fingerprint scanners, facial recognition) to prevent unauthorised access and protect sensitive data.

Technical Security

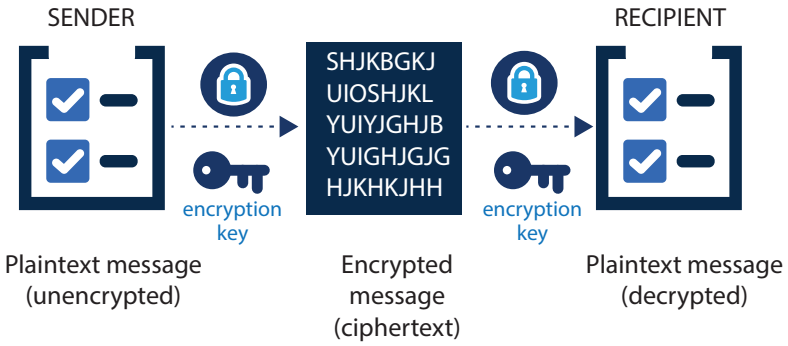
Technical security measures refer to software and hardware tools that help safeguard systems from cyber attacks. These include:

Firewalls	Act as protective barriers, monitoring network traffic to block unauthorised access.

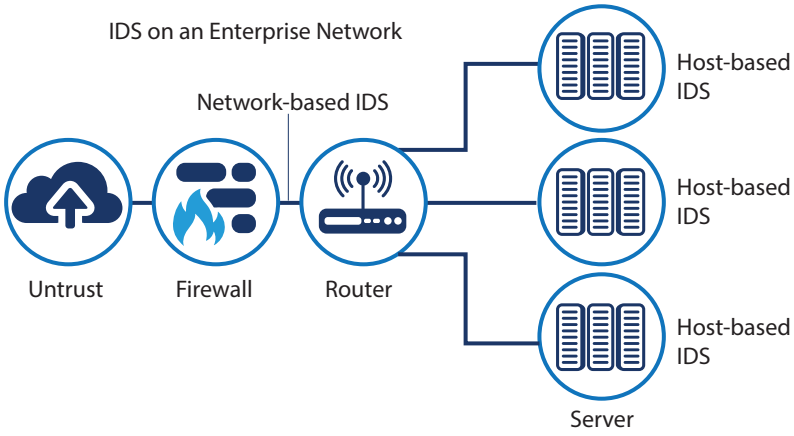


Anti-virus Programmes	Detect and remove malware, preventing damage or data theft.

Data Encryption	Ensures that even if data is accessed, it remains unreadable without a decryption key.



Intrusion Detection Systems (IDS)	Monitor network activity for suspicious behaviour, alerting administrators to potential cyber attacks.



Web Content Filters

Function: These filters block access to known malicious or inappropriate websites, protecting devices from potential harm and allowing customisation based on organisational policies or personal preferences.

Need for Protection of Privacy and Data

In our increasingly interconnected world, safeguarding user privacy is paramount. Protecting user privacy is crucial as we entrust vast amounts of personal information to the online world. Ensuring control over who accesses this data and how it's used is essential to prevent identity theft, financial loss, and misuse of our digital footprint.

Data Protection Laws: Building a Digital Security Fence

Fortunately, data protection laws are globally emerging to help safeguard user privacy. These laws set guidelines for how organisations should collect, store, and use personal information. Here are some key aspects of data protection laws:

User consent	Organisations must obtain clear and informed consent from users before collecting or using their personal data.
Data minimisation	Organisations should only collect the data they absolutely need for a specific purpose and not retain it for longer than necessary.
Right to access and control	Users have the right to access their personal information, request corrections to inaccurate data, and even request deletion under certain circumstances.
Data Security measures	Organisations have a legal obligation to implement appropriate security measures to protect user data from unauthorised access. Knowing the threats to our privacy and the laws that protect it helps us navigate the online world with more confidence.

The Evolving Threat Landscape

Throughout this lesson, we've focused on the importance of securing our computers and mobile devices. We've explored various measures we can take to safeguard our information, but remember, keeping things secure online is like fighting a monster - it never stops changing. New dangers appear all the time, and bad guys are always coming up with new tricks to steal information.

Zero-day Attacks

These are novel attacks that exploit previously unknown vulnerabilities in software. Since there's no security patch available yet, these attacks can be particularly dangerous.

Social Engineering

Cyber criminals are skilled at manipulating people. They may use phishing emails, phone calls, or even social media, to trick users into revealing sensitive information or clicking on malicious links.

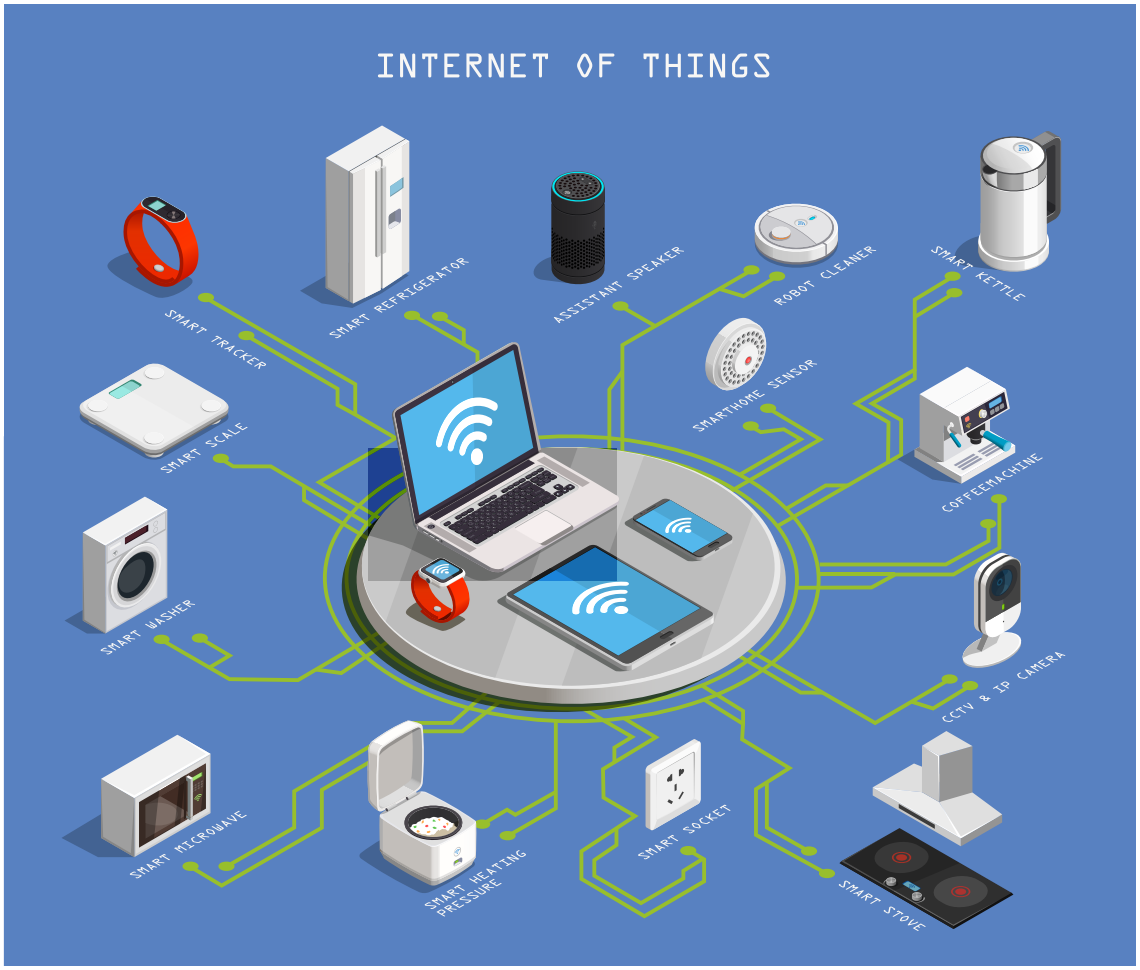
Advanced Persistent Threats (APTs)

These are highly targeted and sophisticated attacks aimed at stealing sensitive data from organisations. APTs often involve a combination of techniques, making them difficult to detect and defend against.

The Internet of Things (IoT)

The more things we connect to the internet, from smart home appliances to industrial control systems, the more ways criminals can find to attack us. This growing number of devices is a new challenge for keeping things secure online.

This is where cyber security analysts come in. These skilled professionals play a critical role in protecting individuals, organisations, and even entire nations from cyber attacks.



They work tirelessly to:

- **Identify new threats and vulnerabilities.** Cyber Security analysts constantly monitor the threat landscape, researching and analysing emerging threats and vulnerabilities and weaknesses in software and systems.
- **Develop and implement security measures to counter these threats**. Based on their research, they develop and implement security measures like firewalls, intrusion detection systems, and security protocols to counter these threats.
- **Investigate and respond to cyber attacks.** In the event of a cyber attack, cyber security analysts play a crucial role in investigating the incident, containing the damage, and recovering systems.
- **Raise awareness about cyber security best practices**. Educating users about cyber security best practices is a very important part of an organisation's defence strategy. Cyber Security analysts often develop training programmes and educational materials to raise awareness about online safety.

Key Takeaways

- In this first lesson, we've laid the groundwork for understanding cyber security fundamentals.
- We explored the significance of protecting our information and devices in an increasingly digital world, covering essential security objectives such as confidentiality, integrity, and availability.
- We looked at common cyber threats, the critical consequences of compromised devices, and various security measures to safeguard our digital assets.
- Additionally, we examined the evolving threat landscape, and the pivotal or important role cyber security analysts play in defending against cyber attacks.
- As we move forward in this module, we will investigate specific threats and advanced security practices, equipping you with the knowledge and skills to navigate the digital realm safely and responsibly. Your journey towards becoming a more informed and proactive digital citizen has just begun.

Assessment

1. Underline the best answer. Why is cyber security crucial in today's digital world?
    1. Because it's a fun hobby for tech enthusiasts.
    2. To protect sensitive information from unauthorised access.
    3. Because it's a legal requirement for all computer users.
    4. To increase internet speed.

2. Provide two real-world examples of the consequences of a compromised device or data breach.

3. Define the objective of integrity in computer and mobile device security.

4. Scenario: You work for a small business that handles customer orders online. Explain why each of the following objectives is essential for your organisation's security:
   - Ensuring confidentiality
   - Maintaining data integrity
   - Ensuring the availability of critical systems

lesson 2

Protecting Your Digital World: Understanding and Countering Cyber Security Threats

Lesson Objectives

By the end of this lesson, learners should be able to:

- Define and explain various computer and network security threats and how they work.
- Identify potential solutions to mitigate these threats.
- Recognise signs of a potential security breach on your computer or network.

Topics

KM-01-KT02 Various computer and network security threats

Topic Elements

KT0201	Malware
KT0202	Viruses
KT0203	Spyware
KT0204	Adware
KT0205	Trojan horses
KT0206	Worms
KT0207	Phishing
KT0208	Spear phishing
KT0209	Insider security threats

IACW

IAC0201	Computer and network security threats and attacks are defined and how they work is explained
IAC0202	Potential solutions are identified

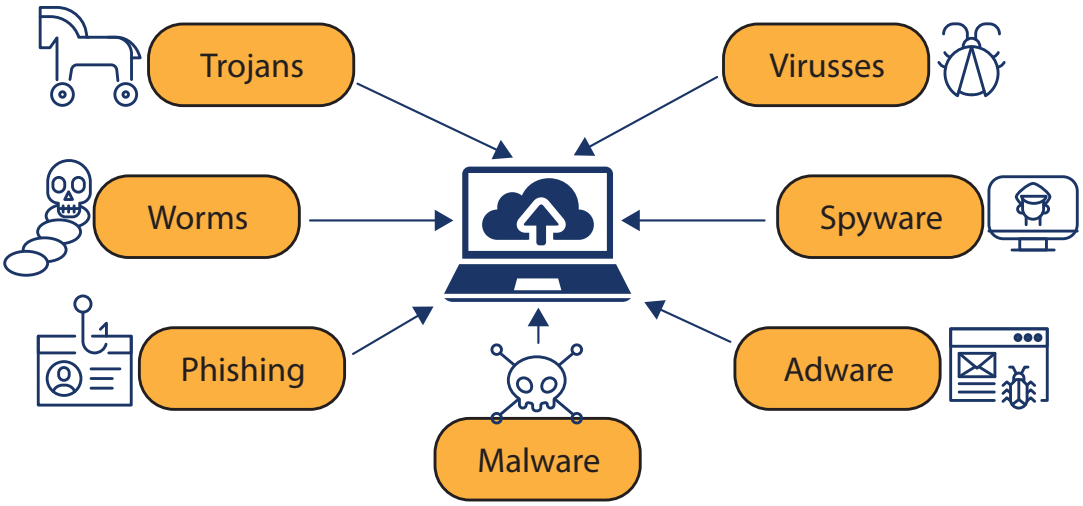
The weighting is 20%

Introduction

In today's interconnected world, your computer and the information it holds are valuable targets for cyber criminals. It's like a virtual treasure chest they're trying to unlock! But don't worry, this lesson will equip you with the knowledge to spot the warning signs and outsmart those bad actors. We'll uncover common external threats like malware, phishing scams, and worms, and discuss how to protect yourself and your data. We'll also learn about the hidden danger of insider threats and how to protect your organisation.

External Threats: Malware, Viruses, Spyware, and Adware

These threats often come from outside your organisation and can infect your computer through various ways like emails, websites, or downloads.



Malware: The Shape-Shifter

Malware is a broad term for any harmful software designed to harm your computer or steal your data - like a master of disguise, appearing in many forms:

Viruses

Like a real-world virus, these tiny programmes spread by infecting other files and making copies of themselves. They can delete files, cause crashes, and slow down your system.

Signs of a virus include:

- Your computer runs slower than usual.
- You get unusual pop-up messages or your browser homepage appearance changes unexpectedly.
- Files disappear or become corrupted.
- Your antivirus software sends you alert warnings.

Spyware

This sneaky software hides on your computer and collects your personal information without you knowing it. It's like a spy watching your every move.

Signs of spyware include:

- Your computer runs slower than usual.
- Unexpected toolbars or icons appear in your web browser.
- Your webcam light turns on by itself.

Adware

Have you ever been bombarded with pop-up ads? That's probably adware. Although it is not as dangerous as other malware, it's a nuisance that clutters your screen and can slow down your system.

Signs of adware include:

- Excessive pop-up ads, even when you're not browsing the web.
- Your browser homepage changes without your permission.

How to Protect Yourself from Malware, Viruses, Spyware, and Adware

Keep Software Updated	Software updates often contain fixes for security holes that hackers could use.
Use Security Software	Antivirus and anti-malware programmes are your first line of defence. Make sure they are updated and run regular scans.
Be Careful What You Download	Do not download files from unknown sources or click on suspicious links. Only download from official websites and app stores.

Cyber Security Analyst's Role

Cyber Security analysts guard an organisation's digital assets. They monitor systems, investigate suspicious activity, and develop strategies to prevent and respond to these threats. They also educate employees about safe computing practices to minimise the risk of infection.

Trojan Horses: The Wolf in Sheep's Clothing

Trojans disguise themselves as legitimate software but contain malicious Code. Once you install them, they can steal your data, install other malware, or give hackers access to your system.

How to Avoid Trojan Horses

Be Careful What You Download	Software should only be downloaded from trusted sources.
Check File Extensions	Be wary of files with double extensions (e.g., filename. txt.exe). These are often disguised as harmless files but are actually executable programmes that can contain malware.
Do NOT Open Unexpected Attachments	Be suspicious of attachments in emails, even if they seem to be from someone you know.

Worms: The Speedy Spreaders

Worms are a type of malware that spread very quickly across networks, infecting many computers. They can cause damage by deleting files, stealing information, or slowing down systems.

Signs of a Worm Infection

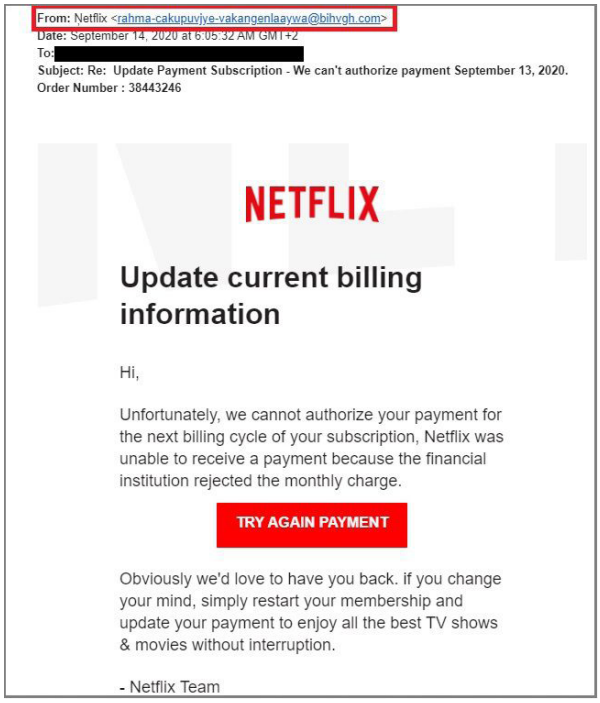
- Slow Network Performance: If your internet or network suddenly becomes much slower than usual, there could be a worm.

How to Stop the Spread

- Use a Firewall: A firewall blocks unauthorised access by acting as a barrier between your computer and the internet.
- Keep Your Software Updated: Software updates often contain security patches that fix vulnerabilities that worms can exploit.

Phishing & Spear Phishing: The Bait and Switch

Phishing emails are like bait – they try to trick you into giving up your personal information. Spear phishing is even more targeted, using information about you to make the bait more tempting.



https://www.investopedia.com/articles/personal-finance/040115/watch-out-these-top-internet-scams.asp]

How to Avoid Getting Hooked

- **Think Before You Click**: Do not click on links or open attachments from emails you weren't expecting, especially if they ask for personal information or seem too good to be true.
- **Verify the Sender**: If an email appears to be from a company or person you know, double-check the sender's address and contact them directly to confirm before clicking on anything.
- **Enable Two-Factor Authentication (2FA):** This adds an extra layer of security to your accounts, even if someone gets your password.

The Insider Threat: A Hidden Danger

Insider threats come from within an organisation. They can be accidental. It's easy to accidentally share confidential information with the wrong person, click on a malicious link, or fall for a phishing scam. Or they can be intentional, for example, a disgruntled (unhappy) employee who steals data for various reasons, like, revenge, financial gain, or even espionage (spying.)

What to Look For

Unauthorised Access	Employees accessing files or systems they don't need for their job.
Unusual Activity	Working odd hours, downloading large amounts of data, or acting suspiciously secretive.
Changes in Behaviour	Sudden changes in an employee's behaviour, such as mood swings or financial difficulties.

How to Prevent and Respond

Background Checks	Conduct thorough background checks on existing and new employees and contractors.
Least Privilege Principle	Give employees access only to the information and systems they absolutely need to do their jobs.
Monitoring	Regularly monitor and audit user activity to detect unusual behaviour or unauthorised access.
Data Loss Prevention (DLP) Tools	Implement DLP software to monitor and control the flow of sensitive data, preventing it from being copied, transferred, or leaked.
Security Awareness Training	Teach employees about insider threats and good security practices.

Key Takeaways

Staying Secure Online: Your Essential Guide

While we have explored various threats, here's how to fortify your defences:

- Scrutinise emails and attachments: Check before you click! Verify who sent an email before opening it, especially if it asks you to do something urgently or has attachments.
- Update software regularly: Updates often include security patches to fix vulnerabilities or security holes.
- Install reliable security software: Antivirus and anti-malware software can help detect and prevent malware infections.
- Practice strong password hygiene: Use unique, complex passwords and consider a password manager.
- Share with caution online: Avoid sensitive information sharing on public platforms and be careful of unknown sources.
- Recognise social engineering: Phishing emails use urgency or curiosity to trick you. Be cautious!
- Report suspicious activity: Help track threats by reporting phishing attempts or malware infections.

By following these steps, you can become a more responsible digital citizen and explore the online world confidently and safely. Happy browsing!

Assessment

1. Match the phrase in column A to the description in column B that best matches it. Write the letter in the answer column.

A	B	Answer
1. Disgruntled/ unhappy employee	a. Someone who steals data for personal gain, potentially selling it to competitors.	
2. Accidental insider	b. A trusted individual who unintentionally compromises data due to negligence.	
3. Financially motivated insider	c. An employee with authorised access, motivated by anger or resentment, to harm the organisation.	
4. Spy	d. An infiltrator posing as a legitimate employee to steal sensitive information.	

2. Underline the best answer. Which of the following is the MOST effective way to completely remove insider threats?

   a. Implementing strong access controls.

   b. Conducting regular security awareness training.

   c. Using a powerful antivirus programme.

   d. There is no guaranteed method to completely remove insider threats.

3. True or False: Insider threats are always intentional and malicious acts.

---

4. True or False: Phishing attacks can be a tactic used by external actors to gain access and potentially become insider threats.

---

5. Describe two security measures organisations can implement to mitigate the risk of insider threats posed by disgruntled employees.

6. Explain the potential consequences of a successful insider attack on a business, considering both financial and reputational damage.

7. In addition to the security measures mentioned in the lesson, what is one personal action you can take to reduce becoming an accidental insider threat?

8. Write and essay to compare and contrast phishing attacks with insider threats. Consider the target, attack methods, and potential consequences for the victim.

lesson 3

Understanding Identity Theft

Lesson Objectives

By the end of this lesson, learners will be able to:

- Define identity theft and explain the different forms it can take (financial, medical, criminal).
- Identify how criminals steal personal information through phishing scams, malware, and social engineering.
- Describe the potential consequences of identity theft for individuals and businesses.
- Explain practical strategies to safeguard your personal information and reduce the risk of identity theft, including strong passwords, secure browsing habits, and monitoring financial accounts.

Topic

KM-01-KT03 Identity theft

Topic Elements

KT0301	Phishing scams
KT0302	Malware
KT0303	Social engineering
KT0304	Financial frauds

IACW

IAC0301	An understanding of types of identity theft and how to mitigate them is demonstrated

The weighting is 10%

Introduction

In our digital world, personal information is valuable to individuals and businesses. Cyber criminals target this data for identity theft. This lesson teaches you how to protect yourself and your organisation. We'll cover forms of identity theft, criminal tactics, and how to identify red flags. You'll learn practical strategies to safeguard personal and organisational data, reducing the risk of identity theft.

What is Identity Theft?

Identity theft is when someone illegally obtains and uses personal information for fraud. This includes name, ID numbers, dates of birth, and financial information. Criminals can use this stolen information in various harmful ways.

Financial Theft	Criminals steal money through unauthorised purchases, account takeovers, or opening new accounts in your name.
Medical Identity Theft	They use your stolen information to receive medical care, leading to mistakes in a patient's medical history, which could cause problems with future care.
Criminal Identity Theft	Criminals use your details to commit crimes, leading to legal trouble and a damaged reputation for you.

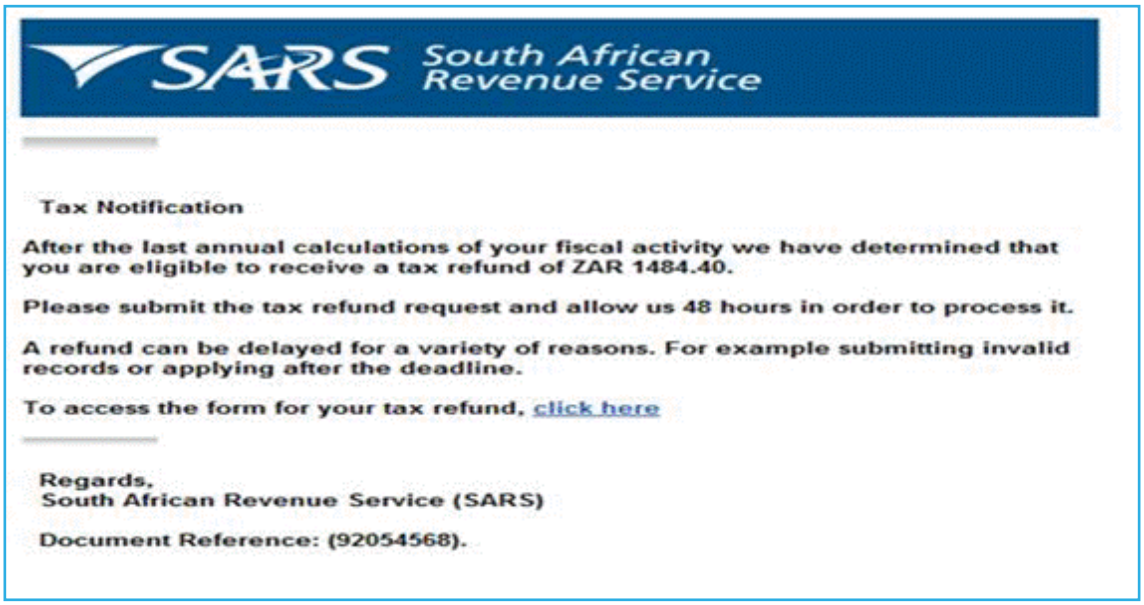
account takeover

credit card fraud

medical identity theft

tax fraud

Phishing Scams: A Deceptive Net for Personal Information



SARS South African Revenue Service

Tax Notification

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of ZAR 1484.40.

Please submit the tax refund request and allow us 48 hours in order to process it.

A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

To access the form for your tax refund, click here

Regards,
South African Revenue Service (SARS)

Document Reference: (92054568).

https://www.tech4law.co.za/lawyerhome/helpful-home-tips-d3/sars-refund-email-phishing-scam-attempt/

Phishing scams are a common trick cyber criminals use to steal personal information. These scams try to lure or encourage you into revealing sensitive details like usernames, passwords, credit card numbers, or Social Security numbers. They often disguise themselves as emails or messages from trusted sources like banks, credit card companies, or even government agencies.

Phishing Scams

Deception is the Game.	Phishing emails or messages appear to come from trusted sources like banks, credit card companies, or even government agencies.
Urgency or Curiosity is the Hook.	They create a sense of urgency (e.g., 'Account suspension!') or curiosity (e.g., 'You've won a prize!') to pressure you into clicking a link or opening an attachment.
Fake Websites or Malicious Attachments.	Clicking the link leads to a fake website designed to steal your login credentials. Opening the attachment installs malware that steals information in the background.

Examples of Phishing Scams

Fake bank email.	You receive an email that appears to be from your bank, warning about suspicious activity and prompting you to click a link to verify your identity. The link leads to a fake website ready to steal your login credentials.
Tax refund scam.	An email arrives claiming to be from SARS, stating you're due for a tax refund. The email asks you to click a link and enter your personal information to claim your refund. This is a scam to steal your tax number and other sensitive data.
Social media phishing.	A message on social media appears to be from a friend or colleague, often accompanied by a malicious link or attachment. Clicking the link could lead to a fake login page or download malware that steals your account information.

Protecting Yourself

- Be wary of unsolicited emails and messages.
- Verify sender identity.
- Scrutinise websites.
- Strong passwords and MFA.
- Businesses.

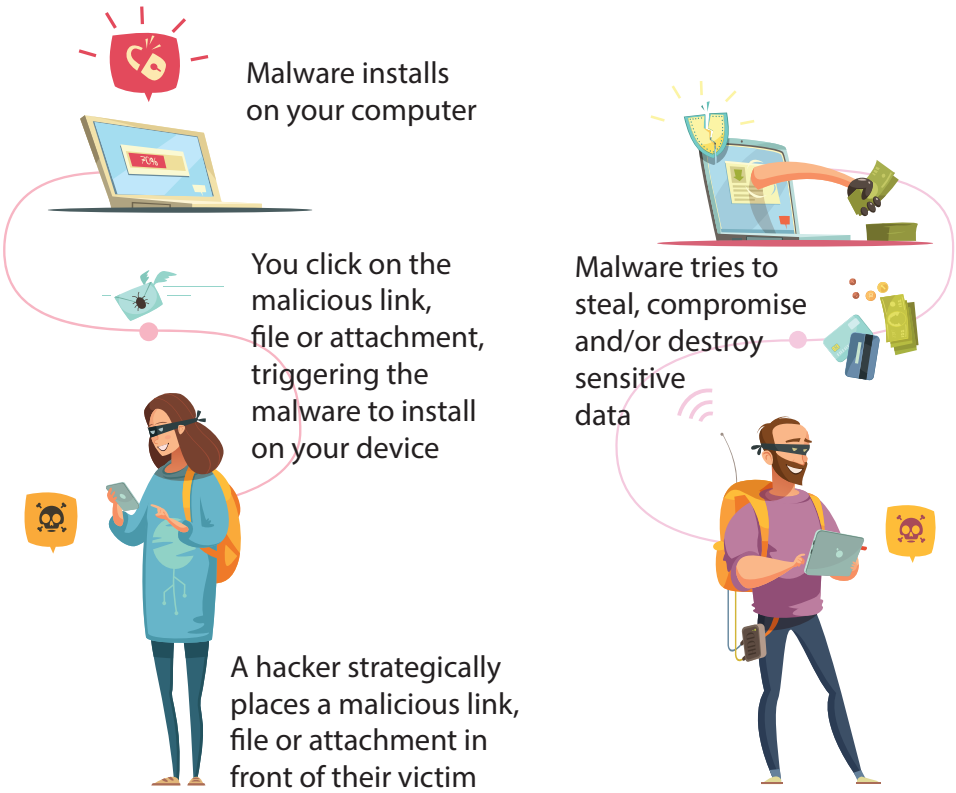
What to Do If You Suspect a Phishing Scam

- Do not click or download.
- Report the scam.
- Change passwords.
- Contact your bank or credit card company.

Business Specific Protections

Implement email filtering.	Businesses should use robust (strong) email filtering systems to identify and quarantine (separate) phishing emails before they reach employee inboxes.
Data encryption.	Encrypt sensitive data to minimise potential damage from successful phishing attempts. Scramble important information to make it useless even if someone falls for a fake email.
Access controls.	Implement access controls - only allow authorised personnel to access sensitive information. Make sure only the right people can see important information by setting access controls.
Phishing simulation exercises.	Regularly do phishing simulation exercises to test employee awareness and preparedness.

Malware Attacks Explained



Malware and Identity Theft: A Malicious Partnership

Malware comes in various forms, like viruses, worms, or trojan horses. You might download them unknowingly through infected attachments, clicking malicious links, or visiting compromised / unsafe websites.

Silent Thief

Once installed, malware operates in the background, stealing your information like usernames, passwords, credit card details, or even browsing history.

With this stolen information, criminals can commit various identity theft crimes, such as:

- Financial Fraud
- Opening New Accounts
- Tax Fraud

Real-Life Example

In 2014, a major point-of-sale breach at a retail chain involved malware that infiltrated the company's systems. This malware scraped customer credit card information. This stolen data was then used to commit large-scale financial fraud, leaving many customers struggling with unauthorised charges and compromised credit.

Protecting Yourself

By understanding how malware infects devices and the potential consequences, you can take steps to protect your personal information:

- Software updates
- Antivirus and anti-malware software
- Download with caution
- Firewalls
- Business Security Measures

In addition to the above, businesses should implement

- Endpoint security solutions
- Vulnerability scanning
- Application whitelisting: Only allow authorised applications to run on company devices, reducing malware infection risk.

If You Suspect Malware Infection

- Run a scan: Use your antivirus or anti-malware software to identify and remove threats.
- Change passwords.

Social Engineering and Identity Theft: The Art of Deception

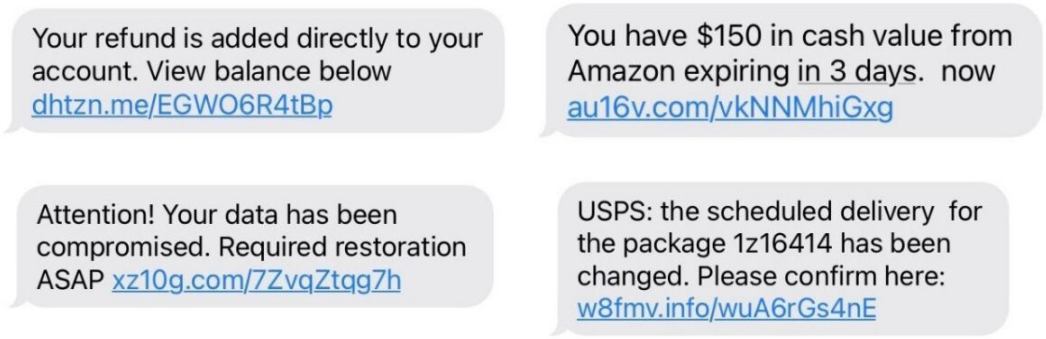
Social engineering is when criminals trick you into giving up personal information or taking actions that compromise your security. They don't need fancy hacking techniques - they just play on your trust and emotions. This can lead to identity theft, where they use your information to steal money or commit crimes in your name.

Common Tricks

Pretexting.	They pretend to be someone you trust, like a bank or tech support person. They'll make up a story to get your personal information.
Baiting.	They offer you something free or exciting, but you have to give them something valuable first, like your credit card details.
Quid Pro Quo.	They offer to help you with something, but then ask for personal information or access to your device in return.

Examples

Phone scam.	You get a call from someone claiming your bank account has suspicious activity. They ask for your credit card details to 'verify' your identity. (Pretexting)
Smishing.	A text message arrives, supposedly from your credit card company, with a link to update your information. Clicking the link takes you to a fake website that steals your login credentials. (Combines social engineering and phishing)
Tech support scam.	A pop-up appears on your computer, saying it has detected malware. The message provides a phone number for 'technical support' who will try to steal your information.



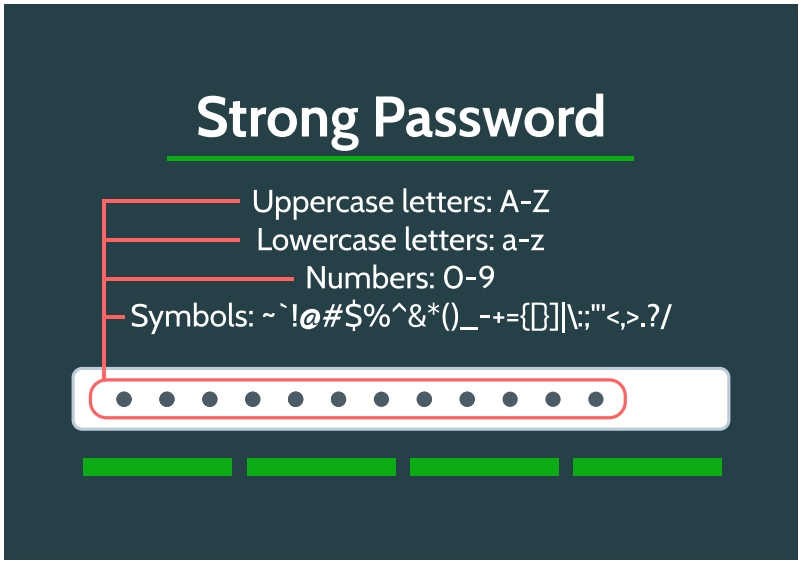
https://www.abcactionnews.com/news/national/scammers-using-text-message-phishing-scheme-to-get-personal-information-money

Stay Safe

- Don't trust unexpected requests
- Beware of urgency
- Don't click suspicious links

What to Do If Targeted

- End the communication
- Report the incident: Report it to the organisation they impersonated (if applicable) and consider reporting it to the FTC
- Change passwords



Financial Fraud: Safeguarding Your Money in a Risky World

Criminals use various tactics (phishing, malware, social engineering) to steal your money through:

Account Takeover.	Gaining access to your bank, credit card, or investment accounts to steal funds.
Payment Card Fraud.	Using stolen credit or debit card details for unauthorised purchases.
Internet Banking Fraud.	Targeting online bank accounts to steal money.
Identity Theft.	Using your stolen ID to open new accounts or claim benefits in your name.

Protect Yourself

- Don't share financial information with strangers.
- Use strong passwords and Multi-Factor Authentication for financial accounts.
- Monitor accounts for suspicious activity.
- Secure your devices with antivirus software.
- Report suspected fraud to your financial institution.
- Businesses: Invest in security measures, train employees, and stay informed about new fraud schemes.

By understanding these common tricks and taking preventative actions, you and your business can significantly reduce the risk of financial fraud.

Key Takeaways

- Identity theft is a serious threat, but you've gained the knowledge to fight back by understanding the tricks criminals use – phishing scams, malware, social engineering, and financial fraud.
- This lesson equipped you to recognise these threats, implement safeguards, and protect your personal information. Remember, a little caution goes a long way. Be wary of unsolicited contacts, scrutinise information before sharing, and secure your devices and accounts with strong passwords and MFA. By staying informed and taking proactive steps, you can confidently navigate the digital world and protect your identity.

Assessment

Multiple Choice. Underline the best answer..

1. Which of the following is NOT a common method used in phishing scams?

   a. Sending emails that appear to be from legitimate sources

   b. Including malicious attachments or links in emails

   c. Creating a sense of urgency to pressure you into acting quickly

   d. Offering free gifts or prizes in exchange for personal information

2. Malware can steal your personal information in several ways. Which of these is NOT a common method?

   a. Recording your keystrokes with a keylogger

   b. Monitoring your browsing history with spyware

   c. Granting remote access to your device to criminals

   d. Directly stealing your information from your online accounts

3. Social engineering relies on manipulating individuals. Which of these tactics does NOT involve social engineering?

   a. Sending a fake email claiming your bank account has been compromised

   b. Calling you and impersonating a tech support representative

   c. Warning you about a data breach and urging you to update your login information on a fake website

   d. Updating your antivirus software automatically

4. Financial fraud encompasses a wide range of illegal activities. Which of the following is NOT a typical method of financial fraud?

   a. Using stolen credit card information to make unauthorised purchases

   b. Stealing your Social Security number to open new accounts in your name

   c. Physically stealing checks from your mailbox and altering them

   d. Offering legitimate investment advice through a secure online platform

5. You receive an email from your bank, informing you about suspicious activity on your account. The email asks you to click on a link and verify your identity by entering your login credentials. What red flags should you identify in this scenario, and what actions should you take instead?

6. While browsing social media, you see an advertisement for a new mobile game that promises exclusive in-game rewards if you share your phone number and email address. How can you assess the legitimacy of this offer and protect yourself from potential identity theft?

7. Imagine you are explaining identity theft risks and prevention strategies to a friend or family member who is not very tech-savvy. In your discussion, discuss two different types of identity theft and outline at least three key security measures they can implement to minimise their risk. (Open Ended Response)

lesson 4

Adopting Good Cyber Security Practices

Lesson Objectives

By the end of this lesson, learners should be able to:

- Identify key practices to secure your devices and data.
- Understand how to prevent attacks and safeguard your information.
- Have the knowledge to navigate the digital world safely.

Topic

KM-01-KT04 Adopting good cyber security practices

Topic Elements

KT0401	Use of registered software
KT0402	Update software when they become old to newer versions which tend to have more security upgrades
KT0403	Encrypt data
KT0404	Use strong authentication (passwords and credentials) for all accounts
KT0405	Change passwords often and make sure they are strong and not easy to guess
KT0406	Data backup

IACW

IAC0401	The importance of adhering to good cyber security practices is justified

The weighting is 15%

Essential Cyber Security Practices

Our daily lives depend on computers and mobile devices. They connect us, inform us, and manage our personal and professional lives. However, this constant connectivity exposes us to potential cyber threats. Get ready to learn how to protect your devices and information, at home and in the office.

Use Registered Software

Why?

- Safe software is built with security in mind from the start.
- Trusted software gets checked thoroughly to find any weak spots.
- Reputable software companies keep sending updates to patch any holes that might appear.

How?

- Download software only from official app stores or verified publisher websites.
- Read reviews before downloading to identify potential security concerns.
- Be wary of free software promises that seem too good to be true.

Benefits:

- Peace of mind knowing you're using secure applications less likely to contain malware.

Software Updates: Keeping Your Defences Current

Why?

- Cyber criminals are continually coming up with new techniques to take advantage of software weaknesses. Software updates address these vulnerabilities / weaknesses with security patches.
- Updates often include bug fixes and performance improvements.

How?

- Enable automatic updates whenever possible for all your devices (computers, phones, routers).
- If automatic updates are disabled, schedule regular checks for available updates.
- Prioritise updates categorised as 'security updates' or 'critical updates.'

Benefits

- Significantly reduces the risk of cyber attacks by patching vulnerabilities. Greatly lowers the chances of cyber attacks by fixing weaknesses in the software.
- Improves software performance and functionality.

Encryption: Adding an Extra Layer of Protection

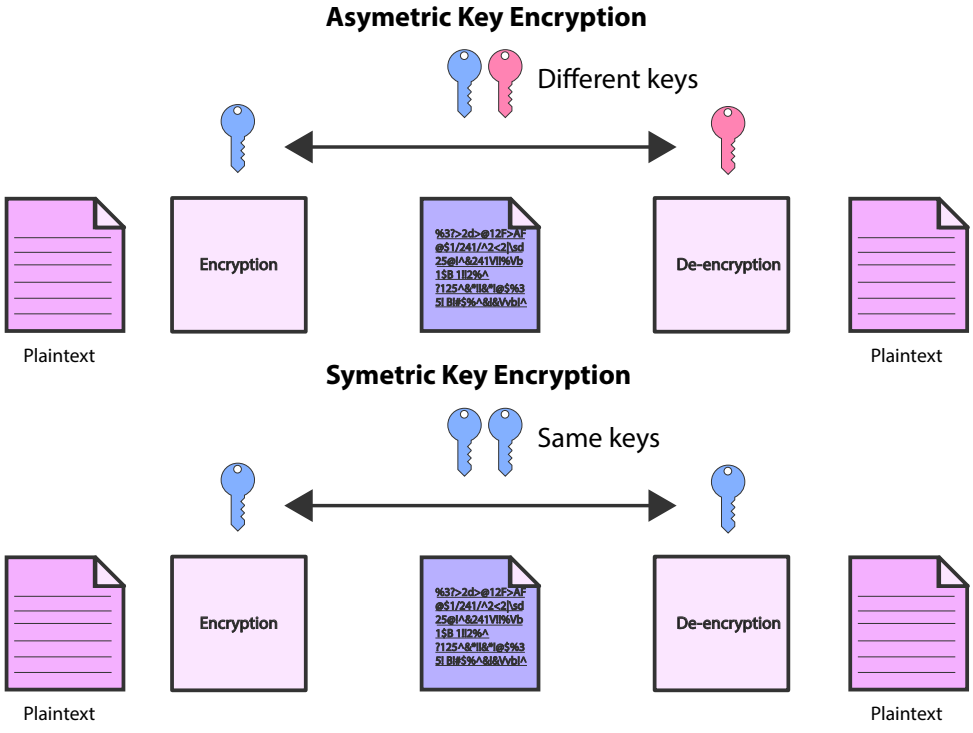
What is Data Encryption?

Imagine a locked safe for your digital information. Encryption scrambles your data, turning it into a secret code. You need a special key to unlock and read the code.

How Encryption Works

There are two main types:

- Symmetric Encryption: Uses the same key to lock and unlock the secret code.
- Asymmetric Encryption: Uses two keys – one to lock the code (public key) and another to unlock it (private key). Only you have the private key.



Why Use Encryption?

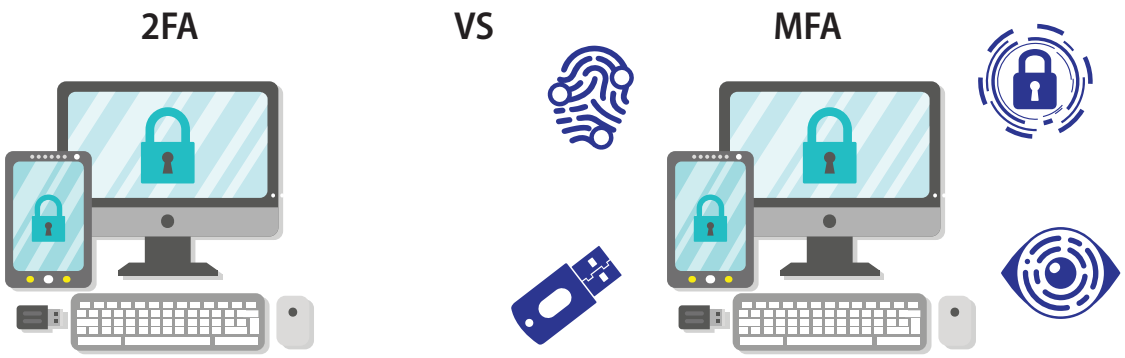
- Encryption keeps your information safe, even if someone steals your device or computer. Only those with the key can read the scrambled data.
- Safeguards data during transfer (e.g., online banking).
- Provides peace of mind for sensitive information.

How to Implement Encryption?

- Full disk encryption (protects entire hard drive).
- File and folder encryption (protects specific files).
- Cloud storage encryption (encrypts data stored in the Cloud).
- Email encryption (protects email content during transfer).
- Choosing an Encryption Method:
  - Personal Use: Built-in encryption features on devices and Cloud storage are often enough.
  - Businesses: May require dedicated encryption software for stronger protection.

Strong Authentication: The Gatekeeper of Your Accounts

Our usernames and passwords are the keys to our online accounts. Weak passwords are easy targets for cyber criminals. Strong authentication practices are very important for securing your accounts and information.



Requires you to prove your identity twice

Requires you to prove your identity multiple times

Why Strong Authentication Matters

- Defends against brute-force attacks (automated attempts to crack passwords).
- Reduces phishing scam risks (even if you enter credentials on a fake website).
- Provides a multi-layered security approach (password + additional verification).

Creating Strong Passwords

- Length is key: Aim for at least 12 characters, ideally exceeding 15.
- Complexity matters: Use a mix of uppercase and lowercase letters, numbers, and symbols.
- Avoid dictionary words, personal information, and reusing passwords across accounts.
- Consider using a password manager for secure storage and generation of strong, unique passwords.

Multi-Factor Authentication (MFA)

- Enables an extra verification step beyond your password (e.g., code sent to your phone, fingerprint scan).
- Significantly increases the difficulty of unauthorised access. / Makes it more difficult for hackers to gain access.

Benefits of Strong Authentication

- Reduces the risk of unauthorised access to online accounts.
- Makes it tougher for criminals to steal your information or pretend to be you.

Business Considerations for Strong Authentication

Businesses hold a wealth of critical information that needs protection. Strong authentication goes beyond individual privacy; it safeguards the entire organisation.

Why Strong Authentication is Crucial for Businesses

- Mitigates insider threats (compromised accounts or disgruntled employees).
- Protects customer data (reduces risk of unauthorised access and data breaches).
- Helps businesses comply with data security regulations.

Enforcing Multi-Factor Authentication (MFA)

Enforce MFA for all user accounts, including privileged accounts (administrators) with access to sensitive data. Popular MFA methods include:

Time-based One-Time Passwords (TOTP)	Users receive a unique code generated by an app on their smartphone or dedicated security token to verify their identity after entering their password.
SMS Verification	A one-time code is sent via text message to the user's registered phone number for additional verification.
Security Keys	Physical hardware tokens that connect to a device's USB port or use Bluetooth for verification.

Additional Security Measures

Single Sign-On (SSO)	Allows users to access multiple applications with a single login, reducing password fatigue (remembering too many passwords) and the risk of weak passwords being used across various platforms.
Adaptive Authentication	Analyses user login attempts and implements stricter verification steps (e.g., additional factors) for suspicious activity or attempts from unrecognised devices or locations.
Employee Training	Regularly educate employees on cyber security best practices, including password hygiene and recognising phishing attempts. This can significantly reduce the risk of social engineering attacks that bypass strong authentication measures.

Benefits of Strong Authentication for Businesses

Reduced Risk of Data Breaches	MFA significantly increases the difficulty of unauthorised access, protecting sensitive business data and customer information.
Enhanced Regulatory Compliance	Many data privacy laws / regulations demand strong authentication for user access, and using these measures helps businesses stay compliant.
Improved Brand Reputation	Data breaches can damage a company's reputation.

Using strong security checks shows you take protecting information seriously. This builds trust with customers and partners who know their data is safe.

Additional Considerations

User Experience	Balancing security with a smooth user experience is important. Choose MFA methods that are convenient and easy for employees to use while maintaining robust (strong) protection.
Scalability	Consider solutions that can scale to accommodate a growing workforce and integrate seamlessly with existing business applications.
Cost	Strong security checks may be costly, but it is much cheaper than the trouble a data breach can cause.

Data Backup: Your Digital Lifeline

In today's digital age, our data is what truly makes our devices and online accounts valuable. It can include irreplaceable personal memories (photos, documents), critical business records (financial information, creative projects), and everything in between. Data backups are the digital equivalent of an insurance policy, keeping this essential information safe.

What is Data Backup and Why is it Important?

- A data backup is a copy of your important files stored separately from the originals. This could be an external hard drive, a solid-state drive (SSD), or even Cloud storage.
- Data loss can happen for many reasons: hardware failures, software malfunctions, cyber attacks (like ransomware), accidental deletion, or even natural disasters. Backups ensure you have a copy readily available for recovery, minimising downtime and potential information loss.
- Knowing your valuable data is securely backed up provides peace of mind. You won't have to constantly worry about losing irreplaceable files due to unforeseen events.

Analogy: The Fireproof Safe Deposit Box

Imagine your computer as your house and your data as important documents, photos, and belongings. A data backup would be like having a fireproof safe deposit box at the bank. In case of a fire (hardware failure), flood (data loss event), or break in (cyber attack), you'll have a secure copy of your valuables to recover.

Data Backup: A Cyber Security Essential

Disaster Recovery	Hardware failures, software malfunctions, and natural disasters can all lead to data loss. Backups ensure you have a copy for recovery, minimising downtime and information loss.
Cyber Security Threats	Ransomware and other cyber threats can encrypt or delete your data. Backups provide a safe haven, allowing you to restore it even if your primary device is compromised.
Accidental Deletion	We've all accidentally deleted important files. Backups offer a safety net, allowing you to retrieve lost data quickly and easily.

How to Implement a Data Backup Strategy

The 3-2-1 Backup Rule:

This industry standard recommends having at least three copies of your data on two different storage media, with one copy stored offsite. This ensures redundancy (making sure that your data is safe) in case of device failure or physical disasters.

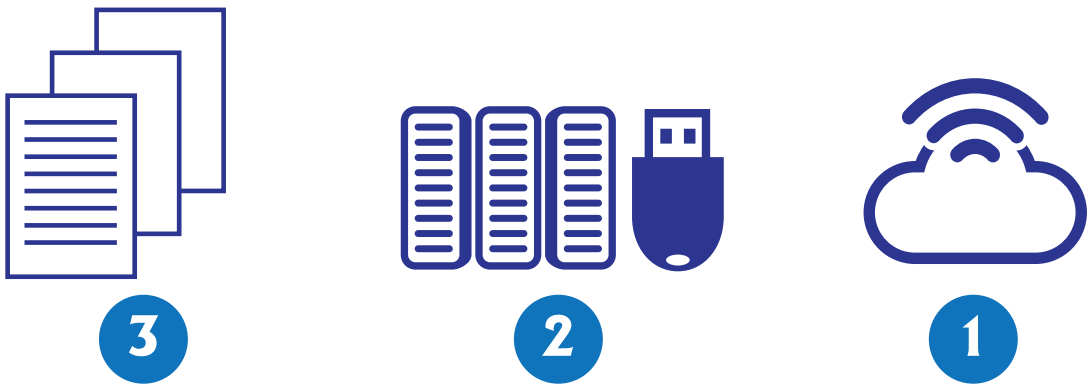
Examples:

Copy 1: External hard drive

Copy 2: Cloud storage service

Copy 3: Rotating external drive stored at a friend's house (offsite)

3-2-1 Backup strategy



Choosing Backup Media:

Consider factors like storage capacity, security features, and accessibility when choosing your backup media:

External Hard Drives (HDDs)	Affordable and high capacity, but susceptible (prone) to physical damage and slow for frequent backups.
Solid-State Drives (SSDs)	Faster and more durable than HDDs, but pricier for comparable storage. Good for frequently accessed backups or critical data.

Scheduling Backups

Don't rely on memory! Schedule automatic backups to run regularly (daily or weekly) depending on how often your data changes.

Data Backup Options: Choosing the Right Safeguard

Local Storage

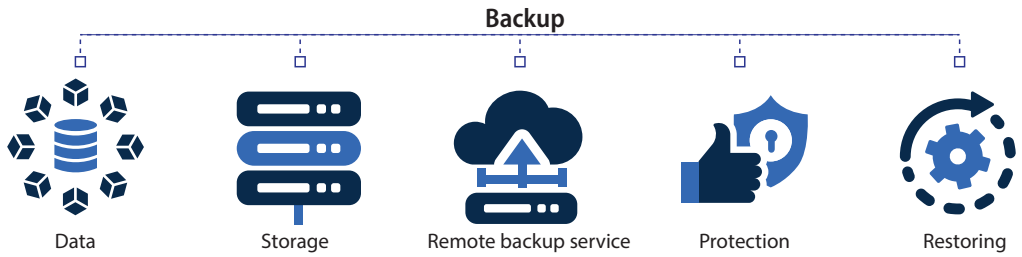
- External Hard Drives (HDDs): Affordable for large data sets, but vulnerable to physical damage.
- Solid-State Drives (SSDs): Faster and more durable than HDDs, but more expensive.

Cloud Storage

- Cloud Backup Services: Convenient, offer automatic backups, but cost subscription fees and may have storage or upload speed limitations.
- Online File-Sharing Platforms: Limited free storage for essential documents, but security features and reliability may vary.

Network-Attached Storage (NAS)

- NAS Devices: Offer centralised storage for backups from multiple devices, balancing local storage and remote accessibility. Requires an initial investment (set up cost).



Choosing the Best Option For You

Volume of Data	How much data do you need to back up? Large data sets might require high-capacity options like external hard drives or Cloud storage with generous plans.
Frequency of Backups	How often do your files change? If you work with frequently updated data, consider faster backup options like SSDs or Cloud storage with automatic features.
Budget	Local storage options are generally more affordable upfront, while Cloud storage might incur ongoing subscription fees.
Accessibility	How important is it to access your backups remotely? Cloud storage offers remote access, while local storage requires physical access to the device.
Security	Ensure your chosen solution offers robust security features, especially for sensitive data.

Key Takeaways

- The internet is a great place to connect with people, share information, and get things done. But just like in the real world, there can be some dangers online.
- This lesson teaches you important ways to protect yourself online, so you can explore the internet safely and confidently.

Assessment

Instructions: Read each question carefully and select the best answer.

Multiple Choice. Underline the best option.

1. Why is it important to download software from reputable sources?
   a. Reputable sources offer free trials for all software.
   b. Registered software is more likely to contain hidden malware.
   c. Registered software undergoes testing and is less likely to have vulnerabilities.
   d. Reputable sources offer discounts on software licenses.

2. What is the main benefit of keeping your software updated?
   a. Updates offer new features and functionalities.
   b. Updates remove unwanted toolbars from your browser.
   c. Updates often include security patches that address vulnerabilities.
   d. Updates automatically back up your data to the Cloud.

3. What does data encryption do?
   a. It organises your data into folders for easier access.
   b. It deletes unnecessary files to free up storage space.
   c. It scrambles your data into an unreadable format.
   d. It automatically uploads your data to a secure Cloud storage service.

4. Why is strong authentication (like two-factor authentication) important for online accounts?
   a. It allows you to access all your accounts with a single password.
   b. It simplifies the login process for frequently used websites.
   c. It adds an extra layer of security beyond just your password.
   d. It automatically generates strong passwords for all your accounts.

5. Which of the following is the BEST practice for creating strong passwords?

   a. Use short and simple passwords that are easy to remember.

   b. Include personal information like your birthday or pet's name.

   c. Create long passwords with a mix of uppercase and lowercase letters, numbers, and symbols.

   d. Use the same password for all your online accounts.

6. What is the main advantage of regularly backing up your data?

   a. It frees up storage space on your device.

   b. It automatically updates your software to the latest versions.

   c. It allows you to recover your data in case of loss or damage.

   d. It strengthens the encryption of your sensitive information.

7. Explain the importance of adhering to good cyber security practices. Use specific examples from the covered topics in your answer.

lesson 5

Safeguard Mobile, Media and Social Networking Profiles as User

Lesson Objectives

By the end of this lesson, learners will be able to:

- Explain the importance of safeguarding mobile devices, media, and social media profiles.
- Identify the risks associated with unsecured devices and social media use, including data loss, identity theft, and reputational damage.
- Implement security measures to protect your mobile devices and media, such as strong passwords, software updates, and encryption.
- Manage your social media presence responsibly by understanding privacy settings, avoiding scams, and thinking before you post.
- Recognise the importance of social media awareness training in a business environment.

Topic

KM-01-KT05 Safeguard mobile, media and social networking profiles as user

Topic Elements

KT0501	Security on social networking sites
KT0502	Securing mobile devices

IACW

IAC0501	The importance of safeguarding mobile and media devices is justified
IAC0502	Mechanisms to safeguard mobile and media devices are discussed

The weighting is 10%

Introduction

In today's digital world, our mobile devices, media files, and social media accounts contain a lot of personal and sometimes sensitive information. Protecting this information is very important for our privacy and security, and it can even affect our professional reputation. This lesson will teach you how to keep your mobile devices and media safe, as well as how to use social media responsibly.

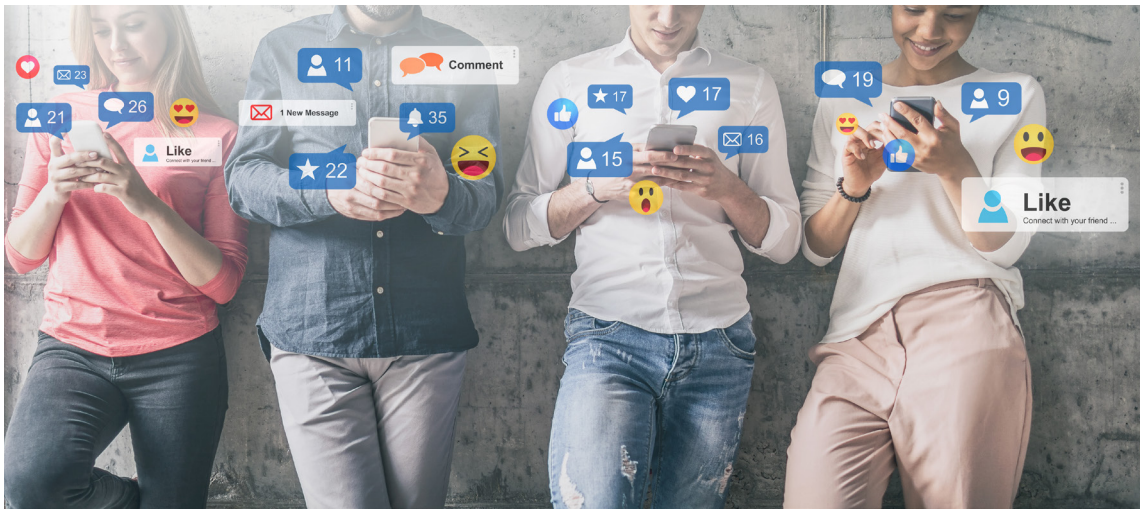
Social Networking Savvy: Tips for Safe and Enjoyable Engagement

Social media platforms offer a great way to connect with others, share experiences, and build relationships. However, it's important to be aware of the potential risks and take steps to protect your privacy and security.

Cultivating a Positive Online Presence

(inspirational quotes, professional achievements, hobbies) contrasted with content to avoid negativity, oversharing personal details)

Mind your content	Share things that show your interests and values. Avoid sharing too much personal information or negative comments.
Be selective about your connections	Connect with people you know and trust. Be careful about accepting friend requests from strangers.
Choose what you see	Follow accounts that are interesting and positive. You can choose not to see content that you don't like.



Privacy and Security Measures

Strong passwords and 2FA	Use strong passwords that are hard to guess and turn on two-factor authentication (2FA) for added security. Don't use the same password for multiple accounts.
Privacy settings	Regularly check and adjust your privacy settings to control who can see your posts and information.
Beware of phishing and scams	Be cautious of clicking on suspicious links or downloading files shared on social media. Don't share personal information readily or fall for online scams promising quick money or prizes.
Think before you post	Once you post something online, it's hard to remove completely. Be careful not to share anything that could harm you or others.
Suspicious links and scams	Be careful of clicking on suspicious links or downloading files from unknown sources shared on social media.

Additional Tips

- Report Bad Content: If you see something inappropriate or harmful online, you can report it.
- Be Aware of Ads: Remember that some content might be trying to sell you something.

The Importance of Safeguarding Mobile and Media Devices

Our mobile devices and media storage hold lots of important information, like personal photos, contact lists, bank information, and work documents. It's important to keep this information safe.

- Personal photos and videos
- Contact information
- Financial records
- Work documents and communication
- Login credentials for various accounts

Losing access to these devices or having them compromised can lead to significant consequences:

- Data loss
- Identity theft
- Financial loss
- Privacy violations
- Business disruption

By implementing proper security measures, we can significantly reduce these risks and safeguard our valuable information.

Mechanisms to Safeguard Mobile and Media Devices

There are various ways that you can protect your mobile devices and media:

Strong PINs and Passwords	Use strong passwords or PINs to lock your phone. Don't use easy-to-guess codes or personal information like your birthday.
Software Updates	Keep your phone's software updated. These updates often include important security fixes.
Mobile Security Software	You can download apps that help protect your phone from viruses and other threats.
Encryption	This scrambles your data so it's unreadable if someone steals your phone.
Regular Backups	Make copies of your important information and store them somewhere safe, like on a computer or in the Cloud.
Be Careful on Public Wi-Fi	Avoid using public Wi-Fi for sensitive activities like online banking.

Business Considerations: Protecting Your Brand Online

It's also important for businesses to protect their mobile devices and social media accounts. A security problem with a work phone or social media account could expose private customer information or company secrets. Here are some things businesses can do:

Data Breaches

- Compromised employee devices or social media accounts can be gateways to a wealth of sensitive information. This could include customer data (names, addresses, financial details), intellectual property, trade secrets, or confidential business communications.
- Businesses should implement strong mobile device management (MDM) solutions to enforce security policies, track devices, and remotely wipe data if needed in case of loss or theft.
- Social media training for employees should emphasise the importance of cyber hygiene and avoiding sharing sensitive information on business profiles.

Reputational Damage

- A single inappropriate social media post by an employee can quickly go viral, damaging your brand image and customer trust.
- Develop clear social media guidelines for employees outlining acceptable use, content restrictions, and confidentiality protocols.

Employee Training

Employees are often the first line of defence against cyber threats. Training should cover best practices for securing mobile devices with strong passwords, keeping software updated, and being cautious about using public Wi-Fi.

Additional Considerations

Social media monitoring	Consider using social media monitoring tools to track brand mentions and identify potential issues early on.
Crisis management plan	Develop a crisis communication plan to address negative publicity or data breaches effectively, minimising damage to your reputation.
Clear social media policy	Have clear rules about what employees can and can't do with company devices and on social media.

Key Takeaways

- Protecting our mobile devices, media, and social media is essential for our safety and well-being, both personally and professionally.
- By taking simple steps like using strong passwords, keeping our software updated, and being mindful of what we share online, we can reduce the risk of data breaches, identity theft, and other threats.
- Remember, cyber security is an ongoing process. It's important to stay informed about the latest threats and adapt our practices accordingly.

Assessment

Multiple Choice. Underline the best answer.

1. Why is setting a strong PIN or password on your mobile device important?

   a. It personalises the look and feel of your device.

   b. It prevents unauthorised access to your data and applications.

   c. It improves the battery life of your device.

2. Identify a benefit of keeping your mobile device software updated.

   a. It allows you to access exclusive features from the developer.

   b. It offers new customisation options for your device.

   c. It addresses security vulnerabilities that could be exploited by attackers.

3. Briefly explain one additional security measure you can take to safeguard your mobile device (besides setting a strong PIN and keeping software updated).

Multiple Choice. Underline the best answer.

4. Why is it important to be cautious about what information you share on social media?

   a. It might damage your professional reputation.

   b. Personal information can be used for targeted scams or identity theft.

   c. All of the above.

5. What is a good practice for managing your social media privacy settings?

   a. Regularly review and adjust your privacy settings to control who can see your information.

   b. Leave all settings to their default options.

   c. Share your login credentials with trusted friends so they can help you manage your profile.

6. Briefly explain one way you can strengthen the security of your social media accounts (besides adjusting privacy settings).

lesson 6

Protecting Your Digital World: Essential Security Measures for Computers, Accounts, and Data 1

Lesson Objectives

By the end of this lesson, learners should be able to:

- Understand the importance of protecting computers, accounts, and data.
- Explain the benefits of having strong security practices in place.

Topic

KM-01-KT06 Protecting computers, accounts and data as user.

Topic Elements

KT0601	Securing operating systems
KT0602	Internet security
KT0603	Securing email communications
KT0604	Securing the Cloud
KT0605	Securing network connections

IACW

IAC0601	Measures of protecting computers, accounts and data are identified
IAC0602	The advantages of protecting computers, accounts and data are elaborated

The weighting is 20%

Introduction

In today's digital age, our computers, online accounts, and data are valuable assets. Protecting them from unauthorised access, theft, or damage is important for both personal and professional security. In this lesson, we'll explore essential security measures you can put in place to safeguard your digital world. By understanding these measures and taking proactive steps, you can significantly reduce the risk of cyber attacks and protect your valuable information.

Section 1: Securing Your Operating System

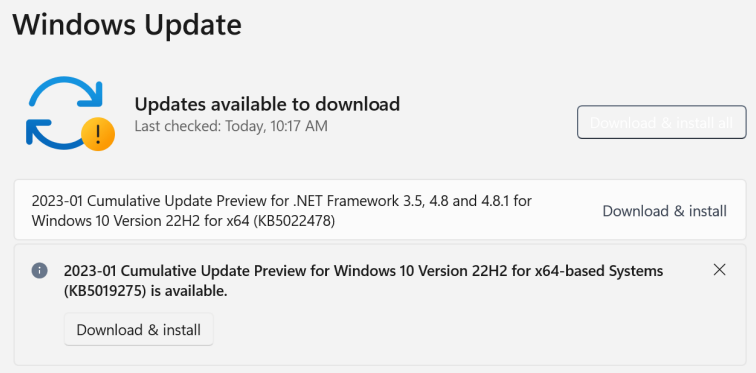
Your computer's operating system (OS) is like the heart of your digital world. Keeping it secure is the first step to overall protection. Here's what you need to do:

Software Updates

Regularly install updates from the operating system provider (like Microsoft or Apple). These updates often include important security fixes to protect against threats.

Example

Microsoft releases updates for Windows every month to address newly discovered vulnerabilities.



Firewalls

A firewall acts as a barrier between your computer and the internet, filtering out bad traffic. Make sure your firewall is turned on and configured correctly.

Example

Windows Firewall is a built-in firewall in Windows operating systems.

Antivirus and Anti-Malware Software

These programmes scan your computer for harmful software like viruses and remove them. Choose a reputable antivirus and anti-malware programme and keep it updated.

Example

Popular antivirus software includes Avast, Norton, and Bitdefender.

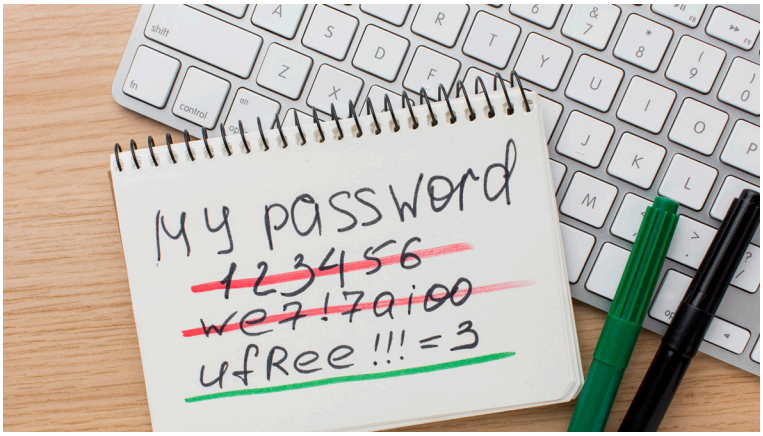
User Account Management

If your computer allows multiple users, create separate accounts for everyday tasks and administrative functions. Use a standard account for daily work and a more protected administrator account for making changes to the system settings.

Example

You might have a 'guest' account for visitors to use your computer without accessing your personal files.

Strong Passwords and MFA	Use strong passwords for all your accounts, including your computer login. A strong password is long, includes a mix of letters, numbers, and symbols, and isn't easy to guess. You can also add extra security by using Multi-Factor Authentication (MFA) whenever possible. This usually involves entering a code from your phone along with your password. *Example* A strong password might be 'MyD0gL0vesB1scu1ts!', while a weak password would be 'password123.'



Virtualisation (Optional)	If you need to run different operating systems on one computer, virtualisation can be helpful. Just remember to keep both the main operating system (host) and the virtual systems (guests) updated and secure. *Example* VirtualBox is a popular virtualisation software that allows you to run multiple operating systems on the same computer.
Vulnerability Assessment and Patch Management	Regularly check for weaknesses in your system and software and install updates ('patches') to fix them. This helps prevent attackers from exploiting these weaknesses. *Example* A vulnerability scanner might identify an outdated web browser version on your system. You would then install the latest version to fix any security holes.

Internet Security Best Practices

Staying safe online is essential, whether you're browsing for fun or doing business. Here's how you can protect yourself:

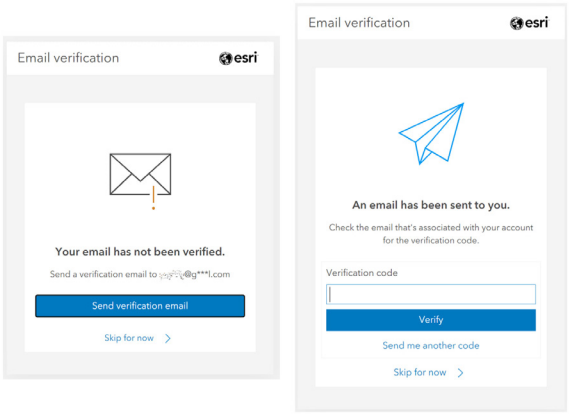
Secure Systems and Software	Keep all your devices (computers, phones, tablets) updated with the latest security patches. Use antivirus and anti-malware software on personal devices, and make sure your business has a strong security solution to protect its network. *Example* Make sure your antivirus software automatically updates its virus definitions to protect against the latest threats.
Strong Passwords and MFA	Use strong, unique passwords for every account, and enable MFA whenever possible. *Example* When banking online, use a password that is different from your social media passwords.
Secure Browsing Habits	Be careful about what websites you visit and what you download. Avoid clicking on suspicious links or opening attachments from unknown senders. Always look for the lock symbol ('https') in the web address bar when you enter personal or financial information. *Example* Avoid clicking on links in emails that promise free money or prizes, as these are often scams.

Network Security (Businesses)	Businesses should use firewalls to control what can enter and leave their networks.
User Education and Awareness	Teach employees how to identify phishing emails, use strong passwords, and stay safe online.
Secure Data Management	**Data Encryption** Use encryption to scramble your important data so it's unreadable if someone tries to steal it. *Example* FileVault is a built-in encryption feature in macOS that can protect your data if your computer is lost or stolen. **Data Backups** Make copies of your important data and store them somewhere safe, like an external hard drive or Cloud storage. **Data Disposal** When you no longer need data, make sure it's completely deleted or destroyed so no one else can access it.

Securing Email Communications

Email is a common way for hackers to try to trick you. Here's how to protect your inbox:

Enable Spam Filters	This will help block many unwanted and potentially dangerous emails. *Example* Most email providers offer spam filtering options in their settings.
Be Careful with Attachments and Links	Only open attachments and click on links from people and organisations you trust.
Check Sender Addresses	Make sure the sender's email address is correct. Scammers often use addresses that look very similar to real ones. *Example* An email that appears to be from your bank might actually come from a scammer using a slightly different address like '[email address removed]' instead of 'yourbank.com.'



Businesses can take extra steps

Email Encryption	This scrambles email messages so they can only be read by the intended recipient. *Example* Pretty Good Privacy (PGP) is a popular email encryption software.
Data Loss Prevention (DLP)	This technology helps prevent sensitive information from being sent out through email.

Securing the Cloud

The Cloud is a convenient way to store and access data, but you still need to keep it secure.

Choose a Trusted Provider	Do your research and choose a reputable Cloud provider with strong security measures.
Strong Passwords and MFA	Use strong, unique passwords for your Cloud accounts and enable MFA.
Encrypt Your Data	If possible, encrypt your data before storing it in the Cloud.
Be Aware of the Shared Responsibility Model	Remember that you are also responsible for protecting your data in the Cloud. The Cloud provider is responsible for the security of the underlying infrastructure, but you are responsible for securing your own data and access.
Regularly Review Cloud Security Settings	Make sure your Cloud storage settings are configured for maximum security.

Securing Network Connections

When you connect to the internet, it's important to protect your connection:

Secure Home Networks	Use a strong password for your Wi-Fi and make sure it's encrypted. For businesses, consider creating a separate guest network for visitors. *Example* Use WPA3 encryption, which is the latest and most secure Wi-Fi security protocol.
Public Wi-Fi	Avoid using public Wi-Fi for private activities such as online banking. If you must use it, consider using a VPN (Virtual Private Network) to encrypt your connection. *Example* A VPN creates a secure tunnel for your internet traffic, making it much harder for hackers to intercept your data.
Unidentified Networks	Don't connect to Wi-Fi networks you don't recognise. They could be set up by hackers to steal your information.

Key Takeaways

- By understanding the threats and taking the necessary precautions, you can protect your computers, accounts, and data from harm. Remember, cyber security is an ongoing process.
- Stay informed, stay vigilant, and don't hesitate to seek help from experts when needed.

Assessment

Multiple Choice. Underline the best answer.

1. The most effective way to keep your operating system secure is to:

   a. Use the same password for all your accounts.

   b. Regularly install updates from the operating system vendor.

   c. Disable your firewall.

   d. Click on all links in emails, even from unknown senders.

2. Describe two additional security measures you can implement to enhance the security of your operating system.

3. True or False: It's safe to download files from any website.

4. True or False: Strong passwords should include a combination of uppercase and lowercase letters, numbers, and symbols.

5. Match the phrase in column A to the description in column B that best matches it. Write the letter in the answer column.

A	B	Answer
a. Phishing scam	1. A complex password that is difficult to guess.	
b. Malware	2. A deceptive email designed to trick you into revealing personal information.	
c. Strong password	3. A programme that can steal your data	

Multiple Choice. Underline the best answer

6. The best way to protect yourself from phishing attacks via email is to:

   a. Always click on links embedded within emails.

   b. Be cautious of emails from unknown senders and avoid clicking on suspicious links or attachments.

   c. Share your login credentials with anyone who requests them.

   d. Never enable spam filters.

7. Why is it important to use strong passwords for your email accounts?

8. Briefly describe two ways you can ensure the security of your data stored in the Cloud.

lesson 7

Protecting Your Digital World: Essential Security Measures for Computers, Accounts, and Data 2

Lesson Objectives

By the end of this lesson, learners should be able to:

- Identify the importance of safeguarding computers, accounts, and data.
- Implement security measures to secure your devices and information.
- Develop responsible online habits.

Topic

KM-01-KT06 Protecting computers, accounts and data as user (second lesson on this KM)

Topic Elements

KT0606	Firewalls
KT0607	Antivirus programmes
KT0608	Antispyware

IACW

IAC0601	Measures of protecting computers, accounts and data are identified
IAC0602	The advantages of protecting computers, accounts and data are elaborated

The weighting is 10%

Introduction

Think of your computer like a house filled with valuable possessions. Just as you lock your doors and windows to protect your home, you need to take measures to secure your digital life. In this lesson, we'll continue exploring essential tools and practices that act like locks, alarms, and security cameras for your digital world. By understanding these measures, you can reduce the risk of cyber attacks and keep your information safe.

Firewalls: Your Network's First Line of Defence

A firewall is like a security guard for your computer network. It controls what information is allowed to enter or leave your computer. Imagine it as a gatekeeper, checking everything that tries to pass through and only letting in what's safe. Firewalls help protect your computer from unauthorised access and harmful programmes (malware). They can block hackers and stop them from stealing your information, helping to keep your network safe and running smoothly.

Types of Firewalls

Packet Filtering Firewalls	These check individual pieces of data (like letters in an envelope) to see if they follow the rules.
Proxy Firewalls	These act as a middleman between your computer and the internet, hiding your information from prying eyes.
Stateful Firewalls	These keep track of ongoing conversations (like phone calls) and block any unexpected interruptions.
Application-Level Firewalls	These look at specific apps and programmes to control what they can do on the internet.
Next-Generation Firewalls (NGFWs)	These are more advanced firewalls with extra features like checking the contents of data packets for hidden threats.

Where to Put Your Firewall

Firewalls can be:

- Hardware: Physical devices, like a router, connected to your network.
- Software: Programmes installed on your computer, like the Windows Firewall.
- Cloud-Based: Services that filter your internet traffic through a remote server.

Antivirus Software: Your Digital Shield

Antivirus software is like a shield for your computer, protecting it from a wide range of harmful software:

Viruses 	Small programmes that can copy themselves and infect other files, causing damage to your computer.
Worms 	Similar to viruses, but they spread quickly through networks without needing to attach to other files.
Trojan Horses 	These programmes disguise themselves as harmless software, but once inside your computer, they can steal information or allow hackers to take control.
Ransomware 	This type of malware encrypts your files, making them inaccessible until you pay a ransom.
Spyware 	This sneaky software hides on your computer and collects your personal information without your knowledge.

How Antivirus Software Works

First, it scans your computer for known threats, comparing files and programmes to a database of known malicious software. It offers real-time protection, continuously monitoring your computer for suspicious activity. If it finds malware, it quarantines (isolates) or removes it to prevent it from harming your system. And finally, it automatically updates itself to stay current with the latest threats.

Benefits of Antivirus Software

- Prevents data loss and damage to your computer.
- Helps protect your personal information from being stolen.
- Reduces the risk of your computer becoming part of a larger attack.

Antispyware: Keeping Your Information Private

Antispyware software is like a detective, searching for and removing spyware that is trying to steal your personal information.

How Antispyware Works

It scans your computer for suspicious programmes and files. Next, it monitors your computer's activity, looking for signs that spyware is trying to collect your data. And if it finds spyware, it removes it to keep your information safe.

Benefits of Antispyware Software

- Protects your privacy by keeping your personal information from being stolen.
- Helps protect your financial information, like credit card numbers and bank account details.
- Can improve your computer's performance by removing spyware that might slow it down.

Key Takeaways

This lesson explored three essential tools to build a strong defence: firewalls, antivirus, and antispyware.

- **Firewalls**: Gatekeepers monitoring traffic, firewalls come in various forms to shield your network from unauthorised access.
- **Antivirus Software**: Your champion against malware like viruses and ransomware, antivirus programmes employ real-time protection and updates to keep your system safe.
- **Antispyware Software**: A shield against stealthy threats, antispyware software detects and removes programmes that steal your personal information.

Assessment

Multiple Choice. Underline the best answer.

1. What is the primary function of a firewall?

   a. To scan your computer for malware

   b. To filter incoming and outgoing traffic on a network

   c. To steal your personal information

   d. To slow down your computer

2. What type of malware encrypts your files and demands payment to decrypt them?

   a. Virus

   b. Worm

   c. Trojan Horse

   d. Ransomware

3. What is the main advantage of using antispyware software?

   a. To improve your computer's performance

   b. To protect your financial information from unauthorised access

   c. To safeguard your privacy from spyware programmes

   d. To block malicious websites entirely

4. Which of the following is NOT a common placement option for firewalls?

   a. Hardware firewall

   b. Software firewall

   c. Internal firewall

   d. Cloud-based firewall

5. True or False: Antivirus software can protect you from all types of cyber threats.

6. True or False: Strong passwords are an important security measure that works well alongside firewalls and antivirus software.

7. Match the phrase in column A to the description in column B that best matches it. Write the number in the answer column.

A	B	Answer
a. Virus	1. Self-replicating programme that spreads from one device to another.	
b. Worm	2. Disguises itself as legitimate software to trick users into installing it.	
c. Trojan Horse	3. Encrypts your files and demands payment to decrypt them.	
d. Ransomware	4. Spreads rapidly through networks, exploiting vulnerabilities.	

8. Briefly explain the difference between a packet filtering firewall and a stateful firewall.

9. Describe two benefits of using antispyware software in addition to antivirus software.

lesson 8

Understand Security Incidents and Reporting

Lesson Objectives

By the end of this lesson, learners should be able to:

- Identify the importance of safeguarding computers, accounts, and data.
- Implement security measures to secure your devices and information.
- Develop responsible online habits.

Topic

KM-01-KT07 Understand security incidents and reporting

Topic Elements

KT0701 Data backup

KT0702 Disaster recovery

IACW

IAC0701 The effect of security incidents is explained

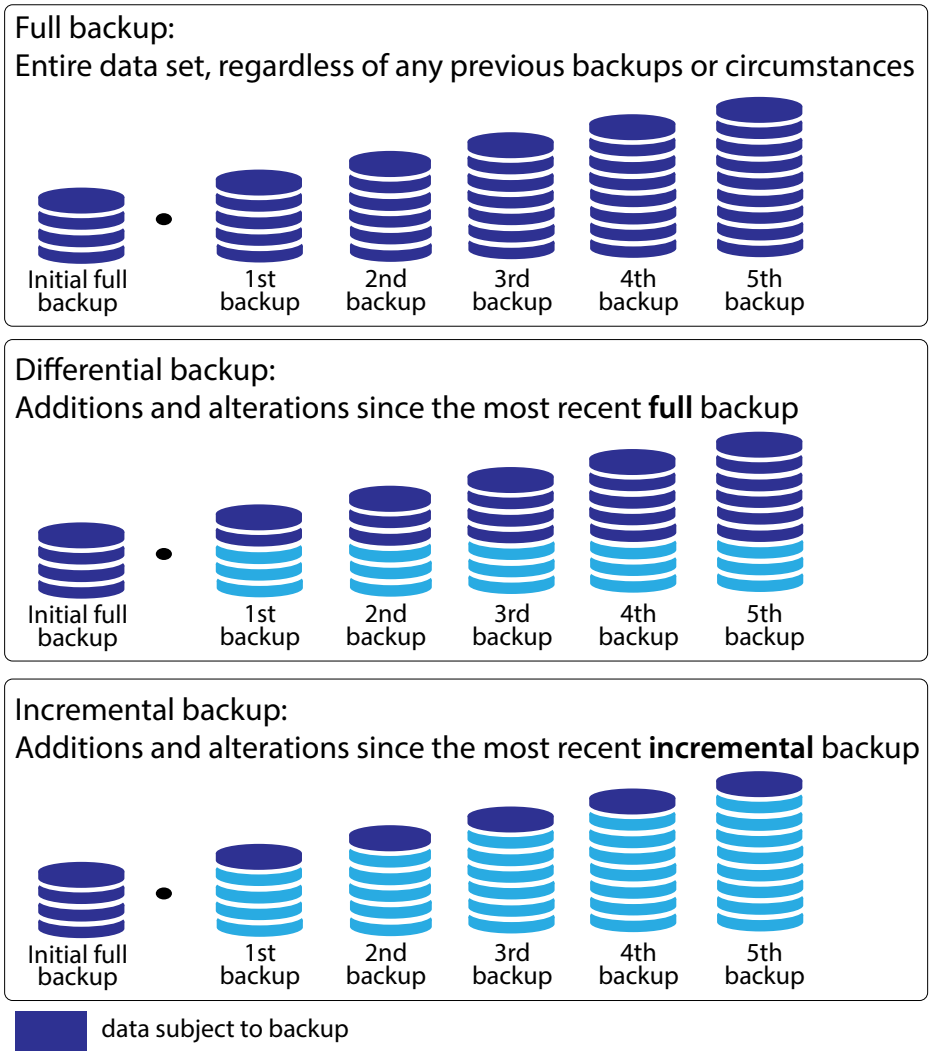
The weighting is 10%

This lesson explores the importance of data backup and disaster recovery (DR) in mitigating the effects of security incidents (SI). By understanding these concepts and their impact you can make informed decisions to safeguard your valuable data.

Data Backup – Your Digital Safety Net

Data backup creates a copy of your important information for recovery in case the original data is lost, corrupted, or becomes inaccessible due to various reasons (hardware failures, accidental deletion, malware attacks, natural disasters, system outages).

Types of Backup



Here's why data backup is crucial

Minimise Downtime	Restore data from backups and resume operations quickly.
Protect Against Data Loss	Safeguard valuable information from accidental deletion, hardware failures, and other threats.
Ensure Business Continuity	Minimise disruptions and financial losses for businesses.
Reduce Stress	Gain peace of mind knowing your data is backed up.

Let's look at an example to illustrate why data backup is so important

Hospitals rely heavily on digital patient records. Imagine a hospital facing a ransomware attack that encrypts all their patient data. Without backups, the hospital would be unable to access critical medical information, potentially delaying treatment and jeopardising patient care. However, with a robust backup strategy in place, the hospital could restore its data from backups and resume operations much faster, minimising disruption and ensuring patient safety.

Data Backup Strategies

Data backup strategies come in various flavours, each with strengths and weaknesses. Selecting the most suitable approach depends on your specific needs, considering factors like data volume, change frequency, and recovery time objectives (RTOs). Here's a closer look at some common data backup strategies:

Full Backups

Description 	Creates a complete copy of all your data at a specific point in time.
Advantages 	Simple to understand and implement, provides a complete and reliable restore point.
Disadvantages 	Time-consuming for large datasets and requires significant storage space.
Use Cases 	Ideal for initial backups, periodic full backups for comprehensive data capture, or when data changes infrequently.

Incremental Backups

Description 	Captures only the data that has changed since the last successful backup (typically a full backup).
Advantages 	Faster than full backups, consumes less storage space.
Disadvantages 	Requires the last full backup to be available for complete restoration, introduces complexity if multiple incremental backups occur before a restore.
Use Cases 	Well-suited for frequently changing data sets, where capturing modifications is crucial.

Differential Backups

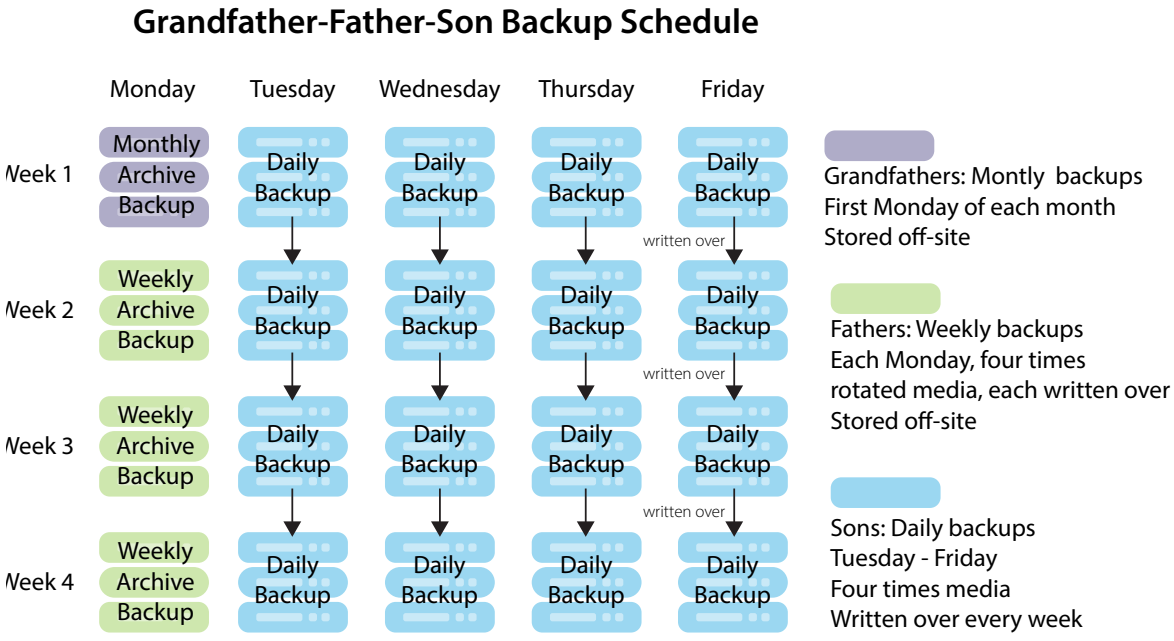
Description 	Backs up all data that has changed since the last full backup, similar to a full backup but smaller in size.
Advantages 	Faster than full backups, uses less storage space compared to full backups, eliminates the need for multiple incremental backups before restoration.
Disadvantages 	Requires the last full back up for a complete restore, slightly more complex than incremental backups.
Use Cases 	A good balance between speed, storage efficiency, and ease of restore compared to full and incremental backups.

Continuous Data Protection (CDP)

Description	Creates a continuous stream of backups, capturing data modifications as they occur.
Advantages	Offers the most up-to-date recovery point, minimising data loss in case of incidents.
Disadvantages	Requires significant storage space and processing power and can be complex to implement and manage.
Use Cases	Ideal for mission-critical applications or scenarios where minimal data loss is tolerated (e.g., financial transactions).

Backup Rotation Strategies

Beyond choosing the backup type, a rotation schedule is crucial. This determines how often backups are performed and how many versions are retained (e.g., Grandfather-Father-Son (GFS) rotation). Choosing the right combination depends on your RTO, RPO, data importance, and storage capacity.



Data Backup Storage Options: Choosing the Right Place For Your Digital

Choosing the right storage location is crucial. Here are common options:

Local Backup Storage

Pros	Fast access, cost-effective (for smaller data volumes), no internet reliance.
Cons	Vulnerable to physical threats (fire, theft), limited scalability, no offsite protection.

Cloud Backup Storage

Pros	Offsite protection, scalability, accessibility.
Cons	Internet reliance, subscription costs, security considerations.

The 3-2-1 Backup Rule

Remember the 3-2-1 rule for added protection:

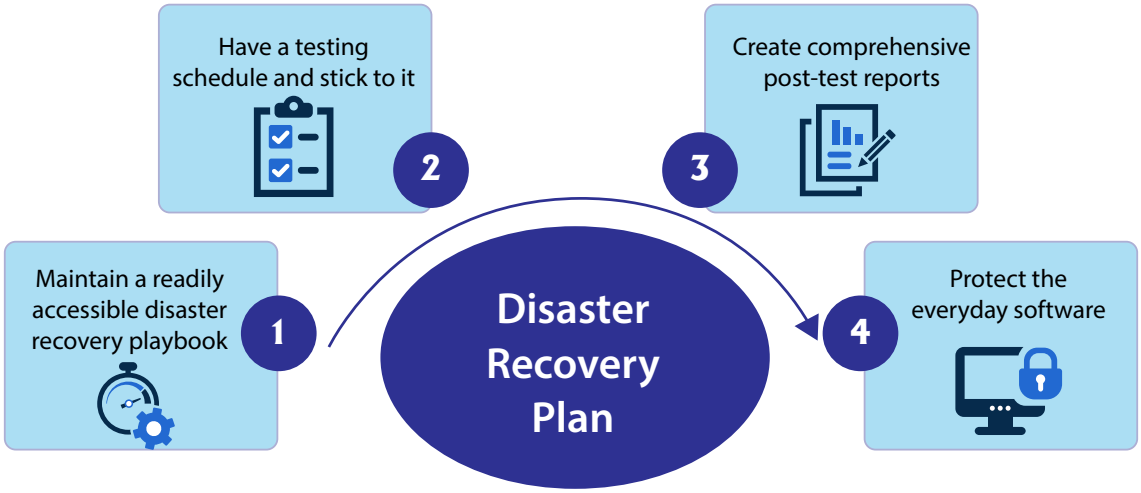
3 Copies	Maintain at least three copies of your data.
2 Media Types	Store backups on two different media types (e.g., local drive and Cloud storage).
1 Offsite Copy	Keep at least one copy of your data offsite (e.g., Cloud storage) for disaster recovery.

Disaster Recovery (DR)

Effective DR plans go beyond data recovery. Benefits to a DR include:

Reduced Downtime	DR plans ensure swift restoration of critical systems and data.
Enhanced Business Continuity	DR plans prioritise restoring core business functions.
Improved Customer Satisfaction	Rapid recovery minimises inconvenience caused to customers.
Reduced Financial Losses	The faster the recovery, the lower the associated costs.
Stronger Security Posture	DR plans often include post-incident analysis to identify vulnerabilities.
Improved Employee Morale	Knowing there's a plan reduces stress and allows employees to focus on recovery.

Best Practices to Create a Disaster Recovery Plan



Differences Between Incident Response and Disaster Recovery

Think of it like this:

Incident Response (IR) is like stopping a burglar. You catch them in the act, call the police (contain the threat), and secure your valuables (minimise damage). You might also investigate how they got in to prevent future break-ins.

Disaster Recovery (DR) is like fixing the broken window after the burglar leaves. You assess the damage, board up the window (recover critical functions), and eventually replace it (get everything back to normal).

In short:

IR Deals with the immediate attack.

DR Focuses on recovering after the incident.

Building Your Disaster Recovery PlanA Step-by-Step Guide

Even the best backups can't stop disruptions. A Disaster Recovery (DR) Plan is your organisation's roadmap to getting back on track quickly. Here's what you need to include:

Know Your Risks 	Identify what could disrupt your business – cyber attacks, power outages, natural disasters. Pinpoint the critical systems and data most vulnerable to these threats.
Prioritise Recovery 	Not all downtime is equal. A Business Impact Analysis (BIA) helps you understand how much downtime different parts of your business can handle. This helps you to prioritise what needs to be recovered first.
Backup Plan in Action 	This section details your data backup strategy (full, incremental, etc.), where your backups are stored (local, Cloud), and how to recover data if needed.
Assemble Your A-Team 	Form a team with people from IT, communication, and different departments to handle various recovery stages.
Communication is Key 	Create a communication plan outlining how you talk to employees, customers, and others during and after a disaster. Who will deliver messages, and what information will be shared?
Practice Makes Perfect 	Don't wait for a real disaster! Test your DR plan through simulations to find weaknesses and ensure everyone understands their role. Train your team on their responsibilities.

By following these steps, you can build a strong DR plan that safeguards your organisation from the unexpected.

Example of a Disaster Recovery (DR) plan

Scenario: Suspected data breach

Team: IT Security Specialist (Jia), Customer Service Manager (Ben)

Detection & Containment (Jia)	Identify suspicious activity (e.g., unusual login attempts, unauthorised access). Isolate compromised systems to prevent further data loss.
Initial Response (Combined)	Take the website offline to stop further breaches. Secure evidence for forensic analysis. Notify internal stakeholders and activate the response team.
Customer Communication (Ben)	Draft and send communication informing customers about the potential breach and steps being taken to investigate and secure their data.
Recovery & Review (Combined)	Restore systems from backups. Investigate what happened to identify vulnerabilities and implement security patches. Review incident response procedures and update the plan as needed.

This simple DR plan gives an example of how a cyber security incident might be handled. Remember, a complete DR plan would include other details and may involve more steps depending on what happened.

Security Incident Impact and DR Benefits

Security Incidents: The Impact

Data Loss/Corruption	Disrupts operations, reduces productivity, and incurs financial losses.
Reputational Damage	Erodes customer trust and harms the organisation's reputation.
Financial Costs	Data recovery, forensics, and system repairs are expensive.
Legal/Regulatory Issues	Breaches may violate regulations and lead to fines.

DR The Lifeline

- Reduced Downtime: DR plans ensure swift restoration of critical systems and data.
- Enhanced Business Continuity: Core business functions are prioritised for faster recovery.
- Improved Customer Satisfaction: Minimises inconvenience caused by disruptions.
- Reduced Financial Losses: Quicker recovery reduces costs associated with downtime.

Key Takeaways

- A proactive approach to cyber security, including data backup and DR, is essential for protecting your organisation's important assets, maintaining business as normal, and mitigating (reduce) the impact of security incidents.

Assessment

Multiple Choice. Underline the best answer.

1. Which of the following is NOT a common reason for data loss?

   a. Hardware failure

   b. Accidental deletion

   c. Software updates

   d. Malware attacks

2. What is the primary purpose of a data backup strategy?

   a. To permanently delete unwanted data

   b. To create a copy of important information for recovery purposes

   c. To improve computer performance

   d. To block unauthorised access to data

3. Which of the following is NOT a benefit of data backups?

   a. Minimises downtime after a security incident

   b. Protects against accidental data deletion

   c. Reduces the risk of malware infections

   d. Ensures business continuity in case of disruptions

4. According to the 3-2-1 backup rule, how many copies of your data should you maintain?

   a. One

   b. Two

   c. Three

   d. Four

5. What is the main difference between Incident Response (IR) and Disaster Recovery (DR)?

   a. IR focuses on recovery, while DR deals with preventing incidents.

   b. DR focuses on long-term recovery, while IR addresses immediate threats.

   c. IR is for cyber attacks, while DR is for natural disasters.

   d. DR is a subset of IR, which has a broader scope.

6. Match the phrase in column A to the description in column B that best matches it. Write the letter in the answer column.

A	B	Answer
a. Recovery Point Objective (RPO)	1. A comprehensive plan outlining steps to resume normal operations after a disruption.	
b. Disaster Recovery (DR)	2. The process of creating a copy of data that can be used for recovery.	
c. Data Backup	3. The maximum tolerable amount of data loss after a security incident.	
d. Offsite Backup	4. A geographically dispersed storage location for backups.	
e. Disaster Recovery Team	5. A team of individuals responsible for different phases of the DR process.	

7. Briefly explain two potential consequences of security incidents for organisations.

8. Describe the three main components of a well-defined DR plan.

9. Explain the importance of testing and refining a DR plan.

10. Your company experiences a power outage that disrupts critical business operations. Outline the steps you would take to recover from this situation according to a DR plan.

11. Describe two different data backup strategies (e.g., full backups, and incremental backups) and explain the advantages and disadvantages of each.

KM-01-KT01: Introduction to computer and mobile device security (15%)

Question 1: Provide three reasons why computer and mobile device security is important in today's digital age.

Marks Allocation Guide:

- Protection of personal information (1 mark)
- Prevention of identity theft (1 mark)
- Ensuring data reliability and accessibility (1 mark)

Total marks: 3

Question 2: Explain one major consequence of neglecting computer and mobile device security.

Marks Allocation Guide:

- Description of data breaches (1 mark)
- Consequence (3 marks)

Total marks: 4

Question 3: Discuss the importance of computer and mobile device security in personal and professional environments.

Marks Allocation Guide:

- Protection in personal environments (3 marks)
- Protection in professional environments (3 marks)

Total marks: 6

Question 4: What are the primary objectives of computer and mobile device security?

Marks Allocation Guide:

- Ensuring confidentiality (1 mark)
- Maintaining integrity (1 mark)
- Guaranteeing availability (1 mark)

Total marks: 3

Question 5: How does encryption help keep computers and mobile devices secure?

Marks Allocation Guide:

- Explanation of encryption process (1 mark)
- Ensuring data confidentiality (1 mark)
- Ensuring data integrity (1 mark)

Total marks: 3

KM-01-KT02: Various computer and network security threats (20%)

Question 6: Define phishing and explain how it works, providing one example.

Marks Allocation Guide:

- Definition of phishing (1 mark)
- Method of operation (1 mark)
- Example or consequence (1 mark)

Total marks: 3

Summative Assessment

Question 7: What is a Distributed Denial of Service (DDoS) attack, and how does it disrupt network services?

Marks Allocation Guide:

- Definition of DDoS (1 mark)
- Explanation of attack mechanism (1 mark)
- Disruption caused (1 mark)

Total marks: 3

Question 8: Discuss five different types of malware and their impact on computer systems.

Marks Allocation Guide:

- Explanation of various malware types (5 marks)
- Impact on computer systems (5 marks)

Total marks 10

Question 9: Identify one solution to protect against phishing attacks and explain how it works.

Marks Allocation Guide:

- Identification of solution (e.g., email filtering) (1 mark)
- Explanation of how it works (1 mark)

Total marks: 2

Question 10: What is a network firewall and how does it help in mitigating security threats?

Marks Allocation Guide:

- Definition of network firewalls (1 mark)
- Explanation of functionality (1 mark)

Total marks: 2

KM-01-KT03: Identity theft (10%)

Question 11: Explain three types of identity theft and suggest mitigation strategies.

Marks Allocation Guide:

- Explanation of different types of identity theft (6 marks)
- Mitigation strategies (3 marks)

Total marks: 9

KM-01-KT04: Adopting good cyber security practices (15%)

Question 12: Justify the importance of adhering (keeping to) to good cyber security practices for both individuals and organisations.

Marks Allocation Guide:

- Importance for individuals (protect personal information, financial assets, privacy) 4 marks
- Importance for organisations (protect data, maintain customer trust, comply with regulations) 4 marks
- Examples of good practices (strong passwords, software updates, awareness of phishing) 4 marks

Total marks: 12

KM-01-KT05: Safeguard mobile, media, and social networking profiles as user (10%)

Question 13: Why is it important to safeguard mobile devices?

Marks Allocation Guide:

- Protection of sensitive information (1 mark)
- Prevention of unauthorised access (1 mark)

Total marks: 2

Question 14: How does encrypting data on mobile devices improve security?

Marks Allocation Guide:

- Explanation of encryption process (1 mark)
- Impact on data security (1 mark)

Total marks 2

Question 15: Name one mechanism to safeguard mobile devices.

Marks Allocation Guide:

- Identification of mechanism (e.g., biometric authentication) (1 mark)
- Explanation of functionality (1 mark)

Total marks: 2

Question 16: How can regular software updates help in safeguarding mobile devices?

Marks Allocation Guide:

- Explanation of software updates (1 mark)
- Impact on device security (1 mark)

Total marks: 2

KM-01-KT06: Protecting computers, accounts, and data as user (20%)

Question 17: Identify and explain four measures to protect computers, accounts, and data. Provide examples for each measure.

Marks Allocation Guide:

- Four Measures (4 marks)
- Examples (4 marks)

Total marks: 8

Question 18: Provide three advantages of protecting your computers, accounts, and data, and provide examples of how these protections can be beneficial.

Marks Allocation Guide:

- Three advantages (3 marks)
- Three examples (3 marks)

Total marks: 6

Question 19: Discuss the role of firewalls and antivirus software in protecting computers.

Marks Allocation Guide:

- Role of firewalls (3 marks)
- Role of antivirus software (3 marks)
- Importance of regular updates and configurations (2 marks)

Total marks: 8

KM-01-KT07: Protecting computers, accounts, and data as an organisation (10%)

Question 20: Discuss the importance of establishing a cyber security policy within an organisation.

Summative Assessment

Marks Allocation Guide:

- Importance of compliance with legal and regulatory requirements (2 marks)
- Standards for employee behaviour regarding security (2 marks)
- Framework for responding to incidents (2 marks)
- Defining roles and responsibilities (2 marks)

Total marks: 8

Summary of Marks and Weighting

KT01: 19 marks (15%)

KT02: 20 marks (20%)

KT03: 9 marks (10%)

KT04: 12 marks (15%)

KT05: 8 marks (10%)

KT06: 22 marks (20%)

KT07: 8 marks (10%)

Total: 98 marks

Learner score	Score achievable	Percentage (%)
	98	%