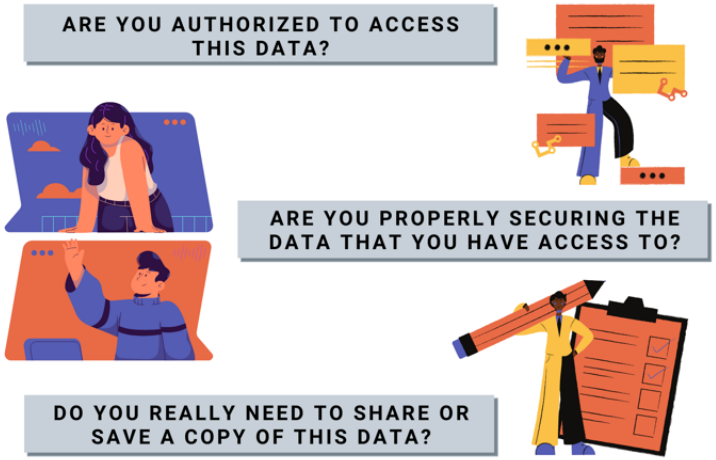
Key Vocabulary

Term	Definition
Malware	Software designed to harm a computer.
Phishing	Attempt to obtain sensitive information fraudulently.
Firewall	A system that blocks unauthorized access to a network.
Encryption	The process of converting data into a code to prevent unauthorized access.
Antivirus Software	Program that detects and removes malicious software.
Two-Factor Authentication (2FA)	Security process requiring two forms of identification.
Social Engineering	Manipulating people into giving away confidential information.
DoS Attack	Attempt to make a machine or network resource unavailable.
MitM Attack	Intercepting communication between two parties.
Confidentiality	Protecting information from unauthorized access.
Integrity	Ensuring the accuracy and trustworthiness of data.
Availability	Ensuring information is accessible when needed.



Cyber Security

- **Definition**: The practice of protecting systems, networks, and programs from digital attacks.
- **Objective**: To defend against threats to ensure the confidentiality, integrity, and availability of information.

Types of Threats

- **Malware**: Malicious software designed to damage or disable computers.
  - Examples: Viruses, worms, trojans, ransomware, spyware.
- **Phishing**: Fraudulent attempts to obtain sensitive information by disguising as a trustworthy entity.
- **Man-in-the-Middle (MitM) Attacks**: Eavesdropping on communication between two parties.
- **Denial-of-Service (DoS) Attacks**: Overloading a system to make it unavailable to users.
- **Social Engineering**: Manipulating individuals into divulging confidential information.

Important Cyber Security Practices

1. **Keep Software Updated**: Regularly update software to patch security vulnerabilities.
2. **Use Strong, Unique Passwords**: Create complex passwords and use different passwords for different accounts.
3. **Enable Two-Factor Authentication (2FA)**: Use 2FA for an added layer of security.
4. **Be Cautious with Emails**: Do not open attachments or click on links from unknown sources.
5. **Backup Data Regularly**: Ensure that important data is backed up to prevent loss.

Educate Yourself: Stay informed about the latest cyber threats and security practices

Cyber Security Measures

- **Firewalls**: Systems that monitor and control incoming and outgoing network traffic.
- **Antivirus Software**: Programs that detect and remove malware.
- **Encryption**: Encoding data to prevent unauthorized access.
- **Strong Passwords**: Using complex and unique passwords to secure accounts.
- **Two-Factor Authentication (2FA)**: Adding an extra layer of security beyond just passwords.

Data Protection

- **Confidentiality**: Ensuring that information is only accessible to those authorized to access it.
- **Integrity**: Maintaining the accuracy and reliability of data.
- **Availability**: Ensuring that information and resources are available when needed.

Useful Resources

- **StaySafeOnline**: staysafeonline.org - Tips and resources for staying safe online.
- **Cyber Aware**: cyberaware.gov.uk - UK government advice on cyber security.
- **Get Safe Online**: getsafeonline.org - Free advice on online safety.

Case Studies

Case Study 1: WannaCry Ransomware Attack (2017)

- **Description**: A global ransomware attack targeting computers running Microsoft Windows.
- **Impact**: Affected over 200,000 computers across 150 countries, causing significant damage to various organizations, including the NHS in the UK.
- **Lessons Learned**: Importance of regular updates and patch management, having up-to-date antivirus software, and ensuring proper data backups.

Case Study 2: Target Data Breach (2013)

- **Description**: Hackers gained access to Target's customer data, stealing credit and debit card information.
- **Impact**: Affected over 40 million credit and debit card accounts, resulting in financial loss and reputational damage.
- **Lessons Learned**: Importance of monitoring network activity, using secure systems for handling sensitive data, and promptly addressing vulnerabilities.

Summary

Understanding and implementing cyber security measures is crucial in today's digital age. By being aware of different types of threats and adopting best practices, individuals and organizations can protect themselves from cyber-attacks. Regular updates, strong passwords, and continuous education are key to maintaining a secure cyber environment.