**Question 1**

Computer Attack Incident Report

* 1. **Describe the attack:**

Recently, a ransomware attack targeted a small logistics company’s server. The attack was initiated through a phishing email containing a malicious attachment that, once opened by an employee, encrypted critical files on the network.

* 1. **What type of damage did the attack inflict?**

The ransomware attack resulted in significant data loss and system disruption. Key operational files were encrypted, rendering them inaccessible, which paralysed order processing and logistics planning for several days.

* 1. **List the reasons you think that the attack was successful:**

The attack succeeded due to several vulnerabilities:

* Lack of employee training on recognizing phishing emails.
* Outdated antivirus software that failed to detect the ransomware.
* Insufficient data backup procedures.
  1. **How was the computer fixed after the attack?**

Post-attack, the company isolated infected systems, removed the ransomware, and restored data from a recent offline backup.

They also updated antivirus software and conducted thorough employee training on cybersecurity best practices.

* 1. **What could have prevented the attack?**

To prevent such attacks in the future, implementing regular cybersecurity training for employees, maintaining up-to-date antivirus software, and establishing a robust data backup strategy are crucial measures.

* 1. **Why is information security important?**

Information security is vital as it protects sensitive data, preserves business continuity, and safeguards against financial losses and reputational damage. Implementing strong security measures ensures trust with customers and partners.

**Question 2**

Strengthening Passwords

1. **What is a weak password:**

A weak password is one that can be easily guessed or cracked by hackers. Examples include short passwords, passwords based on common words or phrases (e.g., “password123” or “123456”), or passwords that rely on personal information like birthdays or names.

1. **The dangers of weak passwords:**

Weak passwords expose users to significant risks, including unauthorized access to accounts, identity theft, and data breaches.

Hackers can exploit weak passwords to gain access to sensitive information, which can lead to financial losses or damage to personal or organizational reputations.

1. **What to consider to create strong passwords:**

Strong passwords should be at least 12-16 characters long and include a mix of uppercase and lowercase letters, numbers, and special characters. Avoid using easily guessable information like names or dates. Using random words or phrases that are not connected makes passwords harder to crack.

1. **Practical solutions for password protection:**

Password managers are an excellent tool for generating and storing complex passwords securely. Multi-factor authentication (MFA) provides an additional layer of protection by requiring a second form of verification, such as a code sent to your phone.

1. **Summary of findings from password testing tools:**

After testing several passwords using online tools like “How Secure Is My Password,” weak passwords like "password123" can be cracked in under a second, whereas a password like "T7@x!J1$Rk9#zQ" would take years to crack. These tools highlight how small changes significantly improve password security.

1. **Impact of password testing tools on password strength:**

Password testing tools are effective in educating users on the weaknesses of their current passwords. By visually demonstrating how easily weak passwords can be cracked, users are more motivated to create stronger, more secure passwords.

**Question 3**

Online Backup Services

1. **Comparison table of online backup services:**

| **Service** | **Features** | **Cost** |
| --- | --- | --- |
| **Backblaze** | Unlimited storage, automated backups, easy file restoration, file versioning | $7/month |
| **Carbonite** | Automatic backup, encrypted cloud storage, file recovery options | $6/month |
| **IDrive** | Multi-device backup, file syncing, 5GB free storage, encryption options | $59.62/year (5TB) |

1. **Importance of creating data backups:**

Regular data backups are crucial to protect against data loss due to hardware failure, cyberattacks, accidental deletion, or natural disasters. Backups ensure that critical data can be recovered quickly, minimizing downtime and potential financial or productivity losses.

1. **Recommendation of a backup service:**

Based on the research, I recommend Backblaze for its unlimited storage and ease of use. It offers robust backup features at an affordable price, making it ideal for both individuals and businesses. Its automated backup and file versioning capabilities ensure that users don’t lose important data.

**Question 4**

Cyber Safety Poster

**Cyber safety poster:**

To create the poster, list the following 10 tips clearly:

1. Use strong, unique passwords.
2. Enable multi-factor authentication.
3. Keep your software up to date.
4. Beware of phishing scams.
5. Don’t share personal information online.
6. Use a VPN on public WiFi.
7. Regularly backup important files.
8. Review privacy settings on social media.
9. Install and update antivirus software.
10. Log out of accounts when using shared computers.

**Explanation of cyber safety tips:**

1. Use strong, unique passwords**:**

A strong password can prevent unauthorized access to your accounts. Use combinations of characters and avoid reusing the same password across multiple sites.

1. Enable multi-factor authentication**:**

This adds an extra layer of security, requiring both a password and a code sent to your device to access an account.

1. Keep your software up to date:

Updates often contain security patches that protect against known vulnerabilities exploited by hackers.

1. Beware of phishing scams:

Phishing attempts can trick you into giving away personal information. Always verify the source before clicking links or downloading attachments.

1. Don’t share personal information online:

Avoid oversharing personal data on social media, as it can be used for identity theft or targeted attacks.

1. Use a VPN on public WiFi:

A VPN encrypts your internet connection, protecting your data from hackers when you’re using unsecured public WiFi networks.

1. Regularly backup important files:

Regular backups ensure that your data can be recovered if it’s lost due to an attack or system failure.

1. Review privacy settings on social media:

Make sure you’re not sharing more information than necessary and limit access to personal details to trusted contacts only.

1. Install and update antivirus software**:**

Antivirus software can detect and neutralize malware before it compromises your system.

1. Log out of accounts when using shared computers:

Always log out of accounts after use, especially on shared devices, to prevent unauthorized access.

**Question 5**

Public WiFi and QR Code Safety

1. Attacker's use of QR code for unauthorized information retrieval:

Attackers can embed malicious URLs in QR codes. When scanned, these codes can redirect users to phishing sites or download malware onto their devices. Users should only scan QR codes from trusted sources.

1. Information to avoid sending over public WiFi:

Sensitive information such as passwords, bank details, credit card numbers, and personal identification numbers should never be transmitted over unsecured public WiFi, as it can be intercepted by cybercriminals.

1. Precautions when connecting to public WiFi:

When using public WiFi, always connect to a secure network (use a VPN if possible), avoid accessing sensitive accounts like banking apps, and disable file sharing. Ensure that the WiFi network is legitimate and not a rogue access point set up by hackers.

1. Advantages and disadvantages of location tracking:

| **Advantages** | **Disadvantages** |
| --- | --- |
| Helps in navigation and finding nearby services. | Compromises privacy by revealing user’s location. |
| Can be used in emergencies to locate individuals. | Can be exploited for stalking or unauthorized tracking. |
| Supports targeted advertising based on location. | Allows companies to track user behaviour without consent. |
| Assists in location-based reminders and automation. | Drains mobile device battery faster. |
| Enables family and friends to track each other. | Data may be shared with third-party companies. |

**Question 6**

Digital Certificates and Secure Connections

* 1. What is a digital certificate?

A digital certificate is an electronic document that verifies the identity of a website or user by linking it to a cryptographic key pair. It is used in secure communication, such as SSL/TLS protocols, to ensure data transmission is encrypted and safe from tampering.

* 1. Browser's secure connection without HTTPS:

Modern browsers automatically attempt to establish secure connections (using HTTPS) when users access websites, even if “https://” is not explicitly typed in the URL. This is part of browsers’ efforts to promote internet security.

* 1. Advantages of secure browser connections:

Secure connections protect users by encrypting data in transit, preventing it from being intercepted by third parties. It ensures that sensitive information such as login credentials or financial details remain confidential.

* 1. Expiration date and issuer of digital certificates:

Digital certificates have expiration dates to ensure they are regularly updated. To view the expiration date and issuer, click on the padlock icon next to the URL in the browser and examine the certificate details. For example, a certificate might expire in 2025 and be issued by a trusted authority like DigiCert.