**Topic: Keeping Data Safe from Security Threats**

Reading Time: 20 mins

**·        Note\* Highlight important/core points while reading**

·        Read the content and write the answers given in the document in your words, to get the solid grip on topic.

**Keeping Data Safe from Security Threats**

With the rise of cyber threats, it is crucial to implement security measures to protect sensitive data. Various methods such as **access levels, anti-malware, authentication, passwords, biometrics, firewalls, proxy servers, and privacy settings** help keep data safe.

**1. Access Levels**

Access levels control **who can view or modify data** in a system. There are usually four levels:

1. **Public Access**: Data accessible by **anyone** (e.g., company websites).
2. **Friends**: Only people identified as ‘friends’ can see certain data (e.g., social media posts).
3. **Custom**: Allows **further refinement** of data visibility (e.g., hiding posts from certain friends).
4. **Data Owner**: Data only **visible to the owner** (e.g., personal financial records).

*Access levels ensure that sensitive data is only visible to the right people, reducing unauthorized access risks.*

**2. Anti-Malware Software**

Anti-malware protects against **viruses, spyware, and other malicious software**. It operates using two methods:

* **Rules-based detection**: Looks for common spyware traits.
* **File structure analysis**: Identifies file patterns linked to spyware.

**Features of anti-spyware software:**

* Detects and removes spyware.
* Blocks spyware downloads.
* Encrypts files to secure data.
* Encrypts keystrokes to prevent keylogging.
* Prevents unauthorized access to webcams and microphones.
* Warns users if personal data is stolen.

**3. Authentication**

Authentication verifies user identity before granting access. Common methods include:

1. **Something you know** – Passwords or PINs.
2. **Something you have** – Security tokens, mobile phones.
3. **Something unique to you** – Biometrics (fingerprint, retina scans).

Using **multi-factor authentication (MFA)** enhances security by requiring multiple verification factors.

**4. Passwords and Usernames**

Passwords secure access to **emails, online banking, shopping, and social media**.

* **Best practices for password security:**
* Use **strong passwords** (at least one capital letter, number, and special character).
* Change passwords **regularly**.
* Avoid using easy-to-guess passwords (e.g., pet names).
* Use **anti-spyware software** to prevent password theft.

Example of a **strong password**: Sy12@#TT90kj=0  
Example of a **weak password**: GREEN

**5. Biometrics**

Biometric authentication uses **unique physical traits** to verify identity. Examples include:

* **Fingerprint scans**
* **Retina scans**
* **Face recognition**
* **Voice recognition**

Biometrics **improve security** by making authentication **difficult to fake**.

**6. Checking Email Spelling, Tone, and URL Links**

* Check for **spelling and grammatical errors** in emails.
* **Legitimate companies** do not use generic email domains like @gmail.com.
* Watch for **urgent or aggressive tone**—scammers try to create urgency.
* Always **hover over links** to check the real URL before clicking.

Example of a scam email:

* Sent from: support@paypal-secure.com (fake domain)
* Subject: "URGENT: Your account will be suspended in 24 hours!"
* Misspelled words and incorrect grammar

**7. Firewalls**

A firewall is a **security system** that monitors and controls incoming/outgoing network traffic.

* Examines traffic between the user’s device and the internet.
* Blocks traffic that **does not meet security criteria**.
* Can prevent access to **undesirable websites**.
* Logs all network traffic for security audits.
* Helps prevent **viruses and hacking attempts**.

Firewalls act as **barriers**, filtering harmful content and blocking cyber threats.

**8. Proxy Servers**

A proxy server acts as an **intermediary** between a user and the internet.

* Filters internet traffic, blocking harmful sites.
* **Hides the user’s IP address** for anonymity.
* Prevents direct access to web servers.

Protects against hacking and **Denial-of-Service (DoS) attacks**.

**Caches web pages** to speed up browsing.

By **redirecting attacks away** from the user, proxy servers enhance security.

**9. Privacy Settings**

Privacy settings help control **what data is shared** online.

* **"Do Not Track" settings** prevent websites from collecting browsing data.
* Check **saved payment methods** to reduce financial risks.
* **Safe browsing alerts** warn about dangerous websites.
* Manage **cookie settings** to control data tracking.

**10. Secure Sockets Layer (SSL)**

SSL is an **encryption protocol** that secures online transactions.

* Used for **banking, shopping, emails, and social media**.
* Ensures that **data is encrypted** before transmission.
* Prevents **man-in-the-middle attacks**.
* Websites with SSL have a **padlock icon** and https:// in the URL.

Always ensure a website uses SSL before **entering sensitive information**.

|  |  |
| --- | --- |
| **Type** | **Description** |
| **Viruses** | Attach to legitimate files and spread when opened. |
| **Worms** | Self-replicating malware that spreads without user action. |
| **Trojan Horse** | Disguised as legitimate software but has a hidden malicious function. |
| **Spyware** | Secretly collects user data (e.g., keystrokes, login details). |
| **Adware** | Displays unwanted advertisements, often leading to malicious sites. |
| **Ransomware** | Encrypts user files and demands a ransom for decryption. |

* **Prevention:** Use **antivirus software**, avoid suspicious downloads, and enable **firewall protection**.

**6. Phishing**

* A cyberattack where hackers **trick users into giving personal information** (e.g., passwords, credit card details).
* Usually done via **fake emails or websites** pretending to be legitimate.
* Example: An email from “your bank” asking you to reset your password on a **fake website**.
* **Prevention:**
  + Verify sender emails before clicking links.
  + Never enter credentials on unknown websites.
  + Use **email spam filters**.

**7. Pharming**

* Redirects users from a legitimate website to a **fake, malicious website**.
* Users **unknowingly enter** login credentials on the fake site.
* Often used to **steal banking details**.
* **Prevention:**
  + Use **DNS protection software**.
  + Always check the URL before entering sensitive data.
  + Enable **multi-factor authentication (MFA)**.

**8. Social Engineering**

* Attackers manipulate people into **revealing confidential information**.
* Methods include:
  + **Pretexting**: Pretending to be a trusted person to get information.
  + **Baiting**: Offering something attractive (e.g., a free download) to trick users into installing malware.
  + **Tailgating**: Following someone into a restricted area without proper authentication.
* **Prevention:**
  + Always verify identities before sharing information.
  + Educate employees about security awareness.
  + Implement **access controls** for sensitive data.

**A-Rated Questions/Answers By Examiner**

**Q1: What are the four access levels for data security?**

**Answer:**

1. **Public Access** – Data is accessible to anyone.
2. **Friends** – Only people marked as ‘friends’ can see the data.
3. **Custom** – Users can limit what friends see.
4. **Data Owner** – Only the owner has access.

**Q2: How does a firewall protect a computer system?**

**Answer:** A firewall:

* **Filters traffic** between a computer and the internet.
* Blocks **suspicious data** that does not meet security criteria.
* Prevents access to **unsafe websites**.
* Logs network activity for security monitoring.
* Helps **prevent hacking and malware infections**.

**Q3: What are two common methods used by anti-malware software to detect threats?**

**Answer:**

1. **Rules-based detection** – Identifies malware by looking for common malicious traits.
2. **File structure analysis** – Recognizes malware based on suspicious file structures.

Anti-malware software detects, removes, and blocks spyware to **keep systems secure**.

**Q4: How can a user identify a phishing email?**

**Answer:**

* **Look for spelling and grammar mistakes**.
* **Check the sender’s email address**—legitimate companies use official domains.
* **Be cautious of urgent language**—scammers create a false sense of urgency.
* **Hover over links** to see the real URL before clicking.7

**Q5: What is Secure Sockets Layer (SSL), and why is it important?**

**Answer:**SSL is a **security protocol** that encrypts data during online transactions.

* Used for **banking, shopping, emails, and messaging**.
* Ensures **data is secure and private**.
* Prevents **data interception (man-in-the-middle attacks)**.

Websites using SSL have **a padlock symbol and ‘https://’ in the URL**.

### Write your Answers on your Notebook and Verify it on Next Screen

**Q6: How does multi-factor authentication (MFA) improve security?**

**Q7: Why is it important to use strong passwords, and how can users manage them effectively?**

**Q8: How do proxy servers help protect users online?**

**Q9: What are the benefits of using biometric authentication for security?**

**Q10: How do privacy settings help protect personal information online?**

**6. Answer:** MFA adds an extra layer of security by requiring multiple verification factors:

* **Something you know** (e.g., password, PIN).
* **Something you have** (e.g., security token, mobile device).
* **Something you are** (e.g., fingerprint, facial recognition).  
  **Benefit:** Even if a hacker steals a password, they cannot access an account without the additional authentication factor.

**7. Answer:** Weak passwords can be easily guessed or cracked, leading to unauthorized access.  
**Best Practices:**

* Use complex passwords with uppercase, lowercase, numbers, and symbols.
* Avoid using personal information like birthdates or names.
* Use a password manager to securely store and generate strong passwords.

**8. Answer:** Proxy servers act as intermediaries between users and the internet. They:

* Hide IP addresses for anonymity.
* Block access to harmful or restricted websites.
* Filter and inspect traffic to prevent cyber threats.
* Improve performance by caching frequently visited web pages.

**9. Answer:** Biometric authentication improves security by using unique physical traits that are difficult to duplicate.  
**Examples:**

* **Fingerprint scanners** (used in smartphones and laptops).
* **Facial recognition** (used for secure logins).
* **Retina scans** (used in high-security environments).  
  **Advantage:** Unlike passwords, biometric data cannot be easily stolen or guessed.

**10. Answer:** Privacy settings control what data is shared and who can access it.  
**Key Features:**

* "Do Not Track" settings limit website tracking.
* Managing cookie settings prevents excessive data collection.
* Restricting profile visibility protects personal information on social media.
* Reviewing saved payment methods reduces financial risks.