Session 1 Assignment

Cybersecurity Awareness Best Practices:

1-Password Management:

1. Use Strong, Unique Passwords:- password should be at least 12 characters long and include a mix of uppercase letters, lowercase letters, numbers, and special characters.(Avoid information like names, birthdays).

2. Enable Multi Factor Authentication:- MFA adds an extra layer of security by requiring a second verification step, like a code sent to your phone or an app.

3. Use a Password Manager:- A password manager securely stores and encrypts all your passwords. reducing the need to rely on memory or write passwords down.

4. Avoid Reusing Password:- If one account is compromised, attackers can potentially access other accounts with the same credentials.

5. Change Passwords Regularly:- Regular password changes can limit exposure if credentials are compromised without your knowledge**.**

2- Email Security:-

1. Recognize and Avoid Phishing Attempts:- Always verify the sender's email address, avoid clicking on suspicious links.

2. Verify the Authenticity of Links and Attachments:- Hover over links to preview the URL before clicking. Malicious links may resemble legitimate websites but with slight alterations in spelling or domain.

3- Downloads:- Only download attachments from trusted sources.

4. Report Suspicious Emails Immediately:- reporting can help prevent the spread of phishing attacks and protect sensitive data.

5. Avoid Sharing Sensitive Information Over Email:- passwords, credit card details, or personally identifiable information, over email.

3-Software Updates:-

1. Regularly Update All Software and Systems:- Software updates often contain security patches that address newly discovered vulnerabilities.

2. Enable Automatic Updates When Possible:- Enabling automatic updates ensures that devices receive critical patches as soon as they are available. This reduces the chances of missing updates due to forgetfulness or oversight.

3. Use Trusted Sources for Software and Updates:- Only download software and updates from official sources or reputable vendors.

4. Monitor for End-of-Life (EOL) Software:- Vendors eventually stop supporting older software versions. EOL software no longer receives updates or security patches, making it a significant security risk.

5. Educate and Remind Users of the Importance of Updates:- Encourage users to view updates as essential for security, not as an inconvenience.

4-Social Engineering:-

1. Educate About Common Social Engineering Tactics:- Social engineering involves manipulating individuals into disclosing sensitive information. Educate users on tactics like phishing (deceptive emails), pretexting (fabricating a scenario to extract information), baiting (luring victims with fake promises), and tailgating (following someone into a restricted area).

2. Verify Identities Before Sharing Information:- Always verify the identity of someone requesting sensitive information, especially if the request is unexpected or involves confidential data.

3. Limit Information Sharing on Social Media:- Social engineers often gather details from social media to build a convincing pretext

4. Implement Strong Access Controls:- Enforce access controls, such as badge or keycard systems, to prevent unauthorized individuals from entering secure areas

5. Encourage Reporting of Suspicious Behavior:- Foster a culture of security awareness where employees feel comfortable reporting suspicious emails, phone calls, or in-person interactions.

5-Data Privacy:-

1. Understand Data Privacy Laws and Regulations:- Be aware of relevant data protection laws that apply to your organization or personal data. Regularly review and update policies to remain compliant with current data privacy regulations.

2. Encrypt Sensitive Data:- Use encryption for sensitive data, both at rest and in transit. This ensures that even if data is intercepted, it remains unreadable without the correct decryption key.

3. Limit Data Collection and Access:-Only collect and retain the data that is necessary for operations. Restrict access to sensitive data to only those who need it for their roles.

4. Educate Employees and Stakeholders:- Regularly conduct cybersecurity awareness training for all employees. Encourage a security-first mindset to ensure everyone understands the importance of data privacy.

5. Conduct Regular Security Audits and Assessments:- Regularly assess your organization’s security practices and privacy measures. Use audits to identify vulnerabilities and areas for improvement.