QUIZ

Question 1:

Scenario: An employee at Suraksha Rakshakah receives an email claiming to be from their bank, asking for personal information. What type of threat is this?

Options:

A. Malware

B. Phishing

C. Firewall

D. Encryption

Correct Answer: B. Phishing

Question 2:

Scenario: Suraksha Rakshakah has suffered a data breach, and sensitive customer information was exposed. What regulation might require the company to report this incident to affected individuals and authorities?

Options:

A. HIPAA

B. PCI DSS

C. GDPR

D. CCPA

Correct Answer: C. GDPR

Question 3:

Scenario: An employee's laptop at Suraksha Rakshakah was stolen. What data protection measure would have been most effective in this situation?

Options:

A. Data in transit encryption

B. Data at rest encryption

C. Multi-Factor Authentication (MFA)

D. Firewall

Correct Answer: B. Data at rest encryption

Question 4:

Scenario: You, as the cybersecurity officer at Suraksha Rakshakah, receive a message on your social media account from an unknown person with a link to a suspicious website. What should you do?

Options:

A. Click the link to see what it's about.

B. Ignore the message.

C. Report the message as spam or suspicious.

D. Reply with your personal information to learn more.

Correct Answer: C. Report the message as spam or suspicious.

Question 5:

Scenario: Suraksha Rakshakah has detected a sudden increase in network traffic, potentially indicating a cyber attack. What type of network threat might this be?

Options:

A. Phishing

B. DoS (Denial of Service)

C. Ransomware

D. Firewall breach

Correct Answer: B. DoS (Denial of Service)

Question 6:

Scenario: An employee's smartphone at Suraksha Rakshakah has facial recognition and fingerprint scanning enabled for unlocking. What authentication methods are being used?

Options:

A. Multi-Factor Authentication (MFA)

B. Token-Based Authentication

C. Biometric Authentication

D. Password-Based Authentication

Correct Answer: C. Biometric Authentication

Question 7:

Scenario: During a security awareness training session at Suraksha Rakshakah, an employee is asked to define "phishing." What is the correct definition?

Options:

A. A type of malware that encrypts files and demands a ransom.

B. An attempt to deceive individuals into revealing sensitive information by impersonating a trustworthy entity.

C. The act of gaining unauthorized access to a computer system.

D. A type of firewall designed to block malicious websites.

Correct Answer: B. An attempt to deceive individuals into revealing sensitive information by impersonating a trustworthy entity.

Question 8:

Scenario: You, as the cybersecurity officer at Suraksha Rakshakah, receive an email from a coworker with a link to a shared document. However, you find the email suspicious. What should you do?

Options:

A. Click the link and open the document.

B. Forward the email to your entire department.

C. Verify with your coworker through a different communication channel if they sent the email.

D. Delete the email without taking any action.

Correct Answer: C. Verify with your coworker through a different communication channel if they sent the email.

Question 9:

Scenario: Suraksha Rakshakah stores medical records for patients. What regulation is most relevant to protecting the privacy and security of this data?

Options:

A. CCPA

B. PCI DSS

C. GDPR

D. HIPAA

Correct Answer: D. HIPAA

Question 10:

Scenario: Suraksha Rakshakah's network experiences a sudden surge in traffic, causing system slowdowns and disruptions. Employees report that they are unable to access critical resources. As the cybersecurity officer, what type of cyber threat should you suspect, and what immediate action should you take?

Options:

A. Suspect a malware attack and immediately disconnect affected devices from the network.

B. Suspect a phishing attempt and inform all employees to change their passwords.

C. Suspect a Distributed Denial of Service (DDoS) attack and collaborate with your Internet Service Provider (ISP) to mitigate it.

D. Suspect a firewall breach and initiate a system-wide lockdown.

Correct Answer: C. Suspect a Distributed Denial of Service (DDoS) attack and collaborate with your Internet Service Provider (ISP) to mitigate it.