Strengthening Office Cybersecurity

Part 1: Office Roleplay Dialogue

Scenario: An IT Technician, James, meets with the office supervisor, Karen, to discuss recent cybersecurity issues affecting employees, such as malware infections, phishing attempts, and unauthorized network access.

Karen: Hi James, I wanted to check in about the cybersecurity issues we've been facing. Some employees reported strange pop-ups on their computers, and a few received suspicious emails asking for login details.

James: Hi Karen, thanks for letting me know. It sounds like we may have both **malware infections** and **phishing** attempts happening at the same time.

Karen: That's what I was worried about. What can we do to prevent this?

James: First, I'll run a full **antivirus** scan on all company computers to detect and remove any malware. Our antivirus software should be able to quarantine infected files.

Karen: That's good to hear. What about the phishing emails? A few employees almost entered their passwords on a fake login page.

James: That's a serious risk. I recommend enabling **Two-Factor Authentication (2FA)** for all employee accounts. With 2FA, even if someone's password is stolen, hackers still need a second verification step, like a mobile code, to log in.

Karen: That makes sense. We've also had some employees report slow internet speeds, and I'm worried that someone unauthorized might be accessing our network.

James: That's possible. I'll check our **firewall** settings to ensure only authorized users and devices can connect. A firewall helps block unauthorized access and monitors incoming and outgoing traffic for potential threats.

Karen: I see. Is there anything else we should be concerned about?

James: Yes, we also need to stay aware of **zero-day exploits**. These are vulnerabilities in software that hackers discover before the software company has a fix. We should always apply security patches and updates as soon as they're released.

Karen: I'll remind employees to keep their software updated. What about sensitive company data? How can we protect it?

James: We should use **encryption** for important files and emails. Encryption ensures that even if someone intercepts the data, they won't be able to read it without the correct decryption key.

Karen: That sounds like a great idea. Thanks for handling all of this, James!

James: No problem, Karen. I'll send out a security reminder to all employees and update our cybersecurity settings. Let me know if you notice anything else!

Part 2: Comprehension Questions

1. How does James plan to handle the malware infections?

(A) By deleting all suspicious files manually

(B) By replacing all office computers

(C) By running a full antivirus scan

(D) By changing employee email passwords

2. What is the purpose of Two-Factor Authentication (2FA)?

(A) To speed up internet connections

(B) To require an extra security step when logging in

(C) To block all emails from unknown senders

(D) To prevent software updates from installing

3. What does a firewall do?

(A) It blocks unauthorized access and monitors network traffic

(B) It cleans the computer's hard drive

(C) It automatically deletes phishing emails

(D) It improves Wi-Fi speed

4. What is a zero-day exploit?

(A) A type of firewall software

(B) A cybersecurity vulnerability that hackers discover before it is fixed

(C) A way to increase encryption strength

(D) A method for blocking antivirus scans

Part 3: Key Vocabulary Definitions in Japanese

1. **Firewall (ファイアウォール)** – ネットワークを保護し、不正アクセスや攻撃をブロックするセキュリティシステム。

2. **Antivirus (アンチウイルスソフトウェア)** – マルウェアやウイルスを検出し、削除するためのソフトウェア。
3. **Two-Factor Authentication (2FA) (二要素認証)** – パスワードに加えて、モバイルコードなどの追加認証を必要とするセキュリティ対策。
4. **Zero-Day Exploit (ゼロデイ脆弱性攻撃)** – ソフトウェアの未知のセキュリティホールを悪用する攻撃。
5. **Encryption (暗号化)** – データを暗号化して、正しい復号キーを持つ人だけが内容を読めるようにする技術。

Part 3: Answers

1. How does James plan to handle the malware infections?

✅ (C) By running a full antivirus scan

2. What is the purpose of Two-Factor Authentication (2FA)?

✅ (B) To require an extra security step when logging in

3. What does a firewall do?

✅ (A) It blocks unauthorized access and monitors network traffic

4. What is a zero-day exploit?

✅ (B) A cybersecurity vulnerability that hackers discover before it is fixed