IT Training & Security Awareness for New Employees

Part 1: Office Roleplay Dialogue

Scenario: An IT Technician, Michael, is training a new employee, Anna, on IT policies, security awareness, and company systems.

Anna: Hi Michael, thanks for setting up this training session. I want to make sure I follow all IT policies correctly.

Michael: No problem, Anna! Let's start with our **knowledge base**. It's an internal system where you can find IT guides, FAQs, and troubleshooting steps. If you ever run into technical issues, this should be your first stop.

Anna: That's really useful! But what if I can't find a solution?

Michael: In that case, you can submit a request using our **help desk ticketing** system. This allows IT to track and respond to support requests efficiently.

Anna: Got it! I'll check the knowledge base first, and if I still need help, I'll submit a ticket.

Michael: Exactly. Now, let's talk about security. We conduct **phishing simulations** to train employees on how to recognize fake emails that try to steal login credentials. If you receive a suspicious email, don't click any links—report it to IT instead.

Anna: That's a great idea! I've heard that phishing attacks are really common.

Michael: Yes, they are. That's why we also require **security awareness training** for all employees. This covers safe password practices, recognizing scams, and securing company data.

Anna: Makes sense! What about system access? Are there any restrictions on what I can do?

Michael: Yes, we follow a strict **user permissions** policy. Employees only have access to the files and systems necessary for their roles. This helps prevent unauthorized access to sensitive data.

Anna: That's reassuring. Thanks for the training, Michael!

Michael: You're welcome, Anna! Let me know if you have any questions.

Part 2: Comprehension Questions

1. What is a knowledge base used for?
(A) Resetting employee passwords
(B) Installing new software
(C) Blocking spam emails
(D) Storing IT guides and troubleshooting information

2. What is the purpose of phishing simulations?
(A) To train employees on how to recognize and avoid fake emails
(B) To upgrade company software
(C) To speed up internet connections
(D) To prevent computer overheating

3. How does the help desk ticketing system assist employees?
(A) It automatically fixes computer issues

(B) It improves Wi-Fi speed

(C) It blocks malware from being installed

(D) It allows employees to track and submit IT support requests

4. What do user permissions control?

(A) The speed of a computer

(B) The number of hours an employee can work

(C) What files and systems an employee can access

(D) The amount of storage on an employee's device

Part 3: Key Vocabulary Definitions in Japanese

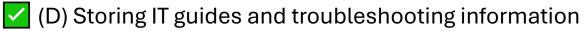1. **Knowledge Base (ナレッジベース)** – IT 関連のガイド、FAQ、トラブルシューティング情報をまとめた社内システム。

2. **Phishing Simulation (フィッシングシミュレーション)** – 従業員がフィッシング詐欺を見分けられるように訓練する模擬攻撃テスト。

3. **User Permissions (ユーザー権限)** – 従業員がアクセスできるデータやシステムを制限する設定。

4. **Help Desk Ticketing (ヘルプデスクチケッティング)** – IT サポートのリクエストを管理・追跡するシステム。

5. **Security Awareness Training (セキュリティ意識向上トレーニング)** – パスワード管理やサイバー脅威対策を学ぶための企業向けセキュリティ研修。

Part 4: Questions & Correct Answers

1. **What is a knowledge base used for?**
   ✅ (D) Storing IT guides and troubleshooting information

2. **What is the purpose of phishing simulations?**
   ✅ (A) To train employees on how to recognize and avoid fake emails

3. **How does the help desk ticketing system assist employees?**
   ✅ (D) It allows employees to track and submit IT support requests

4. **What do user permissions control?**
   ✅ (C) What files and systems an employee can access