

# Employee Cyber Hygiene Self-Assessment Questionnaire

## 1. Password & Access Management

**Do you use unique passwords for different accounts (work and personal)?**

No (0)

I reuse passwords across many accounts (1)

I use different passwords but sometimes reuse old ones (2)

I use different passwords and change them occasionally (3)

I use different, strong passwords and a password manager (4)

**Do you store your passwords securely?**

No, I write them down or save them in unprotected files (0)

I use a simple password-protected document (1)

I memorize most but reuse some weak passwords (2)

I use a password manager but sometimes write down passwords (3)

I exclusively use a password manager or secure method (4)

**Do you use multi-factor authentication (MFA) when available?**

No (0)

Only for highly sensitive accounts (1)

I enable MFA for some work accounts (2)

I enable MFA for most work accounts (3)

I enable MFA for all possible accounts (4)

**Do you lock your computer and devices when leaving them unattended?**

No (0)

Sometimes, but I often forget (1)

I lock them when in public spaces (2)

I lock them in most situations (3)

I always lock them, even at home (4)

---

## 2. Phishing Awareness & Email Security

**Would you recognize a phishing email?**

No, I am not familiar with phishing attacks (0)

I have heard of phishing but wouldn't always recognize it (1)

I recognize some phishing attempts but have fallen for them before (2)

I can recognize most phishing emails and verify links before clicking (3)

I always verify sender details, URLs, and report phishing attempts (4)

**Have you received cybersecurity training on phishing attacks?**

- No (0)
- Once, but I do not remember much (1)
- Occasionally, but not regularly (2)
- I receive training at least once a year (3)
- I regularly receive training and participate in phishing tests (4)

**Do you verify sender addresses before clicking on links or opening attachments?**

- Never (0)
- Rarely (1)
- Sometimes, if an email looks suspicious (2)
- Often, but I have clicked on a suspicious link before (3)
- Always, I verify senders and links before clicking (4)

**Do you report suspicious emails to IT/security?**

- No (0)
  - I delete them but don't report them (1)
  - I report some emails but not consistently (2)
  - I usually report them (3)
  - I always report phishing attempts (4)
- 

### **3. Device & Data Security**

**Do you regularly update your work device (OS, apps, security patches)?**

- No, I ignore updates (0)
- Sometimes, but I delay updates (1)
- I update most things within a few weeks (2)
- I update devices promptly when notified (3)
- I always update immediately or have auto-updates enabled (4)

**Do you use personal USB drives or unauthorized software on work devices?**

- Yes, regularly (0)
- Sometimes, if necessary (1)
- Rarely, only when required (2)
- Almost never, and only after IT approval (3)
- Never, I follow IT policies strictly (4)

**Do you use encrypted communication channels for sensitive work discussions?**

- No (0)
  - Sometimes, but not always (1)
  - I use encrypted channels when instructed (2)
  - I use them for most sensitive communications (3)
  - I always use encrypted channels (4)
- 

### **4. Remote Work & Public Network Security**

**Do you use a VPN or secured connection when working remotely?**

- No (0)
- Only for highly sensitive work (1)
- Sometimes, but not consistently (2)
- Mostly, unless I forget (3)
- Always, I never work remotely without a VPN (4)

**Do you avoid using public Wi-Fi for work tasks?**

- No, I use public Wi-Fi without precautions (0)
- Sometimes, but I don't take security measures (1)
- I use public Wi-Fi but with some security precautions (2)
- I avoid public Wi-Fi when possible (3)
- I never use public Wi-Fi for work tasks (4)

**Do you ensure that family members or friends do not use your work devices?**

- No, I share my work device (0)
  - Sometimes, but only for non-work purposes (1)
  - Rarely, but they have accessed it before (2)
  - Almost never, except in emergencies (3)
  - Never, I strictly keep work devices private (4)
- 

## **5. Incident Reporting & Cybersecurity Culture**

**Do you know how to report a cybersecurity incident?**

- No (0)
- I think I know, but I'm not sure (1)
- I know where to report but have never done it (2)
- I know how to report and have done it before (3)
- I actively report security incidents and encourage others to do so (4)

**Do you feel your organization provides adequate cybersecurity training?**

- No, I have never received training (0)
- Some training, but not enough (1)
- Training is provided, but it could be better (2)
- Training is good, but I'd like more practical exercises (3)
- Training is excellent and prepares me well for threats (4)

**Would you feel comfortable reporting a mistake or security issue to IT/security?**

- No, I am afraid of consequences (0)
- I am unsure if I should report mistakes (1)
- I would report it, but I worry about judgment (2)
- I would report it without hesitation (3)
- I feel encouraged to report mistakes for learning purposes (4)