

Cybersecurity Awareness & Training Program 2025

Contents

1. Defining Goals:.....	2
2. Defining Scope:.....	2
3. Defining Targeted Audience:	2
4. Defining Validation Criteria:	2
5. Cybersecurity Awareness & Training Program Content.....	3
6. Program Implementation	4
7. Review and Update	4

Version	Adjustment Date	Approved By	Approval Date and signature
2.0	25-5-2025	Saud Alsulami	28-5-2025



1. Defining Goals:

- Increase employee awareness of cybersecurity risks and potential threats.
- Equip employees with the necessary knowledge and skills to protect the assets and information.
- Change unsafe behaviors and promote good security practices.
- Ensure employee compliance with the cybersecurity policies and procedures.
- Reduce the likelihood of security incidents resulting from human error.

2. Defining Scope:

- The program will cover all employees of Taqnyat, with the possibility of customizing training content based on their roles and responsibilities.
- The program will focus on the practical and applied aspects of cybersecurity in the daily work environment.
- The program content will be updated yearly to keep pace with the latest threats and security developments.

3. Defining Targeted Audience:

- All employees of Taqnyat (including senior management, permanent and temporary staff, and contractors).
- The audience can be divided into subgroups based on their roles and level of access to sensitive systems and information for training customization.

4. Defining Validation Criteria:

- Conduct surveys to gather participant feedback and improve the program.
- Monitor and evaluate changes in employee behavior and security practices (e.g., reporting phishing attempts).
- Measure compliance with cybersecurity policies
- Assess the decrease in the number of security incidents resulting from human error over time.



5. Cybersecurity Awareness & Training Program Content

5.1. Cybersecurity Roles and Responsibilities of the Targeted Audience:

- Clarify each employee's responsibility in maintaining the security of the Taqnyat's information.
- Explain how to identify and report potential security threats.
- Emphasize the importance of adhering to cybersecurity policies and procedures.
- Clarify the potential consequences of non-compliance with security procedures.
- Encourage a culture of security responsibility among all employees.

5.2. Trending Cybersecurity Events and Threats:

- Explain the concept of social engineering and its various types (e.g., phishing, phone scams, impersonation).
- Provide real-world examples of recent cybersecurity events and threats.
- Explain how phone scams and impersonation call work and how to identify them.
- Provide advice on how to handle suspicious messages and calls and avoid becoming a victim.
- Raise employee awareness of the latest tactics used by attackers

5.3. Advice to Personnel Not to Attempt Unauthorized Activities:

- Explanation of the official procedures for requesting any new program, ensuring that no individual permissions are granted for installing or using any non-approved programs
- Explain the procedures for requesting and authorizing the transfer of equipment between different locations.
- Emphasize that any attempt to bypass security controls is a violation of policies.

5.4. Secure Handling of Portable Devices and Storage Media, Email Services, Internet Surfing Services and Social Media:

- Secure portable devices with strong passwords, fingerprints, or facial recognition.
- Avoid storing sensitive information on unencrypted external storage media.
- Be cautious when connecting portable devices to public and unsecured Wi-Fi networks.
- Recognize the signs of spam and phishing emails (e.g., suspicious links, spelling and grammatical errors, unusual requests).



- Do not open emails or attachments from unknown or suspicious sources.
- Be cautious when clicking on links or downloading attachments in emails.
- Carefully verify the sender's email address.
- Avoid visiting suspicious or untrusted websites.
- Be cautious about the information shared on social media.
- Avoid sharing sensitive or work-related information on public platforms.
- Be wary of suspicious links and requests received through social media.
- Secure social media accounts with strong passwords and enable two-factor authentication.

5.5. Clear Desk and Clear Screen Policy

- All sensitive documents and information must be stored in secure locations (such as locked cabinets or drawers) when not in use or after work is completed.
- Documents that are no longer needed must be securely disposed of (e.g., shredding).
- Sensitive documents or confidential information should not be left exposed on desks.
- Computer screens and terminals must be locked when leaving the desk or when not in use for a short period.
- Avoid leaving computers or terminals running unattended.

6. Program Implementation

Given Taqnyat Company's commitment to cybersecurity as an ongoing process, the training and awareness program is designed to be continuous. Annual awareness sessions are conducted for all employees, and training and awareness sessions are organized as needed for each department in coordination with their respective management.

7. Review and Update

- Review the program annually
- Update the program content based on changes in security threats
- Collect employee feedback and use it to improve the program.
- Continuously measure the program's impact on security awareness and employee behavior.

