Organization Logo (Optional)

Employee Awareness Training Plan

Organization Name

Date

Created by: CYBERSAFE SQUAD

**** CYBERSAFE SQUAD HAS DEVELOPED THIS FILLABLE TEMPLATE AS PART OF THE CYBERSECURE BLUEPRINT PROCESS FOR EDUCATIONAL PURPOSES ONLY. THIS TEMPLATE IS INTENDED TO PROVIDE GUIDANCE ON HOW TO ORGANIZE AND DOCUMENT INFORMATION FOR LOG MANAGEMENT POLICIES. PLEASE NOTE THAT THE USE OF THIS TEMPLATE DOES NOT GUARANTEE SUCCESSFUL CERTIFICATION OR COMPLIANCE WITH ANY REGULATORY REQUIREMENTS. ORGANIZATIONS ARE NOT OBLIGATED TO USE THIS TEMPLATE AND MAY CHOOSE TO PROVIDE CERTIFICATION REQUIREMENTS IN A FORMAT THAT BEST SUITS THEIR NEEDS AND REQUIREMENTS. ****

Index

Instructions for Using the Template

- This template is designed to assist users in meeting the certification requirements for the CyberSecure Blueprint security control area of Provide Employee Awareness Training. The purpose of this template is to provide a clear outline and guide users in creating an effective employee awareness training plan.
- To ensure a comprehensive understanding of the training requirements, it is recommended that users review the eLearning module for the Provide Employee Awareness Training and study the completed example of this plan. Both resources can be used as references to aid in the creation of an effective training plan.
- Please note that the instructions provided within each section of this template are highlighted in red font. It is important to carefully read and follow these instructions in order to meet the certification requirements.
- Upon completion of the template, users should delete the instructions and ensure that the plan is clear, concise, and relevant to their organization's needs. We encourage all users to prioritize the creation of an effective employee awareness training plan as it is essential in protecting against cyber threats and ensuring the overall security of their organization.

Plan to follow

The following items constitute the framework for an organization's employee awareness training program:

- policies for employee awareness training that define the mandatory and role-specific training requirements and the frequency of training;
- a record of employee awareness training that tracks the type of training and when it was scheduled or completed;
- an outline of employee awareness training that includes ice breakers, specific topics to be covered, and other relevant activities, which can be used to standardize training across the organization;
- employee awareness training materials that are provided during the training sessions and intended to support the learning and retention of critical concepts.

Strategy on employee education and awareness

Date	Version	Modification	Modifier
[Date edited]	[Document version]	[Description of changes made]	[Name of the editor]

Policy Statements

The aim of this policy is to offer comprehensive cyber security training to all employees of [Organization Name], covering both scheduled and mandatory sessions as well as role-specific training. The scope of this policy encompasses all guidelines and policies related to cyber security. The goal is to ensure that employees are well-versed in cyber security best practices, reducing the organization's risk of cyber-attacks and protecting sensitive data.

Scheduled training

The [Organization Name] has planned [Frequency] sessions of employee training to cover various aspects such as policies, provisions, and other relevant elements that require training. In order to ensure that employees are well-informed, an employee awareness training record will be created, maintained, and regularly updated to reflect any modifications, updates, or rescheduled training.

Mandatory trainings

All personnel employed at [Organization Name] are required to complete the following training program:

- Establishing passwords that are safe and secure
- Practicing safe internet and social media usage
- Utilizing solely authorized software and applications on company devices
- Recognizing harmful links and fraudulent emails (phishing)

Role dependant training

It is mandatory for personnel occupying the designated positions within [Organization Name] to complete the prescribed training.

Role	Training	Frequency
[Type of role]	[What type of training]	[What Frequency]

Enforcement

As an organization, it is incumbent upon us to identify the instances where mandatory and job-specific training is warranted for our workforce, and ensure that such training is provided to the relevant employees.

Training Record

Role	Training	Topics	Scheduled	Staff	Completed	Date of completion

Outline of the Training

To educate employees on how to identify and prevent cybersecurity threats in the workplace.

Duration: 1 hour

I. Introduction (5 minutes)

- Welcome and overview of the training
- Importance of cybersecurity awareness

II. Cybersecurity Threats (15 minutes)

- Overview of common cybersecurity threats (e.g. phishing, malware, social engineering)
- Real-life examples of cyber attacks

III. Best Practices for Cybersecurity (30 minutes)

- Password management and best practices for creating strong passwords
- Safe browsing and email practices
- Avoiding suspicious links and attachments
- Reporting suspicious activity

IV. Company Policies and Procedures (5 minutes)

- Overview of company policies and procedures related to cybersecurity
- Consequences of violating company policies

V. Q&A and Evaluation (5 minutes)

- Opportunity for employees to ask questions and clarify any confusion
- Brief evaluation of the training

VI. Conclusion (5 minutes)

- Recap of key points covered in the training
- Emphasis on the importance of cybersecurity awareness and how it contributes to a secure work environment.

*To ensure effective communication and engagement, it is recommended that a structured approach be employed when delivering topics. The approach should involve an initial explanation of each topic, which should take no more than 5 minutes. This should be followed by an activity that lasts for approximately 10 minutes, aimed at allowing participants to actively engage with the topic. Finally, a debriefing session should be held for 5 minutes, aimed at allowing participants to reflect on their experiences during the activity and further enhance their understanding of the topic. This approach should be repeated for each topic in the sequence before proceeding to the next. Employing such a structured approach will not only help ensure that each topic is thoroughly covered but also increase participant engagement and retention of information.

Employee awareness training topics

- Use of effective password: This topic would cover best practices for creating strong passwords, such as using a mix of letters, numbers, and symbols, avoiding common words or phrases, and changing passwords regularly. It may also cover the risks associated with reusing passwords across multiple accounts.
- Use passcodes or pins: Similar to password best practices, this topic would cover guidelines for creating strong passcodes or pins and avoiding common patterns or easily guessable numbers.
- Use two-factor authentication: This topic would explain what two-factor authentication is and why it's important for security. It would also cover how to set up and use two-factor authentication for various accounts and services.
- Identification of malicious emails and links: This topic would cover how to recognize signs of phishing attempts, such as suspicious senders or requests for personal information. It may also include tips for avoiding phishing links and how to report suspected phishing attempts.
- Phishing emails: This topic would go into more detail about the different types of phishing attempts and how to recognize them. It may also cover what to do if you accidentally click on a phishing link or provide sensitive information.
- What makes spear phishing so effective?: This topic would explain how spear phishing differs from other types of phishing and why it can be more difficult to detect. It may also cover strategies for identifying and avoiding spear phishing attempts.
- Use of approved software: This topic would cover guidelines for installing and using approved software on work devices. It may also include policies around using personal devices for work-related tasks and how to report potential security issues with software.
- Safe use of social media: This topic would cover best practices for using social media safely, such as avoiding oversharing personal information and recognizing fake profiles or accounts. It may also cover policies around using social media at work and the risks associated with using social media on work devices.

As part of our organization's commitment to maintaining the confidentiality and integrity of our sensitive information, it is important that all employees receive training on data privacy and protection, cybersecurity best practices, physical security, incident response, and social engineering awareness. Please see below for a summary of each topic:

- Data privacy and protection:
  - It is crucial to identify and safeguard sensitive information to ensure its confidentiality and integrity.
  - Access controls and encryption measures should be applied to secure data appropriately.

Cybersecurity best practices:

- Deploying firewalls and anti-virus software is necessary to prevent and detect malicious activity.
- Public Wi-Fi networks should be avoided, and secure authentication protocols should be implemented.

Physical security:

- Proper storage and disposal practices must be followed to secure physical devices and documents.
- All employees must be vigilant in identifying and reporting suspicious behavior or potential security threats.

Incident response:

- All security incidents must be reported promptly and in accordance with established incident response procedures.
- In the event of a security breach, it is crucial to minimize damage and restore systems and data to their normal functioning state.

Social engineering:

- Employees must be trained to recognize and respond to social engineering tactics, such as pretexting and baiting, which are used to manipulate individuals into divulging sensitive information or performing actions that compromise security.

Spear Phishing: Understanding the Risks and Mitigating Them

Spear phishing is a highly effective and dangerous form of cyber attack that can compromise an organization's security. The following points outline the factors that make spear phishing so effective, and provide guidance on how organizations can mitigate the risk of attack:

Factors that make spear phishing effective:

- Spear phishing emails often contain branding and logos of legitimate organizations, making them appear authentic and trustworthy.
- Malicious software can be contained in files that look legitimate, such as PDFs or images.
- Subject lines are often crafted to be relevant and compelling, encouraging trust and prompting the recipient to take action.

Guidance to mitigate the risk of spear phishing:

- Employee awareness training is an important part of any cybersecurity program. Employees should be trained to identify phishing and spear phishing emails and links.
- Employees should be able to identify legitimate links from phishing links, which is crucial for navigating the internet safely at work. Hovering the mouse over the link without clicking it will show the whole URL.
- Fraudulent links often do not match the domain name of the sender, contain misspelled domain names from common brands, or contain extra terms.
- Spear phishing emails can contain attachments that when opened, can infect the network with viruses, including ransomware. Employees should never open an attachment they were not expecting and should compose a separate email to the sender to ask if the attachment is legitimate.
- Organizations must develop clear policies for safe internet use at work and communicate those policies to employees before they participate in cybersecurity training.
- Policies may include prohibitions on criminal activity online, instigating or propagating malware or viruses, downloading software without permission, sharing credentials without authorization, and connecting to the dark web or other inappropriate sites.
- Employees should be trained on the safe use of social media, including applying all possible security steps to accounts, using good judgment when accessing unknown websites or accounts, and avoiding sharing unnecessary personal information on company social media feeds.
- Social media can contain malware hidden on seemingly harmless links, and sharing personal information can make it easy for threat actors to compromise accounts. A good training exercise is to ask participants to audit their own social media accounts to see if they comply with best practices.

Using approved software:

- A recommended activity for this lesson is to present a list of software applications and ask participants to determine if they are authorized for use.
- Organizations must establish clear policies for safe internet use in the workplace and communicate those policies to employees prior to their participation in cybersecurity training. These policies may include restrictions on criminal activity, propagating malware or viruses, downloading unauthorized software, sharing credentials without authorization, and accessing inappropriate sites.
- These policies should be clearly explained in the training program, with real-life examples and case studies for employees to work through and apply their knowledge. You can even show various websites and ask if they are acceptable to visit under the company policy.

Ensuring safe use of social media:

- Social media plays an increasingly important role in marketing any business, but it also poses unique risks. Providing employees with training on the nature of those risks and how to avoid them can prevent costly and embarrassing cyber incidents.
- To ensure the safe use of social media, apply all possible security measures to accounts, including securing all devices and eliminating unused accounts.
- Use good judgment based on cybersecurity best practices when accessing unknown websites or accounts. Avoid sharing unnecessary personal information on company social media feeds.
- Social media can be a target for threat actors seeking access to your profile. Using every available security feature for log-ins can help prevent this.
- Social media can contain malware hidden on seemingly harmless links. Ensure that any links you click are from trusted sources, and that those sources themselves haven’t been recently hacked.
- Sharing personal information like birthdays, children’s names, pets’ names, and other details can make it easy for threat actors to compromise your accounts.
- A valuable training exercise is to ask participants to audit their own social media accounts to see if they comply with best practices.