Phishing Awareness, Training and Testing

|  |  |  |
| --- | --- | --- |
| **Document Owner** | **Title** | |
| Your Name | | Chief Information Security Officer (or your Title) | |

**Document History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Rev #** | **Name** | **Date** | **Description** | **Signature** |
| 1.0 | Your Name |  | Initial draft | Electronically signed |
| 1.1 | Your Name |  | Initial release | Owner signature |

Version: 1.0 – *DRAFT Find / Replace “COMPANY” with your organization’s name, update cover logo and header logo*

Date: \_\_\_\_ , \_\_\_\_

**Table of Contents**

[1. Introduction 3](#_Toc31703801)

[1.1 Objective 3](#_Toc31703802)

[1.2 Scope 3](#_Toc31703803)

[1.3 Audience 3](#_Toc31703804)

[1.4 Document Changes and Feedback 3](#_Toc31703805)

[1.5 Referenced Documents 3](#_Toc31703806)

[2. Policy Requirements 4](#_Toc31703807)

[2.1 Phishing 4](#_Toc31703808)

[2.1.1 Combatting Phishing 5](#_Toc31703809)

[2.1.2 Actions for Suspected or Confirmed Phishing Attempt 5](#_Toc31703810)

[2.2 COMPANY Phishing Awareness Training 5](#_Toc31703811)

[2.3 Simulated Social Engineering Exercises 5](#_Toc31703812)

[2.4 Remedial Training Exercises 6](#_Toc31703813)

[3. Compliance & Non-Compliance with Policy 6](#_Toc31703814)

[3.1 Non-Compliance Actions 6](#_Toc31703815)

[3.2 Compliance Actions 6](#_Toc31703816)

[3.3 Removing Failure Events through Passes 7](#_Toc31703817)

[4. Responsibilities and Accountabilities 7](#_Toc31703818)

[Appendix A – Schedule of Failure Penalties 8](#_Toc31703819)

[Appendix B – Methods for Determining Staff Risk Ratings 9](#_Toc31703820)

[Appendix C – Glossary of Terms if Applicable 10](#_Toc31703821)

## 

## 1. Introduction

Technical security controls are a vital part of our information security framework but are not in themselves sufficient to secure all information assets. Effective information security also requires the awareness and proactive support of all staff, supplementing and making full use of the technical security controls. This is obvious in the case of social engineering attacks, especially phishing and other current exploits being used, which specifically target vulnerable humans rather than IT and network systems.

Lacking adequate information security awareness, staff is less likely to recognize or react appropriately to phishing and other information security threats and incidents, and are more likely to place information assets at risk of compromise. In order to protect information assets, all workers must be informed about relevant, current information security matters, and motivated to fulfill their information security obligations.

### 1.1 Objective

This policy specifies the COMPANY internal phishing information security awareness and training program to inform and assess all staff regarding their information security obligations. This policy specifically covers phishing and phishing awareness training.

### 1.2 Scope

This policy applies throughout the organization as part of the corporate governance framework. It applies regardless of whether staff use computer systems and networks, since all staff are expected to protect all forms of information assets including computer data, written materials/paperwork, and intangible forms of knowledge and experience. This policy also applies to third party employees working for the organization whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of ethics and acceptable behavior) to comply with our information security policies.

### 1.3 Audience

In general, this policy applies to all COMPANY employees and contractors with access to COMPANY systems, networks, company information, nonpublic personal information, personally identifiable information, and/or customer data.

### 1.4 Document Changes and Feedback

This policy will be updated and re-issued at least annually to reflect, among other things, changes to applicable law, update or changes to COMPANY requirements, technology, and the results or findings of any audit.

### 1.5 Referenced Documents

Documents that are relevant to this policy include the following:

|  |  |  |
| --- | --- | --- |
| **Policy** | **Policy Owner** | **Link** |
| Information Security Policy (ISP) | Information Security | TBD |
| HR/Employee Handbook | Human Resources | TBD |

## 2. Policy Requirements

All phishing awareness training must fulfill the requirements for the security awareness program as listed below:

* The information security awareness program should ensure that all staff achieve and maintain at least a basic level of understanding of phishing and other information security matters, such as general obligations under various information security policies, standards, procedures, guidelines, laws, regulations, contractual terms, and generally held standards of ethics and acceptable behavior.
* Additional training is appropriate for staff with specific obligations towards information security that are not satisfied by basic security awareness, for example Information Risk and Security Management, Security Administration, Site Security and IT/Network Operations personnel. Such training requirements must be identified in departmental/personal training plans and funded accordingly. The training requirements will reflect relevant prior experience, training and/or professional qualifications, as well as anticipated job requirements.
* Security awareness and training activities should commence as soon as practicable after staff joins the organization, generally through attending information security induction/orientation as part of the on boarding process. The awareness activities should continue on a continuous/rolling basis thereafter in order to maintain a reasonably consistent level of awareness.
* Where necessary and practicable, security awareness and training materials and exercises should suit their intended audiences in terms of styles, formats, complexity, technical content, etc. Everyone needs to know why information security is so important, but the motivators may be different for workers focused on their own personal situations or managers with broader responsibilities to the organization and their staff.
* The company will provide staff with information on the location of the security awareness training materials, along with security policies, standards, and guidance on a wide variety of information security matters.

### 2.1 Phishing

Phishing is a type of attack carried out to steal usernames, passwords, credit card information, Social Security Numbers, and other sensitive data. Phishing is most often seen in the form of malicious emails pretending to be from credible sources such as COMPANY technology departments or organizations related to the organization.

Attackers can use this information to:

* Steal money from victims (modify direct deposit information, drain bank accounts)
* Perform identity theft (run up charges on credit cards, open new accounts)
* Send spam from compromised email accounts
* Use your credentials to access other systems, attack other systems, steal COMPANY data, and jeopardize the mission of the organization

Phishing emails targeting campus want your COMPANY credentials. Some attackers will set up fake web sites and send emails with an immediate call-to-action that demands you to "update your account information" or "login to confirm ownership of your account". If you enter your COMPANY credentials into these illegitimate web sites you are sending your COMPANY username and password directly to the attackers.

#### 2.1.1 Combatting Phishing

COMPANY stops thousands of phishing attempts, spam emails, and virus infected messages every day, but the methods scammers use change very quickly.  Due to the variety of use for COMPANY email, we must also be careful when implementing filtering which may block otherwise legitimate email.

* Never send passwords, bank account numbers, or other private information in an email.
* Avoid clicking links in emails, especially any that are requesting private information.
* Be wary of any unexpected email attachments or links, even from people you know.
* Look for ‘https://’ and a lock icon in the address bar before entering any private information.
* Have an updated anti-virus program that can scan email.

#### 2.1.2 Actions for Suspected or Confirmed Phishing Attempts

The COMPANY Information Security (IS) department requires that each, in the event of suspected or confirmed phishing targeting conduct the following actions.

* Change your COMPANY login credentials
* Change your COMPANY and other related passwords
* Set mobile devices to delete all data via Exchange and/or FindMyiPad.
* Change login and password for any personal accounts that share the same password such as:
* Online banking
* Personal email
* Online purchasing (PayPal, Amazon, eBay, etc.)
* iTunes account
* Social media (Facebook, Twitter, blogs, etc.)
* Online backup service or file sharing (Dropbox, Mozy, Carbonite, etc.)
* Contact the abuse or fraud department of the service being impersonated (eBay, PayPal, etc.)
* Call the Technology Service Center
* If you suspect a bank or credit card account may have been compromised, contact that institution to check your account immediately and request a credit report.

### 2.2 COMPANY Phishing Awareness Training

The COMPANY Information Security (IS) department requires that each employee upon hire and at least annually thereafter successfully complete <selected course here>. Certain staff may be required to complete additional training modules depending on their specific job requirements upon hire and at least annually. Staff will be given a reasonable amount time to complete each course so as to not disrupt business operations.

### 2.3 Simulated Social Engineering Exercises

The COMPANY IS department will conduct periodic simulated social engineering exercises including but not limited to: phishing (e-mail), vishing (voice), smishing (SMS), USB testing, and physical assessments. The COMPANY IS department will conduct these tests at random throughout the year with no set schedule or frequency. The COMPANY IS department may conduct targeted exercises against specific departments or individuals based on a risk determination.

### 2.4 Remedial Training Exercises

From time to time COMPANY staff may be required to complete remedial training courses or may be required to participate in remedial training exercises with members of the COMPANY IS department as part of a risk-based assessment.

## 3. Compliance & Non-Compliance with Policy

Compliance with this policy is mandatory for all staff, including contractors and executives. The COMPANY IS department will monitor compliance and non-compliance with this policy and report to the executive team the results of training and social engineering exercises.

The penalties for non-compliance are described in Appendix A of this policy.

### 3.1 Non-Compliance Actions

Certain actions or non-actions by COMPANY personnel may result in a non-compliance event (Failure).

A Failure includes but is not limited to:

* Failure to complete required training within the time allotted
* Failure of a social engineering exercise

Failure of a social engineering exercise includes but is not limited to:

* Clicking on a URL within a phishing test
* Replying with any information to a phishing test
* Opening an attachment that is part of a phishing test
* Enabling macros that are within an attachment as part of a phishing test
* Allowing exploit code to run as part of a phishing test
* Entering any data within a landing page as part of a phishing test
* Transmitting any information as part of a vishing test
* Replying with any information to a smishing test
* Plugging in a USB stick or removable drive as part of a social engineering exercise
* Failing to follow company policies in the course of a physical social engineering exercise

Certain social engineering exercises can result in multiple Failures being counted in a single test. The maximum number of Failure events per social engineering exercise is two.

The COMPANY IS department may also determine, on a case by case basis, that specific Failures are a false positive and should be removed from that staff member’s total Failure count.

### 3.2 Compliance Actions

Certain actions or non-actions by COMPANY personnel may result in a compliance event (Pass).

A Pass includes but is not limited to:

* Successfully identifying a simulated social engineering exercises
* Not having a Failure during a social engineering exercise (Non-action)
* Reporting real social engineering attacks to the IS department

### 3.3 Removing Failure Events through Passes

Each Failure will result in a Remedial training or coaching event as described in Appendix A of this document. Subsequent Failures will result in escalation of training or coaching. De-escalation will occur when three consecutive Passes have taken place.

## 4. Responsibilities and Accountabilities

Listed below is an overview of the responsibilities and accountabilities for managing and complying with this policy program.

The Chief Information Security Officer/Information Security Manager is accountable for running an effective information security awareness and training program that informs and motivates workers to help protect the organization’s and the organization’s customer’s information assets.

Information Security Management is responsible for developing and maintaining a comprehensive suite of information security policies (including this one), standards, procedures and guidelines that are to be mandated and/or endorsed by management where applicable. Working in conjunction with other corporate functions, it is also responsible for conducting suitable awareness, training, and educational activities to raise awareness and aid understanding of staff’s responsibilities identified in applicable policies, laws, regulations, contracts, etc.

All Managers are responsible for ensuring that their staff and other workers within their responsibility participate in the information security awareness, training, and educational activities where appropriate and required.

All Staff are personally accountable for completing the security awareness training activities, and complying with applicable policies, laws, and regulations at all times.

# Appendix A – Schedule of Failure Penalties

The following table outlines the penalty of non-compliance with this policy. Steps not listed here may be taken by the COMPANY IS team to reduce the risk that an individual may pose to the company.

|  |  |
| --- | --- |
| **Failure Count** | **Resulting Level of Remediation Action** |
| First Failure | Mandatory completion of <selected course here>. |
| Second Failure | Mandatory completion of <selected course here>. |
| Third Failure | Mandatory completion of <selected course here>. |
| Fourth Failure | Face to face meeting with their manager |
| Fifth Failure | Face to face meeting with their manager and Head of Human Resources |
| Sixth Failure | Face to face meeting with the CISO and the Head of Human Resources   * Possibility that additional administrative and technical controls will be implemented to prevent further Failure events |
| Seventh Failure | Meeting with CISO, CEO and Head of Human Resources   * Possibility that additional administrative and technical controls will be implemented to prevent further Failure events |
| Eighth Failure | Formal review of employment with Head of Human Resources   * Possibility that additional administrative and technical controls will be implemented to prevent further Failure events |
| Ninth and Subsequent Failures | Potential for Termination of Employment or Employment Contract |

# Appendix B – Methods for Determining Staff Risk Ratings

The following is a list of situations that may increase a risk rating of a COMPANY staff member. Higher risk ratings may result in an increased sophistication of social engineering tests and an increase in frequency and/or type of training and testing.

* Staff member email resides within a recent Email Exposure Check report
* Staff member is an executive or VP (High value target)
* Staff member possesses access to significant company confidential information
* Staff member is using a Windows or Apple-based operating system
* Staff member uses their mobile phone for conducting work-related business
* Staff member possesses access to significant company systems
* Staff member personal information can be found publicly on the internet
* Staff member maintains a weak password
* Staff member has repeated company policy violations

# Appendix C – Glossary of Terms if Applicable