Central Office Phishing Exercise Compliance Reward and Non-Compliance Escalation Procedure

Effective Date: March 1, 2024
Function: Compliance – Information Security
Contact: Office of Compliance Services – Chief Information Security Officer

Basis for Procedure

Phishing and other social engineering tools are often used to illegally access computer networks and systems. The Research Foundation requires annual information security training for Central Office Employees and runs routine phishing exercises to reinforce the training and identify those who successfully navigate the exercise and those who require remedial training and reinforcement. Consistent with the RF's Progressive Discipline Policy this procedure outlines the process for handling those individuals who repeatedly engage in a Non-Compliance Action and offers incentives for those that satisfied the parameters of the exercise with a Compliance Action.

Procedure Summary

This procedure outlines the measures taken when an individual engages in Compliance or Non-Compliance Actions.

Procedure

Step	Role or Responsibility
1. Review exercise results	Information Security
2. Identify Non-Compliance Actions	Information Security
3. Identify Compliance Actions	Information Security
4. Take remedial action for Non-Compliance Actions	Information Security, DISO, supervisor, VP
5. Take incentive action for Compliance Actions	DISO, Supervisor, VP

Incentives for Compliance

Four consecutive Compliance Activities	• Individual is entered into a prize drawing to be held two times per year
Eight consecutive Compliance Activities	• Individual's supervisor is notified • Individual is recognized at the next All CO Staff Meeting

Remedial Action for Non-Compliance

Failure Count	Resulting Level of Remediation Action
First Failure	• Email to individual from DISO or designee
Second Failure	• Mandatory completion of Information Security Course Level I • Supervisor is notified
Third Failure	• Mandatory completion of Information Security Course Level II • Discussion with DISO and Supervisor
Fourth Failure	• Mandatory completion of Information Security Course Level III • Face to face meeting with DISO, Supervisor & Departmental VP
Fifth and Subsequent Failures	• Face to face meeting with DISO, Supervisor & Departmental VP • Possibility that additional administrative and technical controls will be implemented to prevent further Failure events

Automatic Resets of Failure Count

If an individual has…	Then their Failure Count will reset to zero when…
One Failure	Six months have passed since the first Failure with no additional Non-Compliance Actions
Two or more Failures	One year has passed since the individual's last Failure with no additional Non-Compliance Actions

Failure to Complete Required Training

If an individual fails to complete training required by this procedure by the deadline without obtaining an extension from the Office of Compliance Services, the individual's supervisor and Departmental Vice President will be notified, the individual may lose network privileges and may otherwise be subject to the Progressive Discipline Policy.

Definitions

Compliance Action - Certain actions or non-actions by Research Foundation users may result in a compliance event (Pass).

A Pass includes but is not limited to:

- Successfully identifying a simulated social engineering exercise
- Not having a Failure during a simulated social engineering exercise (Non-action)

Non-Compliance Action - Certain actions or non-actions by Research Foundation systems users may result in a non-compliance event (Failure).

A Failure includes but is not limited to:

- Failure of a simulated or actual social engineering exercise or incident

Failure of a simulated or actual 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
- Requesting release from email quarantine of a phishing email

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 Research Foundations Office of Compliance Services may also determine, on a case by case basis, that specific Failures are a false positive and should be removed from that users total Failure count.

Related Information

Acceptable Use and Security of RF Data and Information Technology Policy
Progressive Discipline Policy

Forms

None

Change History

Date	Summary of Change
March 1, 2024	This is a new procedure.

Feedback

Was this document clear and easy to follow? Please send your feedback to webfeedback@rfsuny.org.