LABOR RELATIONS

UNITED STATES POSTAL SERVICE

April 26, 2022

Mr. Ivan Butts
President
National Association of Postal Supervisors
1727 King Street, Suite 400
Alexandria, VA 22314-2753

Dear Mr. Butts:

The Postal Service proposes to create new training entitled, Repeat Clicker Remediation.

This training will be a requirement for any employee with an active ACE ID identified as a repeat offender of Postal Service Phishing Simulations. The training will be conducted via a webinar and is intended to increase awareness of security requirements for employees who repeatedly fail Corporate Information Security Office (CISO) phishing exercises. Failure to attend the training will result in the restriction of an employee's ability to receive external emails.

Please find enclosed a copy of the proposed Repeat Clicker Remediation Plan.

If you have any questions on this matter, please contact Bruce Nicholson at extension 7773.

Sincerely,

David E. Mills
Director
Labor Relations Policies and Programs

Enclosure

475 L'ENFANT PLAZA SW
WASHINGTON DC 20260
WWW.USPS.COM

UNITED STATES POSTAL SERVICE

Repeat Clicker Remediation Plan - Standard Operating Procedure

CONTENTS

INTRODUCTION

This standard operating procedure (SOP) describes the process of remediation for repeat clickers during phishing simulations.

CISO conducts monthly phishing simulations. Any personnel that fell victim to the phish and clicked on the embedded link or file, i.e. lure, are then phished again the following week with the same lure. If they fail this simulation again, they are considered repeat clickers.

The repeat clicker data will be provided at the time the monthly summary is prepared and presented to Postal Service leadership.

Specifically, this procedural overview provides the information necessary for remediation of repeat clicker behavior and reduction in click rate during monthly phishing simulations.

This remediation procedure will be overseen by the Cybersecurity Awareness and Training program. Any user that has been a repeat clicker 10 or more times will become part of the Remediation Program. In time, the scope will expand to 5 or more times. This will be a gradual process, going to 9 or more, then 8 or more, etc.

PROCEDURE

Step 1:

1. A first-time repeat clicker will be recorded as a repeat clicker. The user will become part of the Repeat Clicker Program.

Step 2:

1. When an individual clicks 10 times or more, they will become a part of the Repeat Clicker Remediation Plan. The user's manager will be required to complete an Acknowledgement Form within 15 days of notification. They will be invited to attend a remediation webinar with their manager, Cybersecurity awareness manager and/or the Deputy Chief Information Security Officer (DCISO). These sessions will be scheduled by Awareness and Training staff. This webinar will include a revised presentation of Phishing ABCs and the steps to identify a potential phish. The webinar will emphasize how to use the Report to Cybersafe Security button in Outlook.
2. CISO will start running webinars for repeat clickers; they will be recurring on the 2nd week of each following month.
3. Failing to attend the first webinar (Exceptions: Approved leave or Training), will result in a user losing access to external email and it will not be restored until the user's manager submits a waiver form.
4. During this session discussion will focus on identifying potential phish, the "hooks" used, and the seriousness of clicking on links or files contained in an email.
5. The employee will be warned that repeated failures of phishing simulations could result in sanctions to the receipt of any external emails.

USPS Policy allows for the enforcement of sanctions for employees not carrying out their information security responsibilities (see AS-805 paragraph 6-2.5; https://about.usps.com/handbooks/as805.pdf).

Step 3:

1. DCISO recommends any individual that has clicked on a phishing lure 10 times or more in the last 3 years, lose access to receive external emails. An Acknowledgement Form will be required.
2. DCISO will coordinate with the user's manager to ensure this restriction does not impact their ability to complete their job.
3. Access to external email will be suspended for a minimum of 90 days, if not indefinitely.
4. If the user qualifies for a waiver due to needing external email for Business Reasons, the user's manager is required to complete and submit a waiver. (A waiver form is included on the last page)
5. With assistance from the CyberSecurity Operations Center (CSOC) the user's email inbox will restrict receipt of all external email.
6. A tracking sheet in the DCISO Teams application will be the official record of when a user is added to the program or when they can be removed from the program. The program tracking will be the responsibility of the CISO Awareness and Training team.
7. In order to re-establish external email privileges, the user must demonstrate their awareness by not clicking on a lure for a period of 3 consecutive months. DCISO will require certification from a PCES manager that the employee's external email privileges should be re-instated.
8. DCISO will regularly monitor the list of repeat clickers with 10 or more clicks and work with the CSOC to implement the aforementioned changes to their email access.
9. Once a user has not been a repeat clicker for a period of 24 months, they will be removed from the repeat clicker remediation program.

Key Requirements	Notes on Timing	Repeat Clicker	New Entrant Remediation Program	Active	*Sanctioned or Waived*	Not Active
1. *User, employee or contractor, fails a phishing test, was re-phished a 2nd time in the same month and clicked on the lure a 2nd time. The user becomes a Repeat Clicker. Subsequent failed phishing tests are recorded and tracked.*	NA	X				
2. *Repeat Clicker that has clicked 10 or more phishing lures in the past 3 years*		X	X			
3. *Notification email sent by DCISO to User & Manager w/ a requirement for the user to attend webinar event and Acknowledgement Form*	1st of Month	X		X		
4. *User accepts webinar invitation and attends next event*	Qtly/Monthly	X		X		
5. *Manager completes Acknowledgement Form within 15 days of email receipt. Manager chooses to "Sanction" or "Waive" the sanction.*	15th of Month	X		X	S or W	
6. *90 days have elapsed from the date on the Acknowledgement Form. User has not clicked on another phishing lure in that period. User may have external email re-activated*	15th of Month	X		X		
7. *To lift the sanction for a User, Manager submits Manager Certification to re-instate external email.*		X		X	W	
Note: exceptions exist for unique situations, i.e. false positives for technical teams testing links in the course of their normal duties. Documentation is required from the manager noting this situation.						
Escalations:						
• User does not attend Webinar (step 4) o Email will be sent to the manager and user notifying them of this issue within 5 days. User will be Sanctioned until they are able to attend the next scheduled Webinar.		X		X	S	
• Manager does not return Acknowledgement Form within 15 days (step 5) o Next higher level manager, receives an email requesting follow-up and advising them of risk to Sanction the user o If no response is provided within 5 days; User will be Sanctioned until the Manager provides the form.				X	S	
• User clicks on a subsequent phishing lure after (step 6 above) o If the User has less than 10 clicks in the past 3 years: User is Sanctioned until they are able to attend the next scheduled Webinar. Manager must submit a new form to remove the sanction. o If the User has 10 or more clicks in the past 3 years: User is Sanctioned for a minimum of 3 months. Manager must submit a new form after 3 months to remove the sanction.				X	S	

CISO requests USPS leadership continue to raise awareness, stress importance of security diligence and remind employees to carefully review emails for suspicious content. USPS personnel who click on phishing email simulations, that could have been an actual credential phishing attack, place the entire organization at risk. Repeatedly clicking on phishing emails may mean the employee no longer can receive external emails.

ARTIFACT(S) REFERENCE

Artifact Number	Name
1	Phishing ABCs Presentation
2	Acknowledgement of External Email Suspension or Waiver
3	PCES Manager Certification to re-instate receipt of external email
4	Remediation Timeline

REMEDIATION PROGRAM TIMELINE

- April: Bring into the remediation program any repeat clickers with 10 or more clicks
- May to June: Expand program to include any clickers with 9 or more clicks
- July to August: Expand program to include any clickers with 8 or more clicks
- Sep to October: Expand program to include any clickers with 7 or more clicks

APPENDIX

ACKNOWLEDGEMENT OF [EXTERNAL] EMAIL SUSPENSION or WAIVER

Employee/Contractor Name: _____

Complete Part I **or** Part II

Part I – [External] email business need waiver

The person listed above has been identified as a repeat clicker for phishing simulations conducted by the Cybersecurity Awareness and Training workstream. This person requires external email access in order to complete their daily work functions.

Certified by (manager's name): _____

Manager's Signature: _____ Date: _____

Part II – Suspension of [EXTERNAL] email

The person shown above has repeatedly clicked on phishing lures indicating that they pose a risk to the Postal Service network. The phish is normally received through email tagged as [EXTERNAL]. For that reason, all email tagged as [EXTERNAL] will be filtered from the user's inbox. This will remain in place for a minimum of 90 days.

As the person's manager I understand the importance of caution when opening and interacting with emails and agree to this restriction.

Certified by (manager's name): _____

Manager's Signature: _____ Date: _____

Manager Certification to Reinstate [External] Email

Employee/Contractor Name: _____

The person listed above has been identified as a repeat clicker for phishing simulations conducted by the Cybersecurity Awareness and Training workstream. This person has received remedial training and has not clicked on a phishing simulation lure for the past 3 months. Therefore, I am requesting this user's External email be reinstated.

Certified by (manager's name): _____

Manager's Signature: _____ Date: _____