

Phishing Incident Response Runbook

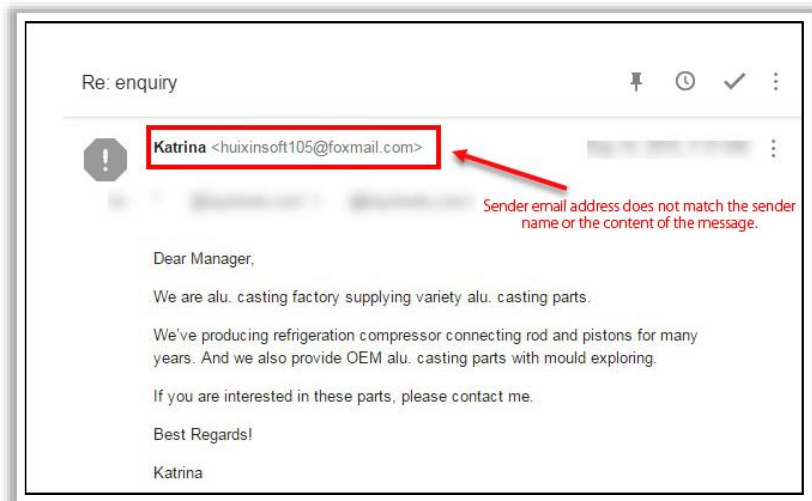
Title	Phishing Incident Response Runbook
Version	1.0
Date issued	DD-MM-YYYY
Status	In progress
Document owner	
Creator name	
Creator organization name	ECC
Subject category	Phishing Incident Management
Access constraints	
Review cycle	Annually

Note: Organizations can use this runbook to deal with phishing incidents alongside the security guidelines of their incidence response plan and the relevant playbook. The IH&R team may add or remove some guidelines from this runbook according to the type of phishing incident and business requirements considering organizational security policies.

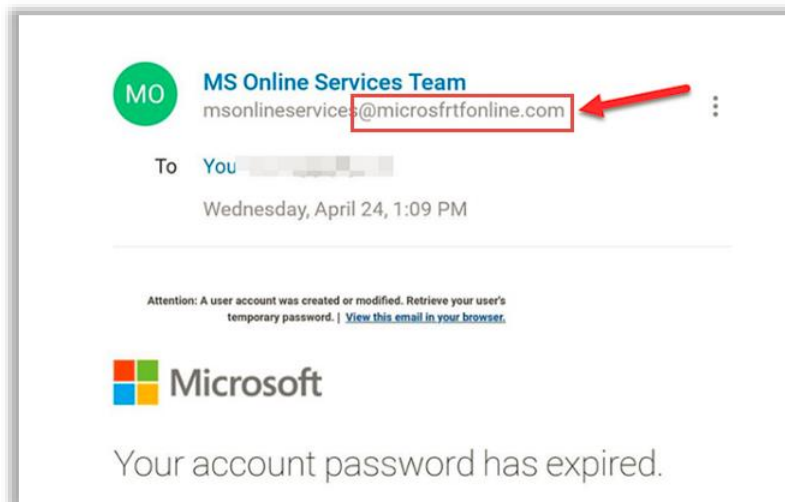
1. Incident Detection

To detect phishing incidents, employees should be well-trained to identify spam/phishing emails by verifying the possible phishing indicators or mistakes in email messages that distinguish a phishing email from the original one. It should be noted that spam/phishing emails contains different variations.

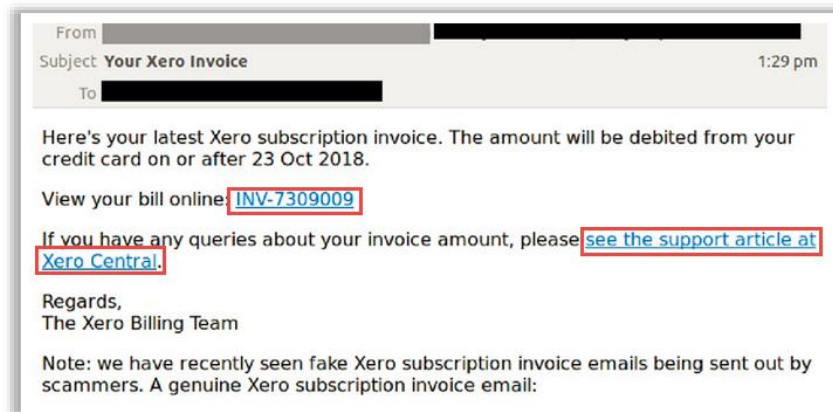
- Evaluate alerts reported by employees:
 - Identify the type of suspected malicious email and the reason for raising the ticket as an incident.
 - Check if the reported email is a phishing email by examining the alert and linked email message.
 - Check if the email originated from an unfamiliar source having attachments with extensions .zip, .exe, or .scr.
 - Verify the email for unusual/suspicious content:
 - If the email represents any organization, check the sender email address ending with @<organization name> or public domains such as @gmail.com or @yahoo.com, as shown in the screenshot below.



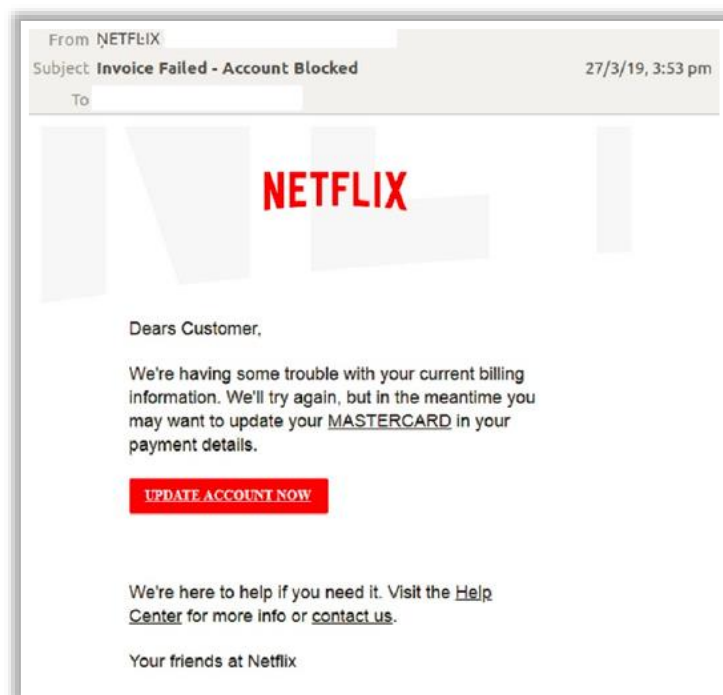
- Check the domain name spelling and compare it with official name, as shown in the screenshot below.



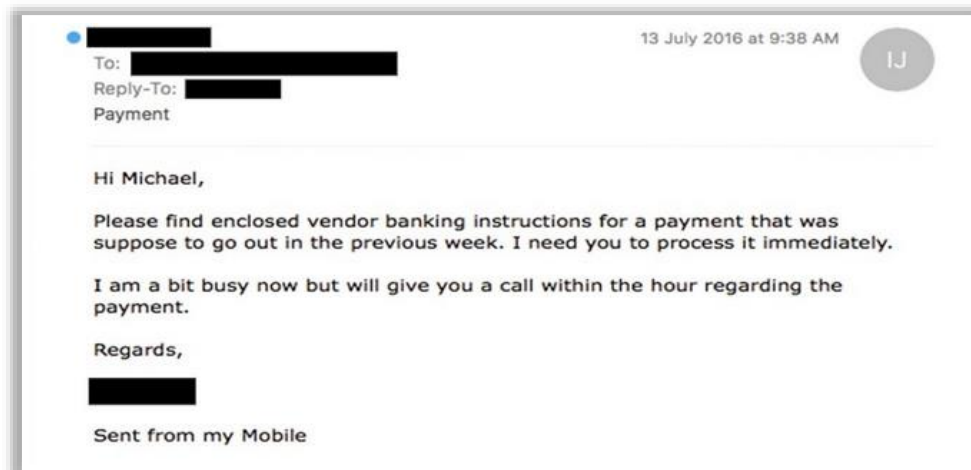
- Check for grammatical mistakes and sentence formations in the email message.
- Ensure that the logo present in the email is the same as the official logo.
- Ensure that the links included in the email navigate to the expected domain by hovering the cursor on them and check the actual URL for the text highlighted in the screenshot.



- Check the destination address of suspicious links and compare them with the email content.
- Check if the email is requesting users to change/reset their password by clicking on the provided link with an unknown destination.
- Check if the email is requesting users to make payments using the provided link that appears to be an official website, as shown in the screenshot below.



- Check whether the email conversation starts with a greeting.
- Check if the email suggests users to take immediate action to avoid unexpected consequences, as shown in the screenshot below.




- Make a list of employees who received the mail, those who reported it as a phishing email, and those who accessed the links and attachments contained in the emails.
- If the alert was generated by an employee, collect the following details:
 - Details of employee who received the email
 - Source email address
 - Links and attachments, if any
 - Email originated domain name
 - Hostname and IP address of the SMTP server

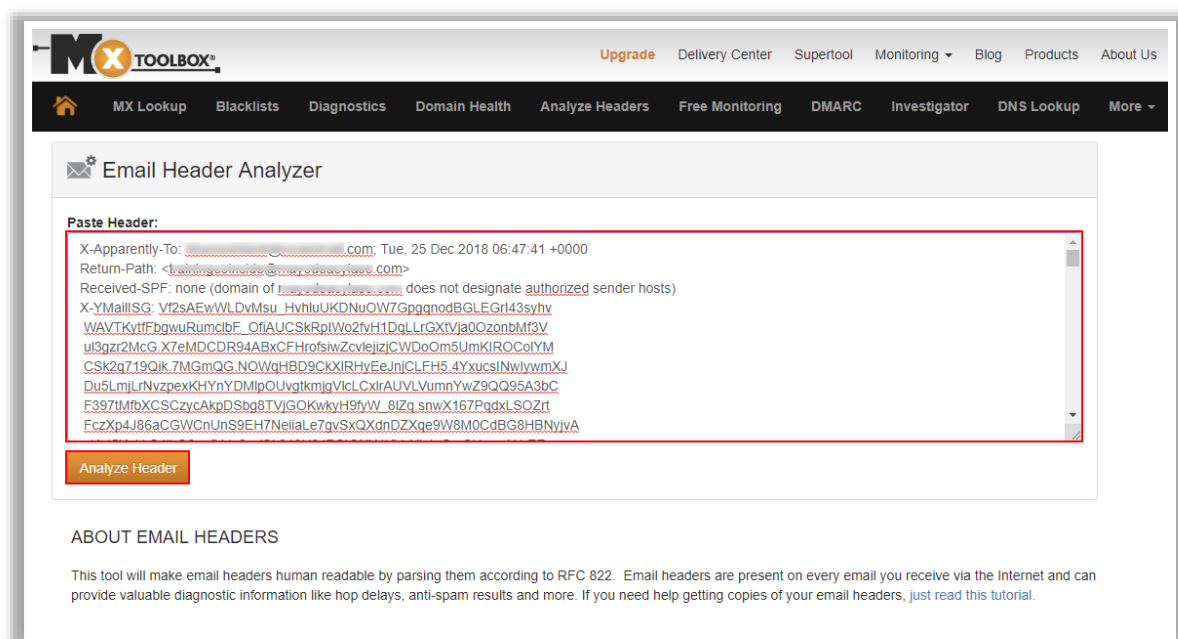
2. Containment

- Isolate the employee system used to access the links or download attachments from the suspected email.
- Close all active sessions through the email from the affected system.
- Delete unread phishing emails present in the queue for all employees.
- Disconnect the system from the internet to remove remote access to the system (if any).
- Reduce the impact of the email on other employees by identifying its key objectives and implementing filters to block emails with a similar signature.
- Block automatic email forwarding to remote unknown domains.
- Use an email link isolation technique that scans the malicious link and opens the in-cloud isolation platform away from the user.
- Use an email attachment isolation technique that isolates the email content and other attachments to protect users from malware infection.
- Enable the mailbox auditing feature.
- Scan the affected system using antivirus or antimalware software such as TotalAV, Bitdefender Antivirus Plus, and Kaspersky Anti-Virus to block further malware activities.

3. Evidence Gathering and Forensic Analysis

Gather evidence from email messages and analyze the email header of Gmail, Outlook, etc. Once the reported email is confirmed to be a phishing email, the IH&R team must perform forensic analysis on the email header to determine complete details of the sender and root cause of the incident. Follow the steps given below alongside the phishing playbook to analyze the suspected email.

- Steps to extract and analyze the email header in Gmail:
 - Log in to Gmail account and open the phishing email.
 - Click on more  → select “Show original.”
 - A new tab opens displaying the original message.
 - Check for SPF and DKIM credentials that verify the authenticity of the email address; then, copy the email header.
 - Open MXToolbox, an online email header analysis tool (**MXToolbox → Analyze Header**) and paste the copied email header for analysis, as shown in the screenshot below.



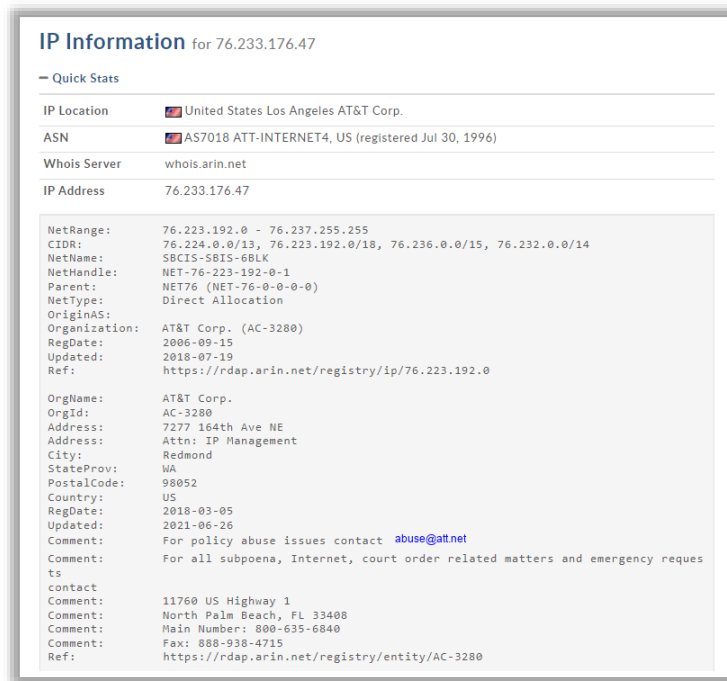
- Gather the following evidence details from the email header:
 - Return path
 - Recipient email address
 - Name of email server
 - Type of email sending service
 - IP address of sending server
 - Unique message number
 - Date and time when the email was sent

- Sender Policy Framework (SPF)
- Domain Keys Identified Mail (DKIM)
- Information on attachment files
- Follow the steps given below to check the validity of an email address:
 - Copy the source email address from the phishing email.
 - Visit any online email address scanning tool such as Email Dossier and enter the email address found in the phishing email
 - Email Dossier checks the validity of the email address, as shown in the screenshot below.

The screenshot shows the Email Dossier website interface. At the top, there's a header with the title 'Email Dossier' and the subtitle 'Investigate email addresses'. Below this is a search bar where an email address is entered, followed by a 'go' button. The user is logged in as 'anonymous' with a balance of '46 units'. There are links for 'log in' and 'account info', and a 'Central Ops.net' logo. The main content area shows 'Validating' status for the email address. Below this, the 'Validation results' section displays a 'confidence rating: 3 - SMTP' and a message stating the email address passed validation without error but is not guaranteed to be good. It also shows the 'canonical address' as '<[redacted]@gmail.com>'. The 'MX records' section contains a table with columns for preference, exchange, and IP address (if included). The table lists five records for gmail-smtp-in.l.google.com with preferences 5, 10, 20, 30, and 40. The 'SMTP session' section shows a log of '[Contacting gmail-smtp-in.l.google.com [redacted]...]' and '[Connected]'.

preference	exchange	IP address (if included)
5	gmail-smtp-in.l.google.com	[redacted]
10	alt1.gmail-smtp-in.l.google.com	[redacted]
20	alt2.gmail-smtp-in.l.google.com	[redacted]
30	alt3.gmail-smtp-in.l.google.com	[redacted]
40	alt4.gmail-smtp-in.l.google.com	[redacted]

- Analyze the source IP address extracted from the email header in the WHOISLookup Search tool, as shown in the screenshot below.



- Use tools such as eMailTrackerPro and MailTracker to track emails and extract information such as the sender identity, mail server, sender IP address, and location.
- If the attachment contains malicious content, perform malware analysis to examine the malware operation.

4. Eradication

- Permanently block unknown IP addresses and websites identified in the phishing email.
- Use antispam and anti-phishing tools such as SPAMfighter, SpamTitan, and MailWasher to filter and block phishing emails.
- Blacklist malicious websites and disable automatic downloads across all systems and devices.
- Scan the affected systems using sophisticated antivirus solutions to ensure the complete elimination of malware-related artifacts.
- Patch the email communication system upon the identification of vulnerabilities during the detection or analysis phase.
- Implement DNS blackholing to block IP addresses used to send malicious emails.
- Follow the steps given below to report phishing emails in Gmail:
 - Open the suspicious mail and click on the “**More**” button (three vertical dots) at the top-right corner of the email.
 - Select the “**Report spam**” or “**Report phishing**” option based on the type of email incident you want to report.

- Follow the steps given below to report phishing emails in Outlook:
 - Open the suspicious email and click on the “**Report message**” option from the toolbar.
 - From the dropdown list, select **Junk** or **Phishing**.
 - A popup window appears; click on **Report**.

5. Recovery

- Change the passwords of affected email accounts and other related accounts.
- Block the bank accounts connected to that email and abort all transactions.
- Recover deleted emails from the trash folder in Gmail, if possible.
- Use tools such as EaseUS Email Recovery Wizard and Stellar Undelete Email for Outlook to recover emails.
- Restore the affected systems using trusted backups.
- Follow the steps given below to restore deleted emails in Outlook:
 - Log in to **MS Outlook** and open the **Deleted Items** folder.
 - Then, in the **HOME** tab, click on **Recover Deleted Items From Server**.
 - The **Recover Deleted Items** window appears; click on the email you want to recover and select the “**Restore Selected Items**” radio button. Then, click on **OK**.
 - Now, navigate back to the **Deleted Items** folder; you can find the recovered email here.

6. Post-incident Actions

- Close the incident and document all steps, procedures, and corresponding results in a clear format and get it reviewed by an editor.
- Disclose incident details to the respective stakeholders and authorities by consulting with the legal department of the organization.
- Contact law enforcement, if required, brief them about the incident, and provide the necessary details.