Runbook:

RESPONDING TO A SUSPICIOUS EMAIL FROM A COMPROMISED COLLEAGUE

MERIT 2.0

OBJECTIVE: Provide a step-by-step guide to help you respond effectively to a suspicious email from a colleague's compromised account while preventing further attack propagation.

1. DO NOT INTERACT WITH THE EMAIL

- **Avoid Clicking Links or Attachments:** Do not open attachments or click on links within the email.
- **Do Not Reply or Forward:** Refrain from replying to or forwarding the email to others, as this may spread the malicious content.

2. PRESERVE THE EMAIL SAFELY

- **Keep the Email Intact:** Leave the email in your inbox to preserve metadata that may be useful for investigation.
- **Take Screenshots:** Capture screenshots of the email content and headers if required for reporting.

3. REPORT TO YOUR IT/SECURITY DEPARTMENT IMMEDIATELY

Contact IT/Security Team:

- Send an email to your IT/security department using a separate email thread.
- Include relevant details such as the sender's address, timestamp, and suspicious content.

Follow Company Protocols: Adhere to your organization's specific reporting procedures.

4. NOTIFY THE AFFECTED COLLEAGUE THROUGH A SECURE CHANNEL

Use Alternative Communication Methods:

- Call them on the phone.
- Speak to them in person.
- Use a secure messaging app if available.

Inform Them Briefly: Let them know that their email account appears compromised and advise them to contact IT/security immediately.

5. AVOID SPREADING THE INFORMATION UNNECESSARILY

- **Maintain Confidentiality:** Do not discuss the incident with other colleagues unless instructed by the security team.
- **Prevent Panic:** Sharing unverified information can cause unnecessary concern.

About MERIT 2.0

MERIT was founded in 1983 and was re-branded in 2020 as MERIT 2.0. Our Mission Statement is *To educate every worker at every client and provide them the technology to improve.*

How to Contact MERIT 2.0

SERVICE/REPAIRS/HELPDESK:
service@meritsolutions.net
or call 757-420-5150

www.meritsolutions.net

6. FOLLOW IT/SECURITY DEPARTMENT INSTRUCTIONS

- **Provide Additional Information if Requested:** Be prepared to assist with any further details the security team may need.
- **Comply with Mitigation Steps:** If instructed to change passwords or update software promptly.

7. MONITOR YOUR ACCOUNTS AND DEVICES

- **Check for Unusual Activity:** Look at your email account and other systems for any signs of compromise.
- **Run Antivirus Scans:** Ensure your device is free from malware by running a full system scan.

8. UPDATE YOUR CREDENTIALS IF NECESSARY

- **Change Passwords:** If there's any chance your account was affected, update your passwords using strong and unique combinations.
- **Enable Multi-Factor Authentication (MFA):** If it is not already in place, this will add an extra layer of security to your accounts.

9. EDUCATE YOURSELF AND STAY VIGILANT

- **Review Security Policies:** Familiarize yourself with your organization's cybersecurity policies and best practices.
- **Attend Training Sessions:** Participate in any offered cybersecurity awareness programs.

10. DOCUMENT THE INCIDENT

- **Keep Records:** Maintain a personal incident log, including dates, times, and actions.
- **Submit Reports if Required:** Fill out any formal incident reports as directed by your organization.

Remember: Quick and cautious action can significantly reduce the impact of cybersecurity threats. Always prioritize communication with your IT/security department and adhere to company policies when dealing with such incidents.