# Runbook:

## COMMUNICATING WITH AFFECTED USERS AFTER A BUSINESS EMAIL COMPROMISE

MERIT 2.0

**OBJECTIVE:** Provide a step-by-step guide for the victim of a business email compromise on how to communicate effectively with users who were targeted in the attack, aiming to mitigate risks, address potential PII leakage, and restore trust.

### 1. COORDINATE WITH YOUR IT/SECURITY DEPARTMENT FIRST

**Report the Incident Immediately:**

- Contact your organization's IT or security team when you become aware of the compromise.
- Provide all relevant details, including the time of the incident and any suspicious activities observed.

**Follow Their Guidance:**

- Adhere strictly to the instructions provided by the security team.
- Do not take independent actions without consulting them, as this could interfere with the investigation.

### 2. SECURE YOUR ACCOUNT AND DEVICES

**Change Passwords:**

- Update passwords for your email and any linked accounts using strong, unique passwords.

**Enable Multi-Factor Authentication (MFA):**

- Add MFA to your accounts to enhance security.

**Check for Unauthorized Access:**

- Review email settings for unfamiliar forwarding rules or permissions.

**Run Antivirus and Anti-Malware Scans:**

- Ensure your devices are free from malicious software.

### 3. IDENTIFY THE SCOPE OF THE IMPACT

**Obtain a List of Affected Contacts:**

- With the help of IT, determine which users were targeted by emails sent from your compromised account.

**Assess the Content Sent and Accessed:**

- Review sent emails and check for unauthorized access to your inbox, especially emails containing sensitive or personal information.

**Determine PII Exposure:**

- Identify any Personally Identifiable Information (PII) that may have been accessible to the threat actor.

## 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

## **4. ADDRESS POTENTIAL PII LEAKAGE

**Consult with Compliance and Legal Teams:**

• Inform your organization's compliance and legal departments about the potential PII exposure.
• Understand any legal obligations for reporting the data breach to authorities or affected individuals.

**Evaluate Reporting Requirements:**

• Determine if the incident requires notification under laws such as GDPR, HIPAA, or other relevant regulations.

**Prepare Notifications for Affected Parties:**

• Draft communications to individuals whose PII may have been compromised, following legal guidelines and company policies.

**Implement Additional Security Measures:**

• Work with IT to enhance security controls around sensitive data.

## 5. PREPARE A COMMUNICATION PLAN

**Draft a Notification Message:**

• Create a clear and concise email informing users about the incident.

**Key Points to Include:**

• A brief explanation of the situation without disclosing sensitive internal details.
• The timeframe during which the compromise occurred.
• Instruct recipients not to open suspicious emails, links, or attachments from you.
• Steps they should take if they interacted with the malicious email (e.g., running a virus scan).
• Information about any PII that may have been exposed and recommended actions (e.g., monitoring accounts, changing passwords).

**Review the Message with IT/Security and Legal:**

• Have your security and legal teams review the draft to ensure accuracy and compliance with regulations.

## 6. COMMUNICATE WITH AFFECTED USERS

**Use a Secure Channel:**

• Ensure your email account is secured before sending out communications.
• If necessary, use an alternative method approved by IT (e.g., phone call, secure messaging).

**Maintain Professionalism:**

• Keep the tone professional and empathetic.

**Respect Privacy:**

• Use BCC for group emails to protect recipients' identities.

## 7. PROVIDE SUPPORT AND RESOURCES

**Offer Assistance:**

• Encourage users to contact you or the IT/security team with questions.

**Share Preventative Tips:**

• Provide general advice on how they can protect themselves from similar incidents.

**Advise on PII Protection:**

• If applicable, recommend that affected individuals monitor their financial accounts and credit reports or take other protective measures.

## 8. AVOID SHARING UNNECESSARY DETAILS

**Maintain Confidentiality:**

• Do not disclose sensitive information about the security breach or internal processes.

**Focus on Actionable Information:**

• Keep communications relevant to what the recipients need to know and do.

## 9. MONITOR AND RESPOND TO FEEDBACK

**Be Responsive:**

• Address any replies or concerns from recipients promptly.

**Escalate When Necessary:**

• Forward complex questions to the IT/security or legal team.

## 10. DOCUMENT ALL COMMUNICATIONS

**Keep Records:**

• Maintain a log of who was contacted and when.

**Report to Management:**

• Provide updates to your supervisor or relevant departments as required.

**Record PII Exposure Details:**

• Document the types of PII that were potentially exposed, and the steps taken to address the issue.

## 11. LEARN AND PREVENT FUTURE INCIDENTS

**Participate in Training:**

• Engage in cybersecurity awareness programs offered by your organization.

**Implement Best Practices:**

• Adopt recommended security measures in your daily activities.

**Review Data Handling Procedures:**

• Work with your team to improve how sensitive information is stored and accessed.

**Remember:** Handling potential PII leakage requires careful coordination with your organization's legal and compliance teams to meet all regulatory obligations. Effective communication is crucial in mitigating the impact of a security incident. By promptly informing affected users and guiding them on necessary actions, you help protect them and maintain their trust.