# **Business Email Compromise (BEC) Incident Communication Evidence Guide Part of the BEC Incident Response Toolkit**

### **Introduction**

In the wake of a Business Email Compromise (BEC) incident, the collection and preservation of communication evidence is a critical step in the response process. This guide is designed to help individuals and organizations efficiently and effectively gather crucial communication data that may be pivotal for investigating the incident.

## **Email Headers and Content**

**Objective**: To capture and record comprehensive details from email correspondence.

***Description****: Paste the entire email header information here.*

| **Email Headers** |
| --- |
|  |

***Instructions for Collecting Email Headers:***

* + **Outlook**:
    - Open the suspicious email.
    - Click on 'File' > 'Properties'.
    - In the 'Internet headers' section, right-click, select all, and then copy.
  + **Gmail**:
    - Open the email.
    - Click on the three dots next to the reply button, select 'Show original'.
    - In the new window, click 'Copy to clipboard'.
  + **Apple Mail**:
    - Open the email.
    - Select 'View' > 'Message' > 'Raw Source'.
    - Copy all the text from this window.

## **Downloading and Documenting Email Chains**

**Objective**: To preserve the entire email chain, including the content and any attachments, in its original format.  
 **Email Chain Documentation:**

| **Email Subject** | **Downloaded File Name** | **Storage Location** |
| --- | --- | --- |
|  |  |  |

***Instructions for Downloading Email Chains***:

* + **Gmail**:
    - Open the email.
    - Click on the three vertical dots in the upper right corner.
    - Select "Download message" to save the email as an .eml file.
  + **Outlook (Web Version)**:
    - Open the email.
    - Click on the three dots ('More actions') in the top menu.
    - Choose "Download as .eml".
  + **Yahoo Mail**:
    - Yahoo Mail does not support downloading the entire email directly. You'll need to save the content and attachments separately.
  + **Apple Mail:**
    - Open the email in Apple Mail.
    - Go to 'File' in the menu bar and select 'Save As'.
    - Choose 'Raw Message Source' to save the email as an .eml file.
* **Documenting the Download**:
  + Once the email chain is downloaded, record the file name and storage location in the table below for easy reference.

### **Additional Resources**

1. **Tools for Screenshots**:

* Snipping Tool / Snip & Sketch (Windows): Built-in tools for capturing screenshots.
* Command + Shift + 4 (Mac): Shortcut for capturing a portion of the screen.
* Lightshot: A free, easy-to-use screenshot tool available for both Windows and Mac.

1. **Antivirus Scanning Software:**

* **VirusTotal**: A free online service that analyzes files and URLs for viruses, worms, trojans, and other kinds of malicious content detected by antivirus engines and website scanners. It's useful for checking suspicious email attachments and links. [VirusTotal Website](https://www.virustotal.com/)
* **Avast Free Antivirus**: A free antivirus program for Windows and Mac.
* **Malwarebytes**: Offers both free and premium plans for comprehensive virus and malware protection.

1. **Online Resources for Understanding Email Headers:**

* MXToolBox Email Header Analyzer: A free tool that helps analyze email headers and identify the source.
* VirusTotal https://www.virustotal.com/
* Google Workspace Learning Center: Provides insights on understanding Gmail headers.

### **Conclusion and Reminder**

* Importance of Documentation: Always prioritize the accurate and detailed documentation of evidence. This ensures reliability and usefulness in any subsequent investigations or legal proceedings.
* Regular Updates: Cybersecurity and communication technologies are rapidly evolving. Stay informed about new tools and best practices to ensure that your incident response approach remains effective.

### **Legal and Ethical Considerations**

* Privacy Laws: Be mindful of privacy and data protection laws, such as GDPR in Europe or HIPAA in the United States, when handling personal or sensitive data.
* Ethical Handling: Use the collected data only for legitimate purposes such as investigation and recovery. Avoid unauthorized sharing or misuse of sensitive information.
* Consent and Disclosure: Understand the legal requirements for consent and disclosure, especially when recording communications or accessing someone else's email with or without their permission.