# **Business Email Compromise (BEC) Incident Discovery Evidence Collection Part of the BEC Incident Response Toolkit**

### **Introduction**

### In the wake of a Business Email Compromise (BEC) incident, the collection and preservation of evidence upon discovery 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.

### **Initial Incident Details**

**Purpose**: This section is designed to capture the essential details of the BEC incident as soon as it is discovered. Accurate and timely documentation here is crucial for effective response and recovery.

#### **Incident Name**

| Incident Name: |  |
| --- | --- |

***Description:*** *Assign a unique name to the incident for easy reference.****Instructions:*** *Use a naming convention that combines the date of discovery and a unique identifier. For example, "BEC\_23Nov2023\_001". This helps in tracking and referring to the incident in communications and reports.*

#### **Date and Time of Discovery**

| Date: |  |
| --- | --- |
| Time |  |

***Description:*** *Record the exact date and time when the BEC incident was first noticed.*

***Instructions:*** *Use the format DD/MM/YYYY, HH:MM (24-hour clock).*

#### **Initial Point of Contact**

| Name: |  |
| --- | --- |
| Contact Information: |  |
|  | |
|  | |
|  | |

***Description****: Identify who discovered the incident and provide their full name and contact details.*

***Instructions****: Include job title if applicable. Provide email and phone number for follow-up communications.*

#### **Suspected Date and Time of Compromise**

| Date of Compromise ( (DoC): |  |
| --- | --- |
| Time of Compromise: |  |

***Description****: Estimate when you believe the BEC scam first occurred.****Instructions****: If exact timing is unknown, provide a best estimate. Use the format DD/MM/YYYY, HH:MM (24-hour clock).*

#### **Location of Discovery**

| Location: |  |
| --- | --- |
|  | |
|  | |
|  | |
|  | |
|  | |

***Description****: Specify the location where the incident was discovered.****Instructions****: This can be an office location, remotely while working from home, etc. Include city and country if relevant.*

#### **Description of Discovery**

***Description****: Briefly describe how the incident was discovered.*

***Instructions****: Include any immediate actions taken upon discovery. This could be noticing an unusual email, an unexpected transaction alert, etc.*

| Describe the Discovery : |  |
| --- | --- |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |

#### **Initial Assessment**

***Description****: Provide an initial assessment of the incident's impact.****Instructions****: Consider aspects such as financial loss, data compromise, operational disruptions, etc. Note if full impact is not yet known.*

| Preliminary Impact Assessment: |  |
| --- | --- |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |

#### **Actions Taken Upon Detection of BEC Incident**

***Description****: Detail any immediate security measures taken upon discovering the BEC incident, such as enabling MFA, changing security questions, or updating passwords.*

***Instructions****: You can also use this space to document last password changes made and if there are other applications that house your passwords like password managers.*

| List Actions Taken : |  |
| --- | --- |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |
|  | |

*Note: It's important to fill out this section as completely and accurately as possible. If certain information is not immediately available, note this and return to complete the section as soon as the information is obtained.*