Phishing Playbook
Version 1.0

Purpose

To help level-one SOC analysts provide an appropriate and timely response to a phishing incident

Using this playbook

Follow the steps in this playbook in the order in which they are listed. Note that steps may overlap.

Step 1: Receive phishing alert

The process begins when you receive an alert ticket indicating that a phishing attempt has been detected.
Phishing with Malicious Attachment

Step 2: Evaluate the alert

Upon receiving the alert, investigate the alert details and any relevant log information. Here is a list of some of the information you should be evaluating:

1. **Alert severity**
    - **Low**: Does not require escalation
    - **Medium**: May require escalation

    High: Requires immediate escalation to the appropriate security personnel

    Severity: Medium
2. **Receiver details**
    - The receiver's email address
    - The receiver's IP address

    <hr@inergy.com> <176.157.125.93>

3. **Sender details**
    - The sender's email address
    - The sender's IP address

Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>

Subject line Re: Infrastructure Egnieer role

4. **Message body** Dear HR at Ingergy,

    I am writing for to express my interest in the engineer role posted from the website.

There is attached my resume and cover letter. For privacy, the file is password protected. Use the password paradise10789 to open.

Thank you,

Attachments or links. Attachment: filename="bfsvc.exe"

5.

Step 3.0: Does the email contain any links or attachments?

Phishing emails can contain malicious attachments or links that are attempting to gain access to systems. After examining the details of the alert, determine whether the email contains any links or attachments. If it does, **do not** open the attachments or links and proceed to **Step 3.1**. If the email does not contain any links or attachments, proceed to **Step 4**.

Suspicious file hash or attachment

Step 3.1: Are the links or attachments malicious?

✔ Yes — the file hash is malicious.

Step 3.2: Update the alert ticket and escalate

Escalation not required because:

- The threat was contained automatically
- No post-delivery activity or endpoint impact is observed

Escalation is typically reserved for:

- Successful execution
- Credential compromise
- Lateral movement or persistence indicators

Step 4: Close the alert ticket

✔ **Close the ticket as "Blocked / No Impact"**, not a false positive.

Note: If a malicious attachment is confirmed but was quarantined or blocked prior to user interaction, and logs confirm no execution or system changes, the alert may be closed as "Blocked / No Impact" without escalation.

Summary:

A phishing email containing a malicious executable attachment (bfsvc.exe) was

detected and quarantined by email security controls. The attachment hash was confirmed malicious via threat intelligence sources. Endpoint and email logs show no evidence of user interaction, file execution, registry modification, or process creation. The threat was blocked prior to execution, and no system impact was observed.

Resolution:

No further action required. Alert closed as **phishing attempt successfully mitigated**.

Phishing Flowchart (Version 1.0)