**Task 3: Identify Phishing Emails**

**OBJECTIVE**

Task: Recognize and handle phishing attempts.

**Details:**

Review common signs of phishing emails (e.g., suspicious links, urgent messages). Practice identifying and reporting phishing emails.

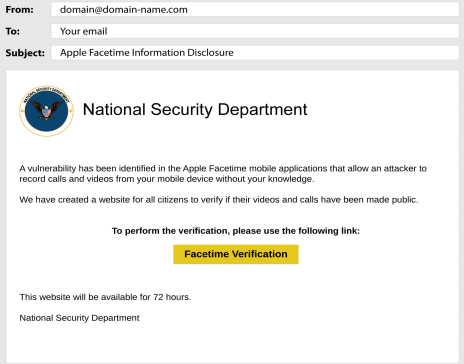
**STEPS:**

1. **Common Signs of Phishing Emails:** Phishing emails often contain specific red flags. Look for the following indicators:

|  |  |
| --- | --- |
| **Phishing Indicator** | ***Description*** |
| **Suspicious Sender** | Check if the sender's email address looks unusual  (e.g., support@amaz0n.com instead of  support@amazon.com). |
| **Generic Greetings** | Emails that start with “Dear Customer” or “Dear  User” instead of your name. |
| **Urgent or**  **Threatening**  **Language** | Phrases like "Act now" or "Your account will be  suspended!" to create panic and prompt  immediate action. |
| **Unexpected**  **Attachments** | Files with unfamiliar formats or unusual names  may contain malware. |
| **Links to Fake**  **Websites** | Hover over links to check the URL for  discrepancies (e.g., http://fakebank.com/login) |
| **Spelling and**  **Grammar Errors** | Many phishing emails have poor spelling or  awkward phrasing. |
| **Requests for**  **Personal**  **Information** | Legitimate organizations rarely ask for sensitive  information via email. |

2. **Analyze Sample Phishing Emails:**

Below is an example phishing email, which shows several red flags:



**Key Red Flags in This Email:**

1. **Suspicious Sender Email:**

* The sender email is from a generic domain: domain@domain-name.com. Official organizations, such as the "National Security Department," would use a legitimate domain (e.g., .gov or .mil).

**ii. Unrealistic Sender Organization:**

* The email claims to be from the "National Security Department," which is

not a real entity. Legitimate emails would use correct governmental titles

like "Department of Homeland Security."

**iii. Urgency and Fear Tactics:**

* The email uses fear tactics, claiming there's a vulnerability in Apple

FaceTime, which might expose private videos and calls. Phishing emails

often try to create urgency to make victims act without considering the

situation properly.

**iv. Suspicious Verification Link:**

* The email directs the user to click a "FaceTime Verification" link to see if

their data is exposed. This is a common phishing method to redirect

victims to malicious sites designed to steal sensitive information.

**v. Unprofessional Appearance:**

* The email lacks professionalism. Official government communications are

generally clear, well-formatted, and free of vague requests for "verification."

**vi. No Personalization:**

* The email does not address the recipient by name (e.g., "Dear [Your

Name]"), which is a common phishing tactic used when targeting a large

number of recipients.

**3. Report Phishing:**

* To report these types of emails, use the "Report Phishing" feature in your email

client or forward them to the legitimate organization's security team.

* When reporting, attach any critical information, but avoid exaggerating or adding

unnecessary details.