Task 3

Identify Phishing Emails

➢ Objective

Recognize and handle phishing emails by identifying common red flags and reporting them safely.

➢ Steps

1: Review of Common Signs of Phishing:

- I visited the Digital Care Hub website, where they outline "The 12 Signs of Phishing."
- Some of the important signs include:
  - Suspicious email addresses.
  - Urgency or fear tactics.
  - Unsolicited attachments or links.
  - Poor grammar or unprofessional language.
- Below are showcasing examples of phishing signs:

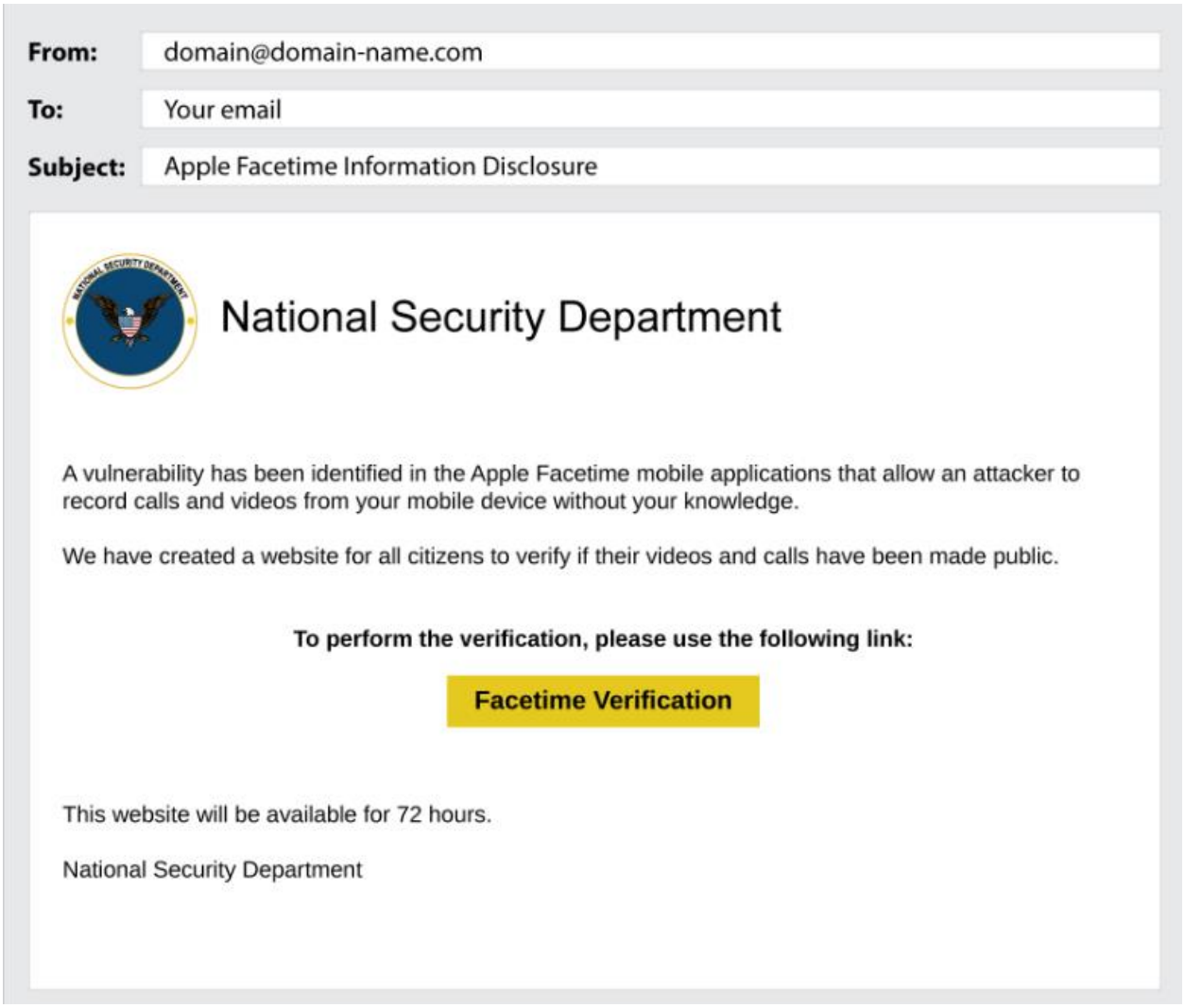
1. **Suspicious Email Addresses:**
   - Ensure the sender's email address matches the domain of a legitimate organization and isn't spoofed.
2. **Urgency or Fear Tactics:**
   - Be cautious of emails that create a sense of urgency or pressure you into immediate action, like warnings of security breaches or urgent requests for personal data.
3. **Unsolicited Attachments or Links:**
   - Avoid opening attachments or clicking on links from unknown or unexpected sources, as these are common methods to deliver malware or redirect to fraudulent sites.
4. **Poor Grammar or Unprofessional Language:**
   - Legitimate businesses typically send professionally written communications. Obvious errors or inconsistent formatting can be a strong indicator of phishing.

Showcasing Examples: Images with examples of phishing signs can be especially helpful for recognizing patterns and comparing suspicious emails to verified red flags. These visual aids often illustrate telltale signs of phishing email like:

- Misleading URLs.

- Fake login pages.
- Requests for sensitive information such as passwords or financial details.

2: Analyze Sample Phishing Emails: Below is an example phishing email, which shows several red flags:



2: Key Red Flags in This Email:

i. **Suspicious Sender Email**:

- The sender's 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**:

- 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 many 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.