TASK-2

Detailed Report on Phishing Email

Sample Email Reference
Subject: "Black Friday Deals Are Available!"
Sender Display Name: "Amazon Shop"
Sender Email Address: "do-not-reply@apponline.info"
Brand Imitated: Amazon (amazon.com logo and layout)

- -
Step 1: Obtain a Sample Phishing Email
- -

For this task, a suspicious promotional email pretending to be from Amazon was selected as the phishing sample. The email claims that “Black Friday Deals Are Available!” and uses Amazon’s logo and formatting to appear legitimate. The purpose of choosing this email is to analyze how attackers imitate well-known brands to trick users into clicking malicious links or providing sensitive information.

Key observations:
- The email uses Amazon’s logo and website style.
- It mentions “Black Friday Deals” to attract attention during a popular sale period.
- The email is formatted like an official promotional newsletter.

Conclusion for Step 1:
A realistic phishing email imitating Amazon was obtained and will be used for further technical and content-based analysis.

- -
Step 2: Examine Sender’s Email Address for Spoofing
- -

The sender details shown in the email header area are:
- Display Name: Amazon Shop
- Email Address: do-not-reply@apponline.info

Legitimate Amazon promotional emails usually come from domains such as:
- @amazon.com
- @amazon.in
- @amazon.co.uk (or other regional Amazon domains)

In this email, the domain used is “apponline.info”, which does not match any official Amazon domain. Attackers often use look-alike or completely unrelated domains to mislead users who only read the display name (Amazon Shop) and ignore the actual email address.

Additional risk indicators:
- The domain name “apponline.info” is generic and unrelated to Amazon.
- The presence of a warning banner (“Mail can’t verify the authenticity of attached messages”) suggests that the mail system itself considers the message suspicious.

Conclusion for Step 2:
The sender’s email address is not from an official Amazon domain and is a strong indication of email spoofing and phishing.

- -

Step 3: Check Email Headers for Discrepancies

- -

(Assuming full technical headers are viewed using an email client or an online header analyzer.)

Typical header checks:
- Received: lines – to see the path the email took.
- From: and Return-Path: – to detect mismatched sending domains.
- SPF, DKIM, and DMARC results – to verify if the domain authorized the sender.

Likely discrepancies for this email:
- The “From” address shows “apponline.info” rather than an official Amazon domain.
- SPF or DKIM may fail or be missing, meaning the email server is not authorized to send on behalf of Amazon.
- The Return-Path or Reply-To fields may point to a different domain, used by attackers to collect responses or credentials.

Conclusion for Step 3:
Header analysis would likely show that the email was not sent from Amazon’s legitimate servers and fails authentication checks, confirming it as a phishing attempt.

- -

Step 4: Identify Suspicious Links or Attachments

- -

The email contains multiple links, including:
- “Black Friday Deals Are Here”
- “product link” entries for each listed item
- “Sign up for Amazon Prime”
- “For More Great Deals”

Even though the visible text suggests Amazon deals, in a phishing email these links usually point to malicious or fake websites that:
- Imitate Amazon’s login page to steal usernames, passwords, or OTPs.
- Collect payment card details or personal information.
- Install malware if files are downloaded.

There are no obvious file attachments shown in the screenshot, but any attachment in such emails would be highly suspicious (e.g., .zip, .exe, or malicious documents).

Conclusion for Step 4:
The high number of promotional links encouraging the user to click, especially on “Sign up” and “Deals” links, is a major phishing indicator. All links should be treated as untrusted and not clicked.

- -

Step 5: Look for Urgent or Persuasive Language in the Email Body

- -

The email uses marketing and urgency-based language such as:
- “Black Friday 2020 store is officially open and the deals are live!”
- “Buy today, Save $50”
- “Sign up now and you will get a free 30-day trial period.”

This type of wording is designed to create:

- A sense of urgency (limited-time offers, Black Friday rush).
- Fear of missing out (FOMO) so that users act quickly without verifying authenticity.

Even though promotional emails from legitimate companies also use urgency, when combined with a suspicious sender address and unknown domain, it becomes a strong phishing sign.

Conclusion for Step 5:
The email uses urgency and attractive offers to pressure the user into acting quickly, which is a common social engineering technique in phishing campaigns.

- -
Step 6: Note Any Mismatched or Hidden URLs (Hover to See Real Link)
- -
In a real analysis, the next step would be to hover the mouse over each hyperlink (without clicking) to view the actual destination URL in the status bar of the email client or browser.

Expected findings in a phishing email:
- The displayed text might say something like “amazon.com” or “Black Friday Deals Are Here”, but the real URL could be:
  - A completely different domain (e.g., http://malicious-site.xyz/login)
  - A look-alike domain (e.g., http://amaz0n-deals.com or http://amazon.verify-login.info)
- The URL may be very long, with tracking parameters or random strings to hide the main domain.

Because the screenshot does not show the real URLs, we assume (based on the suspicious sender domain) that the links do not lead to official Amazon pages.

Conclusion for Step 6:
The links are likely mismatched or lead to non-Amazon domains. Users must always check the real URL before clicking and only enter credentials on official domains such as https://www.amazon.com or the official Amazon app.

- -
Step 7: Verify Presence of Spelling or Grammar Errors
- -
From the visible text, the grammar appears mostly correct and the content is written in standard marketing language. However, attackers sometimes copy large parts of legitimate content to look authentic.

Important points:
- Not all phishing emails contain obvious spelling or grammar mistakes.
- Even when language looks professional, other indicators (sender domain, unknown links, and verification warnings) can still reveal phishing.

Conclusion for Step 7:
This sample does not show obvious spelling or grammar errors, proving that lack of mistakes does NOT guarantee the email is safe. Other technical and contextual checks remain essential.

- -
Step 8: Summarize Phishing Traits Found in the Email
- -
Based on the above analysis, the following phishing indicators were identified:

1. Suspicious Sender Domain

- The email address “do-not-reply@apponline.info” does not match official Amazon domains such as “@amazon.com”.

2. Brand Impersonation
- Uses Amazon logo, name, and layout to create trust and trick users.

3. System Warning Banner
- The mail system displays a warning that it cannot verify the authenticity of the message, which is a strong red flag.

4. Multiple Action-Oriented Links
- Many links push the user to click for deals or to “Sign up for Amazon Prime,” increasing the chance of leading the user to a fake site.

5. Urgency and Attractive Offers
- Limited-time Black Friday deals and free trial messages are used to pressure users into quick action.

6. Potential Mismatched URLs
- Although not visible in the screenshot, phishing emails typically hide malicious URLs behind legitimate-looking link text.

7. Generic Greeting
- The email addresses the recipient as “Dear Amazon.com Customer” instead of using their real name, which is often a sign of mass phishing campaigns.

Overall Conclusion:

Combining all these indicators, the analyzed email is highly likely to be a phishing email designed to impersonate Amazon, lure users with Black Friday deals, and trick them into clicking malicious links or providing sensitive information. Users should delete such emails, avoid clicking any links, and report them to their email provider or the impersonated organization’s security team.