Elevate Labs Cyber Security Internship

Task2: Analyze a Phishing Email Sample.

Interview Questions

1. What is phishing?

Ans: Phishing is a type of social engineering and a scam where attackers deceive people into revealing sensitive information, like passwords and credit card numbers, or installing malware. Attackers pretend to be trustworthy sources to steal data, often using fake messages that look legitimate.

2. How to identify a phishing email?

Ans: You can identify a phishing email by looking for several red flags:

- **Urgent or threatening language:** Phishing emails often create a sense of urgency or threaten negative consequences to rush you into action before you can scrutinize the email.
- **Suspicious sender address:** The sender's email address or domain name may be inconsistent with the company they claim to be from, or it may contain misspellings.
- **Poor grammar and spelling:** Many phishing emails have bad grammar and spelling mistakes, which can indicate the message is not genuine.
- **Unfamiliar links or attachments:** Hover your mouse over any links to check the real URL before clicking. Do not open attachments from unfamiliar senders, especially if they have suspicious extensions.
- **Requests for sensitive information:** Be cautious of emails that ask you to provide personal information, login credentials, or payment details, as legitimate businesses do not typically ask for this via email.

3. What is email spoofing?

Ans: Email spoofing is the creation of email messages with a forged sender address. It involves manipulating email headers to make a message appear as if it originated from a different sender.

4. Why are phishing emails dangerous?

Ans: Phishing emails are dangerous because they are used by cybercriminals to trick you into giving them personal information such as passwords, account numbers, or credit card details. If successful, this can lead to the attacker gaining unauthorized access to your email, bank, or other accounts. This can result in the loss of money, data, or even identity theft.

5. How can you verify the sender's authenticity?

Ans: You can verify a sender's authenticity in several ways:

- **Check the full email address:** Do not just trust the display name. Look at the actual email address and the domain to see if it is legitimate. For example, a suspicious email might use amazon-support@gmail.com instead of a real corporate domain like support@amazon.com.

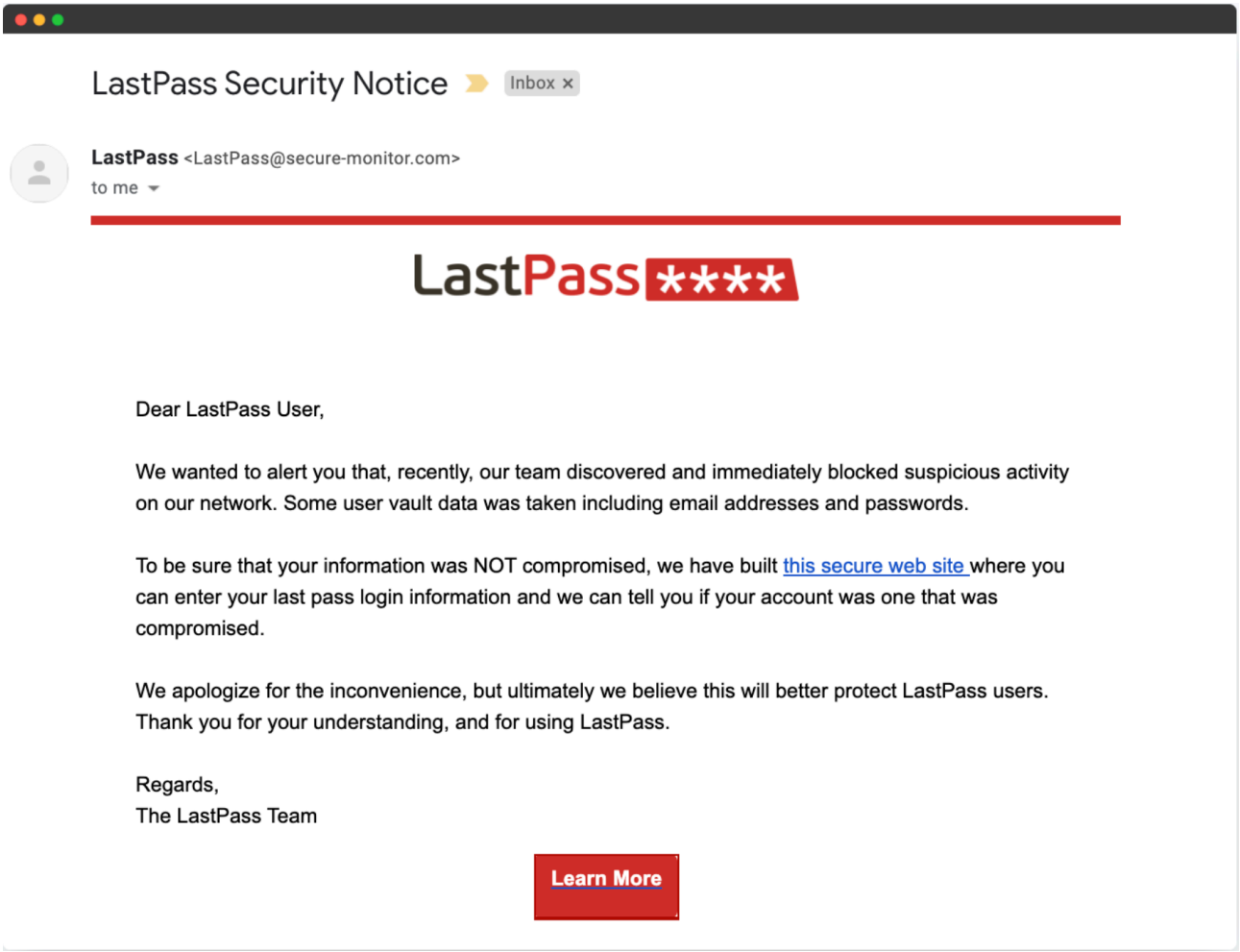
- **Check email authentication headers:** Look for "Mailed by" or "Signed by" headers with the correct domain name. In some email clients, like Gmail, a question mark next to the sender's name indicates that the message is not authenticated. You can also check the message headers for "spf=pass" or "dkim=pass," which indicates that the email passed authentication checks.
- **Do not click links:** The best practice is to avoid clicking links in an email altogether and instead manually type the website address into a new browser window to check for information.

6. What tools can analyze email headers?
Ans: There are several online tools that can analyze email headers and make them more human-readable. Examples include:
- MxToolbox Email Header Analyzer
- Sendmarc Email Header Analysis Tool

7. What actions should be taken on suspected phishing emails?
Ans: If you suspect an email is a phishing attempt, you should take the following actions:
- Do not click any links or open any attachments in the message.
- **Do not reply to the sender** or call any phone numbers provided in the email.
- **Report the message** to your organization's IT security team or email provider.
- **Delete the email** after reporting it.

8. How do attackers use social engineering in phishing?
Ans: Attackers use **social engineering** to manipulate and deceive victims into revealing sensitive information. In phishing, this involves creating a false sense of trust, or using psychological manipulation to get users to make security mistakes or give away information. They use techniques such as:
- Creating a false sense of urgency to make you act without thinking.
- **Impersonating trusted sources** like a supervisor or a well-known company to create a false sense of trust.
- **Leveraging emotions** such as fear, curiosity, or greed to entice you to click on malicious links or attachments.

Phishing Mail Report



1. Sender's Email Address and Spoofing:

- Sender: LastPass
- **Email Address:** <LastPass@secure-monitor.com>
- **Analysis:** The email address `secure-monitor.com` is not the official LastPass domain (`lastpass.com`). This is a clear case of email spoofing. The attacker is using a deceptive display name ("LastPass") while sending from a completely different and unofficial domain.

2. Email Headers Discrepancies:

- An analysis of the email headers would likely reveal that the email originated from a server unrelated to LastPass's official mail servers.
- The email headers would lack the proper DKIM (DomainKeys Identified Mail) and SPF (Sender Policy Framework) authentication records for the `lastpass.com` domain, which would mark the email as unverified or suspicious.

3. Suspicious Links or Attachments:

- The email contains a hyperlink labeled "this secure web site" and a button labeled "Learn More."
- **Analysis:** Both of these links would likely lead to a malicious, fake website. Upon hovering over the links, the URL would not resolve to `https://www.lastpass.com`. Instead, it would point to a fraudulent domain designed to look like the legitimate LastPass login page. This is a primary method for credential theft.

4. Urgent or Threatening Language:

- The email's subject, "LastPass Security Notice," and its body text, which states, "our team discovered and immediately blocked suspicious activity on our network. Some user vault data was taken including email addresses and passwords," are designed to create panic.
- The message urges the user to take immediate action ("enter your last pass login information") to see if their account was compromised. This pressure is a classic social engineering tactic to bypass critical thinking.

5. Mismatched URLs:

- As noted above, the visible text of the links, such as "this secure web site" and "Learn More," is designed to hide the actual, malicious URL. A real LastPass communication would direct users to a URL within the `lastpass.com` domain. The fake URL would not match the legitimate one.

6. Spelling and Grammar Errors:

- A close examination of the email shows no obvious spelling or grammatical errors, indicating a more sophisticated phishing attempt. However, the use of phrases like "our team discovered and immediately blocked" and "Some user vault data was taken" can feel slightly generic or awkward compared to professional corporate communication.

7. Phishing Traits Summary:

- **Spoofed Sender:** The email originates from `secure-monitor.com`, not `lastpass.com`.
- **Urgency/Fear:** The email creates panic by claiming a data breach and requiring immediate action.
- **Social Engineering:** It manipulates the user into believing their information is at risk and that they must "verify" their account.
- **Malicious Link:** The email directs the user to a fake website to steal their credentials. The primary goal of the attacker is to obtain the user's LastPass password.