Sample Phishing Email

Subject: Immediate Action Required: Your Amazon Account is at Risk!

From: Amazon Support <support@amazon-secure.net>

To: [Recipient's Email]

Body:

Dear Valued Customer,

We have noticed suspicious activity on your Amazon account. Your account may be compromised! To secure your account, you must update your login credentials within 24 hours, or your account will be suspended.

Click here to update your information:

[Secure Your Account] (http://amazon-login-secure.com/update)

If you did not request this, please contact our support team urgently.

Sincerely,

Amazon Security Team

[Attachment]: Account_Security_Update.pdf

Analysis

1. Obtain a Sample Phishing Email

The sample above is a fictional but realistic phishing email, modeled after common examples from cybersecurity training resources (e.g., Terranova Security, Microsoft 365 Defender). It mimics an Amazon-themed phishing attempt, a frequently spoofed brand due to its widespread recognition.

2. Examine Sender's Email Address for Spoofing

- **Sender's Email**: <support@amazon-secure.net>

- **Analysis**: The email address includes "amazon" in the domain, which may appear legitimate at first glance. However, legitimate Amazon emails typically originate from <@amazon.com> or regional domains like <@amazon.co.uk>. The domain <amazon-secure.net> is not an official Amazon domain. A WHOIS lookup (using tools like those referenced in web resources) would likely confirm it's unrelated to Amazon. The display name "Amazon Support" is generic and often used to mask fraudulent addresses, indicating spoofing.

3. Check Email Headers for Discrepancies (Using Online Header Analyzer)

- **Process**: Email headers reveal the email's origin, including "From," "Return-Path," "Received," and authentication fields (SPF, DKIM, DMARC). Headers can be accessed via email clients (e.g., Gmail's "Show Original") and analyzed with tools like MxToolbox or Google MessageHeader.

- **Hypothetical Header Example**:

```
From: Amazon Support <support@amazon-secure.net>

Return-Path: <info@randomserver.biz>

Received: from randomserver.biz (IP: 203.0.113.5)

SPF: Fail (sender not authorized)

DKIM: None

DMARC: Fail
```

```

- **Analysis**:

  - **Mismatched Domains**: The “From” field (<support@amazon-secure.net>) differs from the “Return-Path” (<info@randomserver.biz>), suggesting the email was sent from an unauthorized server.

  - **SPF Failure**: The SPF check fails because the sending server (randomserver.biz) isn’t authorized to send on behalf of amazon-secure.net.

  - **No DKIM Signature**: Legitimate companies like Amazon use DKIM for authenticity. Its absence is a red flag.

  - **Suspicious IP**: The IP (203.0.113.5) could be checked via tools like TalosIntelligence to identify associations with spam or malicious activity. These discrepancies confirm the email’s fraudulent nature.

#### 4. Identify Suspicious Links or Attachments

- **Link**: “Secure Your Account” points to <http://amazon-login-secure.com/update>.

- **Attachment**: “Account_Security_Update.pdf”

- **Analysis**:

  - **Link**: The URL <amazon-login-secure.com> is not Amazon’s official domain (<amazon.com>). This is a spoofed domain designed to mimic the legitimate one, likely leading to a phishing page to steal credentials.

  - **Attachment**: The file “Account_Security_Update.pdf” appears harmless but could contain embedded malware or macros, especially if it prompts the user to enable content. Unsolicited PDFs from unverified sources are suspicious, as they may exploit vulnerabilities or trick users into downloading malware.

#### 5. Look for Urgent or Threatening Language in the Email Body

- **Language**: Phrases like “suspicious activity,” “account may be compromised,” “update within 24 hours,” and “account will be suspended” are used.
```

- **Analysis**: These phrases create urgency and fear, pressuring the recipient to act quickly without verifying the email's legitimacy. This tactic, common in phishing emails, exploits emotional responses to bypass rational scrutiny, as noted in cybersecurity training materials.

6. Note Any Mismatched URLs (Hover to See Real Link)

- **Displayed Link Text**: "Secure Your Account"

- **Actual URL**: <http://amazon-login-secure.com/update>

- **Analysis**: Hovering over the link reveals a URL that does not match Amazon's official domain (<amazon.com>). The spoofed domain <amazon-login-secure.com> is designed to deceive users into entering credentials on a fake login page. This mismatch is a clear phishing indicator.

7. Verify Presence of Spelling or Grammar Errors

- **Text Analysis**: The email is well-written with no obvious spelling or grammar errors. However, the generic greeting "Dear Valued Customer" is a red flag, as legitimate companies like Amazon typically use the recipient's name for personalization.

- **Analysis**: While the lack of errors suggests a sophisticated phishing attempt (potentially AI-generated, as modern phishing emails can be polished), the generic greeting indicates a lack of personalization, a common phishing trait.

8. Summarize Phishing Traits Found in the Email

The email exhibits multiple phishing characteristics:

- **Spoofed Sender Address**: The email address (<support@amazon-secure.net>) uses a non-official domain, mimicking Amazon's branding.

- **Header Discrepancies**: Mismatched "From" and "Return-Path" domains, SPF and DMARC failures, and no DKIM signature indicate a fraudulent origin.

- **Suspicious Link**: The link leads to a spoofed domain (<amazon-login-secure.com>) designed to steal credentials.

- **Suspicious Attachment**: The PDF file could harbor malware or malicious macros, especially as it's unsolicited.

- **Urgent/Threatening Language**: Terms like “compromised” and “suspended” create panic to prompt immediate action.

- **Mismatched URL**: The link’s displayed text hides a fraudulent destination URL.

- **Generic Greeting**: “Dear Valued Customer” lacks personalization, unlike legitimate corporate emails.

Awareness of Phishing Tactics and Email Threat Analysis Skills

This analysis demonstrates key skills for identifying phishing emails, critical for cybersecurity awareness:

- **Sender Verification**: Checking the email address and domain against official sources to detect spoofing.

- **Header Analysis**: Using tools to inspect headers for authentication failures and mismatched origins.

- **Link and Attachment Scrutiny**: Identifying spoofed URLs and suspicious file types to avoid phishing pages or malware.

- **Language Evaluation**: Recognizing urgent or threatening language as a manipulation tactic.

- **Attention to Detail**: Noting generic greetings or subtle cues like mismatched URLs to question legitimacy.

Recommendations for Training:

- **Employee Education**: Conduct workshops using real-world phishing examples to teach header analysis, link inspection, and language evaluation.

- **Simulation Exercises**: Use phishing simulation tools (e.g., KnowBe4) to test employees’ ability to spot phishing emails in a controlled environment.

- **Tool Familiarity**: Train staff on using header analyzers and URL checkers for hands-on threat analysis.

- **Action Protocols**: Emphasize never clicking links or opening attachments from unsolicited emails and verifying requests via official channels (e.g., navigating to <amazon.com> directly).