**Phishing Attempt #1: Suspicious Link in an Email**

**Email Details:**

* **Sender:** services@amazn.com (Note the misspelling of "Amazon")
* **Subject:** “Your account has been suspended, action required!”
* **Body:**  
  "Dear customer, your Amazon account has been suspended due to suspicious activity. Please click the link below to verify your identity and reactivate your account."
* **Link:** http://amazn-support.com/account-recovery (A fake domain meant to resemble Amazon)

**Analysis:**

* **Suspicious Domain:** The sender’s email domain, "amazn.com", is a clear red flag as it is misspelled. Legitimate companies like Amazon use their official domain, "amazon.com".
* **Urgency and Fear:** The message uses urgent language to instill fear, pressuring the recipient to act quickly. This is a common tactic used in phishing emails.
* **Mismatched URL:** The link provided points to "amazn-support.com", which is not a valid Amazon domain. Always hover over links before clicking to verify their legitimacy.
* **Conclusion:** This is a clear phishing attempt designed to steal personal information by directing the recipient to a fake website.

**Phishing Attempt #2: Unsolicited Email Requesting Personal Information**

**Email Details:**

* **Sender:** security-update@paypal-services.com
* **Subject:** “PayPal: Please confirm your account details.”
* **Body:**  
  "Dear valued customer, to ensure the security of your PayPal account, we need you to confirm your details by clicking the link below. Failure to do so will result in account suspension."
* **Link:** http://paypal-services.com/security/verify

**Analysis:**

* **Sender’s Domain:** While this appears to come from "PayPal", the domain used, "paypal-services.com", is not PayPal’s official domain, which is "paypal.com". Scammers often create similar-looking domains to trick users.
* **Unsolicited Request:** PayPal will never ask you to provide sensitive information via email. Any unsolicited request to confirm personal details is highly suspicious.
* **Conclusion:** This is a phishing attempt aimed at collecting personal and financial details by imitating a trusted company.

**Phishing Attempt #3: Attachment with Malware**

**Email Details:**

* **Sender:** hr@recruitment.com
* **Subject:** “Your Job Application Status.”
* **Body:**  
  "Congratulations! Your job application has been reviewed. Please download the attached document for further instructions regarding your interview schedule."
* **Attachment:** interview\_schedule.pdf

**Analysis:**

* **Suspicious Attachment:** Receiving an unsolicited attachment is always risky. In this case, although the file appears to be a PDF, phishing attacks often hide malware within attachments, and PDFs can also contain harmful scripts.
* **No Prior Contact:** This email was received without any prior interaction or job application. This is suspicious as legitimate job offers are not sent out of the blue.
* **Conclusion:** This is likely a phishing attempt using a malicious attachment to infect the system.

**Phishing Attempt #4: Fake Billing Email**

**Email Details:**

* **Sender:** billing@spotify-bills.com
* **Subject:** “Action Required: Your Spotify Payment Failed.”
* **Body:**  
  "Dear customer, your recent payment for Spotify Premium has failed. Please click the link below to update your billing details and avoid service interruption."
* **Link:** http://spotify-bills.com/update-payment

**Analysis:**

* **Suspicious Domain:** The sender's email domain, "spotify-bills.com", is not associated with the official Spotify website.
* **Urgent Request:** Phishing emails often create a sense of urgency. In this case, the user is pressured to update billing information, which could lead to stealing credit card details.
* **Legitimate Emails:** Real companies like Spotify do not send such billing requests via random domains, and the official Spotify billing page is always accessible through their website.
* **Conclusion:** This is a phishing attempt designed to steal payment details by impersonating Spotify.