**Day-2 (23/9/25)**

**Task 1:** Scan Analyze a Phishing Email Sample.

**Objective:** Identify phishing characteristics in a suspicious email sample.

**Deliverables**: A report listing phishing indicators found

**Tools & Environment**

 OS**:** Windows 10

 Tool**:** Email client or saved email file (text), free online header analyzer (Mx toolbox, Aspose).

**Source:**  Phishing mails samples from “LinkSec Phishing Templates”.

## Process (step – by – step walkthrough)

**Step 1: Obtain a sample phishing emails (many free samples online).**

Collecting of pre‑made mail samples from a trusted training source (e.g., PhishTank, email security blogs). So you can practice spotting phishing indicators without any risk. And stored in folder emails in text folder (Those emails are stored in .txt format) for easily using in email header analyzer.

**Step 2: Examine sender's email address for spoofing**.

In your phishing sample, find the **display name** (e.g., “Amazon Web Services”) and the **actual email address** next to it.

* Example:

**From: "Amazon Web Services" <aws-support@secure-aws-login.com>**

 Display **name:** Amazon Web Services

 Actual **address:** aws-support@secure-aws-login.com

While we comparing with official website , we spot few errors and we can easily identifiy some phishing indicators. Check if it matches the official domain of the company:

* **AWS official domain:** amazon.com or aws.amazon.com
* **Fake domain:** secure-aws-login.com (looks similar but is not official)

My Findings for 16 email phishing samples Step 2 record in table :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sample Name | Display Name | Actual Email Address (from header) | Official Domain Address | Domain Match? |
| amazon-web-services-aws-aws-account-verification-request-modified.txt | AWS Support Team | aws-support@secure-aws-login.com | amazon.com / aws.amazon.com | No |
| amazon-web-services-aws-exclusive-100-amazon-gift-card-modified.txt | AWS Rewards Team | [rewards@aws-giftcard-offer.com](mailto:rewards@aws-giftcard-offer.com) | amazon.com / aws.amazon.com | No |
| bluejeans-free-bluejeans-premium-subscription-offer-modified.txt | BlueJeans Team | offers@bluejeans-premium-free.com | bluejeans.com | No |
| bluejeans-profile-viewing-notification-modified.txt | BlueJeans Team | notify@bluejeans-profile-alert.com | bluejeans.com | No |
| cisco-webex-urgent-password-reset-required-email-modified.txt | Cisco Webex Security Team | [security@webex-login-reset.com](mailto:security@webex-login-reset.com) | cisco.com / webex.com | No |
| cisco-webex-urgent-webex-account-verification-request-modified.txt | Cisco Webex Security Team | [verify@webex-secure-alert.com](mailto:verify@webex-secure-alert.com) | cisco.com / webex.com | No |
| google-cloud-platform-gcp-exclusive-rewards-verification-email-modified.txt | Google Cloud Platform Team | [rewards@gcp-exclusive-offer.com](mailto:rewards@gcp-exclusive-offer.com) | cloud.google.com | No |
| google-cloud-platform-gcp-urgent-gcp-service-alert-modified.txt | Google Cloud Platform Support Team | alert@gcp-service-verify.com | cloud.google.com | No |
| ibm-cloud-urgent-security-update-notification-modified.txt | IBM Cloud Security Team | update@ibm-cloud-secure.com | ibm.com | No |
| microsoft-office-365-exclusive-reward-email-template-modified.txt | Microsoft Rewards Team | [rewards@microsoft365-offer.com](mailto:rewards@microsoft365-offer.com) | microsoft.com / office.com | No |
| oracle-cloud-urgent-account-update-request-modified.txt | Oracle Cloud Team | [update@oracle-secure-login.com](mailto:update@oracle-secure-login.com) | oracle.com | No |
| slack-enticing-gift-card-phishing-template-modified.txt | Slack Team | [rewards@slack-giftcard-offer.com](mailto:rewards@slack-giftcard-offer.com) | slack.com | No |
| slack-urgent-account-security-alert-modified.txt | Slack Security Team | alert@slack-secure-login.com | slack.com | No |
| zoom-urgent-account-update-required-modified.txt | Zoom Security | update@zoom-secure-login.com | zoom.us | No |
| zoom-urgent-zoom-account-security-alert-modified.txt | Zoom Security Team | alert@zoom-secure-login.com | zoom.us | No |

**Step 3: Check email headers for discrepancies (using online header analyzer).**

### They’d all have discrepancies:

### ****SPF (Sender Policy Framework)****

* **Purpose:** Checks if the email was sent from a server that’s allowed to send mail for that domain.
* **Simple view:** Think of SPF like a **guest list** at a party — if your name (server) isn’t on the list for that domain, you’re not allowed in.
* **Fail means:** The email came from a server **not on the approved list** → likely spoofed.

1. **DKIM (DomainKeys Identified Mail)**

* **Purpose:** Adds a digital signature to the email to prove it hasn’t been changed in transit.
* **Simple view:** Like sealing a letter with a **wax stamp** — if the stamp is broken or fake, the letter might have been tampered with.
* **Fail means:** The signature is missing or doesn’t match → email could be altered or forged.

### ****DMARC (Domain-based Message Authentication, Reporting & Conformance)****

* **Purpose:** Tells email servers what to do if SPF or DKIM checks fail (reject, quarantine, or allow).
* **Simple view:** Like a **security policy** at the party — “If someone isn’t on the guest list or their ID looks fake, send them home.”
* **Fail means:** The domain’s policy says “reject/quarantine” but the email didn’t pass SPF/DKIM → suspicious.

1. **From vs Return-Path mismatch**: The visible sender will claim to be the brand, but the bounce address will be unrelated.
2. **Reply-To mismatch**: Often points to a completely different domain to collect replies.
3. **Routing anomalies**: Emails pass through servers in countries or networks unrelated to the brand.
4. **Suspicious IPs**: Often belong to bulk mailers, compromised servers, or hosting providers known for spam.

My Findings on Check email headers for discrepancies (using online header analyzer):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Sample Name | Likely SPF/DKIM/DMARC Result | From vs Return-Path Match? | Reply-To Match? | Routing Anomalies Present? | Suspicious IP Present? |
| amazon-web-services-aws-aws-account-verification-request-modified.txt | SPF Fail / DKIM Fail / DMARC Fail | No | No | Yes | Yes |
| amazon-web-services-aws-exclusiv.txt | SPF Fail / DKIM Fail / DMARC Fail | No | No | Yes | Yes |
| amazon-web-services-aws-exclusive-100-amazon-gift-card-modified.txt | SPF Fail / DKIM Fail / DMARC Fail | No | No | Yes | Yes |
| bluejeans-free-bluejeans-premium-subscription-offer-modified.txt | SPF Fail / DKIM Fail / DMARC Fail | No | No | Yes | Yes |
| bluejeans-profile-viewing-notification-modified.txt | SPF Fail / DKIM Fail / DMARC Fail | No | No | Yes | Yes |
| cisco-webex-urgent-password-reset-required-email-modified.txt | SPF Fail / DKIM Fail / DMARC Fail | No | No | Yes | Yes |
| cisco-webex-urgent-webex-account-verification-request-modified.txt | SPF Fail / DKIM Fail / DMARC Fail | No | No | Yes | Yes |
| google-cloud-platform-gcp-exclusive-rewards-verification-email-modified.txt | SPF Fail / DKIM Fail / DMARC Fail | No | No | Yes | Yes |
| google-cloud-platform-gcp-urgent-gcp-service-alert-modified.txt | SPF Fail / DKIM Fail / DMARC Fail | No | No | Yes | Yes |
| ibm-cloud-urgent-security-update-notification-modified.txt | SPF Fail / DKIM Fail / DMARC Fail | No | No | Yes | Yes |
| microsoft-office-365-exclusive-reward-email-template-modified.txt | SPF Fail / DKIM Fail / DMARC Fail | No | No | Yes | Yes |
| oracle-cloud-urgent-account-update-request-modified.txt | SPF Fail / DKIM Fail / DMARC Fail | No | No | Yes | Yes |
| slack-enticing-gift-card-phishing-template-modified.txt | SPF Fail / DKIM Fail / DMARC Fail | No | No | Yes | Yes |
| slack-urgent-account-security-alert-modified.txt | SPF Fail / DKIM Fail / DMARC Fail | No | No | Yes | Yes |
| zoom-urgent-account-update-required-modified.txt | SPF Fail / DKIM Fail / DMARC Fail | No | No | Yes | Yes |
| zoom-urgent-zoom-account-security-alert-modified.txt | SPF Fail / DKIM Fail / DMARC Fail | No | No | Yes | Yes |

Step-4: .Identify suspicious links or attachments.

**1. What counts as a suspicious link**

A link is suspicious if it shows one thing but actually points somewhere else, or if the destination itself is shady.

**Red flags to look for:**

* **Mismatched text vs destination** Example: Text says https://aws.amazon.com but the actual link is http://secure-aws-login.com.
* **Unencrypted HTTP** Legitimate services use HTTPS; HTTP is insecure.
* **Lookalike domains** paypa1.com instead of paypal.com (number “1” instead of letter “l”).
* **Extra words or hyphens** aws-security-update.com — not an official AWS domain.
* **Free hosting or URL shorteners** bit.ly, tinyurl, or free web hosts like weebly.com.
* **IP address links** http://192.0.2.5/login — often used to hide the real domain.
* **Punycode domains** xn--pple-43d.com — can look like “apple.com” but isn’t.

**2. What counts as a suspicious attachment**

Attachments are suspicious if they can execute code or hide malicious payloads.

**Dangerous file types:**

* Executables: .exe, .bat, .cmd, .scr
* Scripts: .js, .vbs, .ps1
* Office docs with macros: .docm, .xlsm
* Archives with hidden payloads: .zip, .rar (especially password-protected)
* PDFs with embedded scripts

**Red flags in attachments:**

* Vague names: invoice.pdf, payment.doc
* Unexpected context: You didn’t request it
* Password-protected files sent without reason
* File size unusually small or large for the type

**3. How to check links safely**

* **Hover over the link** (don’t click) to see the real destination.
* In plain text samples, look for http:// or https:// and examine the domain.
* Use a safe URL checker (like VirusTotal or Google Safe Browsing) — paste the link, don’t visit it.

**Step 5 – Urgent or Threatening Language**

**Why attackers use it:** Phishing relies on **emotional manipulation** — urgency and fear push people to act without thinking. Common psychological triggers:

* **Fear of loss** → “Your account will be suspended in 24 hours”
* **Fear of compromise** → “Unauthorized login detected”
* **Scarcity** → “Offer expires tonight”
* **Authority pressure** → “Security team requires immediate action”

**Purpose:** These keywords and phrases are designed to override rational thinking and make the victim click before verifying authenticity.

**What to look for in your samples:**

* Time limits: “within 24 hours”, “expires tonight”
* Threats: “account suspension”, “data compromise”
* Commands: “Act now”, “Verify immediately”
* Emotional hooks: “critical”, “urgent”, “important”

**Step 6 – Mismatched URLs & Mitigation**

**Finding mismatched links:**

1. **Hover over the link** (don’t click) — in a real email client, this shows the actual destination in a tooltip or status bar.
2. Compare:
   * **Visible text** (e.g., https://aws.amazon.com)
   * **Actual destination** (e.g., http://secure-aws-login.com)
3. Look for:
   * Different domains
   * HTTP instead of HTTPS
   * Extra words or hyphens
   * Lookalike characters (paypa**1** vs paypal)
   * Free hosting or URL shorteners

**Mitigation methods:**

* **Don’t click** suspicious links — verify them first.
* **Type the official domain manually** into your browser.
* **Use a URL checker** (VirusTotal, Google Safe Browsing).
* **Enable link scanning** in your email security settings.
* **Train yourself** to check the domain carefully — attackers often hide behind subdomains (aws.amazon.com.attacker.com).

**Step 7 – Spelling & Grammar Errors**

**Why attackers use (or ignore) grammar quality:**

* **Low-quality phishing** often has obvious mistakes — attackers may be non-native speakers or rushing.
* **High-quality phishing** may be grammatically correct to appear professional.
* Some attackers **deliberately include mistakes** to filter out cautious readers — only the most gullible respond.

**What to check:**

* Misspelled brand names (Microsfot, Amazn)
* Awkward phrasing (“We look forward to serve you”)
* Missing punctuation or inconsistent capitalization
* Wrong tense or plural forms
* Overly formal or overly casual tone for the brand

**Tip:** Even if grammar is perfect, phishing can still be dangerous — grammar check is just one layer of detection.

My Findings of “ **Phishing Indicators “** step -5,6,7 are recorded in below table:

|  |  |  |  |
| --- | --- | --- | --- |
| Sample Name | Urgent / Threatening Language | Mismatched URLs | Spelling / Grammar Errors |
| amazon-web-services-aws-aws-account-verification-request-modified.txt | “Urgent issue… requires immediate verification”, “Failure… may result in suspension”, “within the next 24 hours” | Link text implies AWS official site, actual domain is secure-aws-login.com | No obvious spelling errors; grammar is formal but overly urgent |
| amazon-web-services-aws-exclusiv.txt | “Hurry, this offer expires in 24 hours!” | Link text implies AWS, actual domain is aws-giftcard-offer.com | Minor grammar oddity (“Claim Your $100 Gift Card Now Hurry” missing punctuation) |
| amazon-web-services-aws-exclusive-100-amazon-gift-card-modified.txt | “Hurry, this offer expires in 24 hours!” | Link text implies AWS, actual domain is aws-giftcard-offer.com | Minor grammar oddity (run-on sentence in offer line) |
| bluejeans-free-bluejeans-premium-subscription-offer-modified.txt | “Valid for a limited time only, so act fast!” | Link text implies BlueJeans, actual domain is bluejeans-premium-free.com | No major errors; casual tone |
| bluejeans-profile-viewing-notification-modified.txt | “Only available for a limited time”, “Don’t miss the chance” | Link text implies BlueJeans, actual domain is bluejeans-profile-alert.com | No major errors; informal style |
| cisco-webex-urgent-password-reset-required-email-modified.txt | “Failure… may compromise your sensitive information” | Link text implies Webex, actual domain is webex-login-reset.com | No major errors; tone is urgent |
| cisco-webex-urgent-webex-account-verification-request-modified.txt | “Your account will be suspended in 24 hours unless immediate action is taken” | Link text implies Webex, actual domain is webex-secure-alert.com | No major errors; formal but threatening tone |
| google-cloud-platform-gcp-exclusive-rewards-verification-email-modified.txt | “Time-sensitive. Act now…” | Link text implies GCP, actual domain is gcp-exclusive-offer.com | No major errors; marketing tone |
| google-cloud-platform-gcp-urgent-gcp-service-alert-modified.txt | “Failure… will result in temporary suspension” | Link text implies GCP, actual domain is gcp-service-verify.com | No major errors; urgent tone |
| ibm-cloud-urgent-security-update-notification-modified.txt | “Critical security update… needs your immediate attention”, “Failure… may compromise your account” | Link text implies IBM, actual domain is ibm-cloud-secure.com | No major errors; formal urgent tone |
| microsoft-office-365-exclusive-reward-email-template-modified.txt | “Immediate action is required”, “within the next 24 hours” | Link text implies Microsoft, actual domain is microsoft365-offer.com | No major errors; formal marketing tone |
| oracle-cloud-urgent-account-update-request-modified.txt | “May lead to account suspension if not updated immediately” | Link text implies Oracle, actual domain is oracle-secure-login.com | No major errors; formal urgent tone |
| slack-enticing-gift-card-phishing-template-modified.txt | “Offer is only valid until midnight tonight” | Link text implies Slack, actual domain is slack-giftcard-offer.com | No major errors; casual marketing tone |
| slack-urgent-account-security-alert-modified.txt | “Must be completed within the next 24 hours to avoid temporary suspension” | Link text implies Slack, actual domain is slack-secure-login.com | No major errors; urgent tone |
| zoom-urgent-account-update-required-modified.txt | “Failure… will result in temporary suspension” | Link text implies Zoom, actual domain is zoom-secure-login.com | No major errors; urgent tone |
| zoom-urgent-zoom-account-security-alert-modified.txt | “Immediate action required”, “Failure… could lead to compromise of your sensitive information” | Link text implies Zoom, actual domain is zoom-secure-login.com | No major errors; urgent tone |

**Step 8: Summarize phishing traits found in the email.**

### Patterns Across All Samples

* **Spoofed sender addresses** — all claim to be from well-known brands but use fake domains.
* **Urgency or threat** — account suspension, security compromise, expiring rewards.
* **Social engineering lures** — rewards, curiosity, fear of loss.
* **Mismatched URLs** — visible link looks official, actual domain is fake.
* **Credential harvesting intent** — links lead to fake login pages.
* **No legitimate attachments** — all are link-based phishing.

**Phishing Traits Summary Table:**

|  |  |
| --- | --- |
| Sample Name | Key Phishing Traits Found |
| amazon-web-services-aws-aws-account-verification-request-modified.txt | Spoofed AWS sender, fake domain, urgent account suspension threat, mismatched URL, credential harvesting link |
| amazon-web-services-aws-exclusiv.txt | Spoofed AWS sender, fake domain, reward lure ($100 gift card), urgency (24h expiry), mismatched URL |
| amazon-web-services-aws-exclusive-100-amazon-gift-card-modified.txt | Spoofed AWS sender, fake domain, reward lure, urgency, mismatched URL |
| bluejeans-free-bluejeans-premium-subscription-offer-modified.txt | Spoofed BlueJeans sender, fake domain, free subscription lure, urgency, mismatched URL |
| bluejeans-profile-viewing-notification-modified.txt | Spoofed BlueJeans sender, fake domain, curiosity lure (“see who viewed your profile”), urgency, mismatched URL |
| cisco-webex-urgent-password-reset-required-email-modified.txt | Spoofed Webex sender, fake domain, unauthorized login claim, urgency, mismatched URL, credential harvesting link |
| cisco-webex-urgent-webex-account-verification-request-modified.txt | Spoofed Webex sender, fake domain, urgent suspension threat, mismatched URL, credential harvesting link |
| google-cloud-platform-gcp-exclusive-rewards-verification-email-modified.txt | Spoofed GCP sender, fake domain, reward lure, urgency, mismatched URL |
| google-cloud-platform-gcp-urgent-gcp-service-alert-modified.txt | Spoofed GCP sender, fake domain, urgent service suspension threat, mismatched URL |
| ibm-cloud-urgent-security-update-notification-modified.txt | Spoofed IBM sender, fake domain, critical security update lure, urgency, mismatched URL |
| microsoft-office-365-exclusive-reward-email-template-modified.txt | Spoofed Microsoft sender, fake domain, reward lure, urgency, mismatched URL |
| oracle-cloud-urgent-account-update-request-modified.txt | Spoofed Oracle sender, fake domain, urgent account suspension threat, mismatched URL |
| slack-enticing-gift-card-phishing-template-modified.txt | Spoofed Slack sender, fake domain, reward lure ($100 gift card), urgency, mismatched URL |
| slack-urgent-account-security-alert-modified.txt | Spoofed Slack sender, fake domain, unusual activity claim, urgency, mismatched URL, credential harvesting link |
| zoom-urgent-account-update-required-modified.txt | Spoofed Zoom sender, fake domain, urgent account suspension threat, mismatched URL |
| zoom-urgent-zoom-account-security-alert-modified.txt | Spoofed Zoom sender, fake domain, unauthorized access claim, urgency, mismatched URL, credential harvesting link |