Task 2: Analyze a Phishing Email Sample.

From: mastercardsIT@gmail.com
To: employee@email.com
Subject: URGENT! Password Reset Required
—
Body:
Hello (insert name) ,

Your email account has been compromised. immediate action is required to reset your password!

Click here to reset your password in the next hour or your account will be locked:
https://en.wikipedia.org/wiki/Phishing

Regards,
Mastercard IT

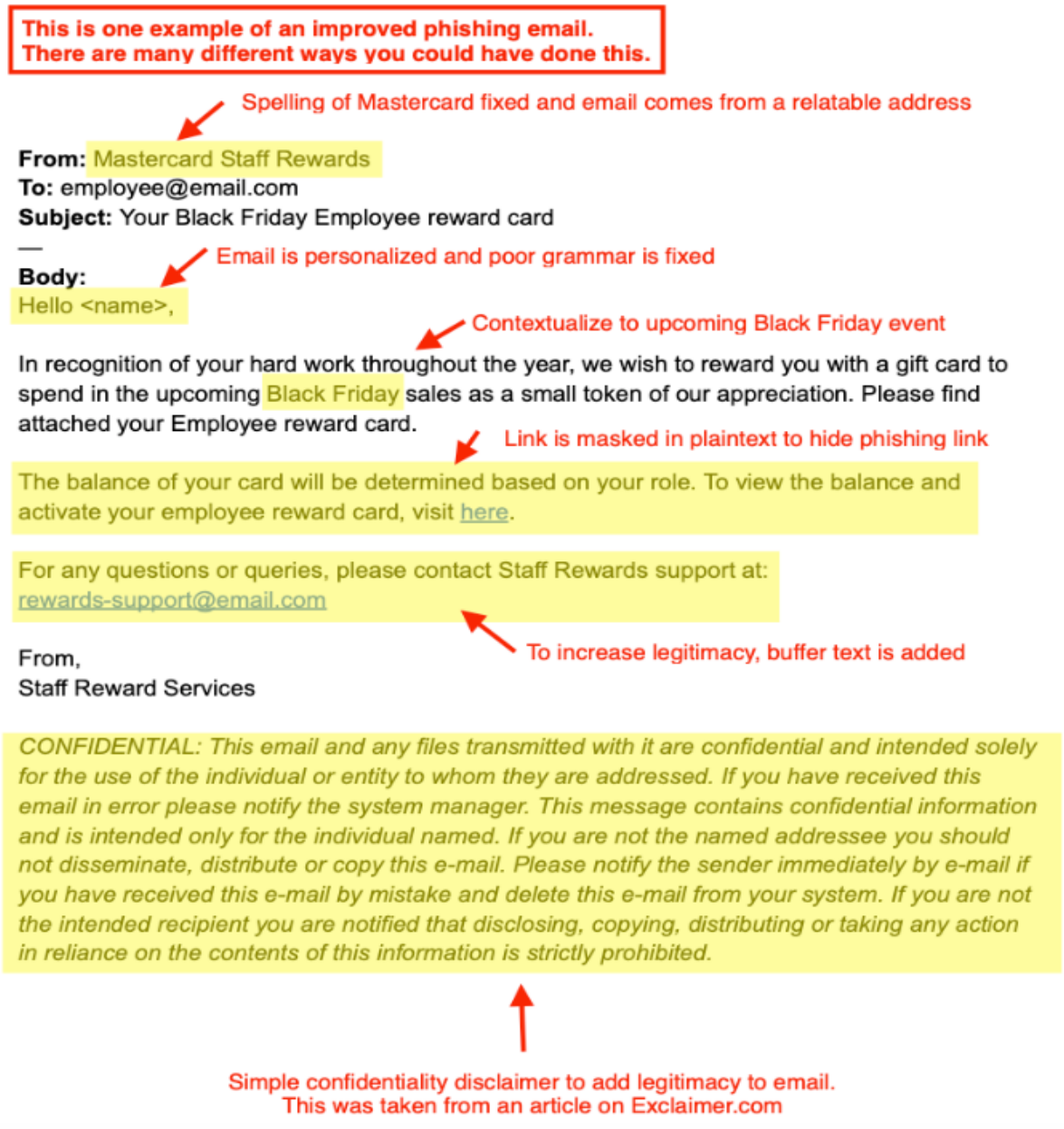
- **Sender:** mastercardsIT@gmail.com
- **Recipient:** employee@email.com
- **Subject:** URGENT! Password Reset Required
- **Body:**
    - The greeting is generic: "Hello (insert name)."
    - It contains an urgent and threatening message: "Your email account has been compromised. immediate action is required to reset your password!"
    - It pressures the recipient to act quickly by stating: "Click here to reset your password in the next hour or your account will be locked:"
    - The embedded link is https://en.wikipedia.org/wiki/Phishing, which does not match a legitimate password reset page.
    - The signature is "Regards, Mastercard IT."

Analysis of Phishing Indicators

- **Suspicious Sender Address:** The sender's email address, mastercardsIT@gmail.com, is not a legitimate Mastercard corporate email domain. It uses a public Gmail account, which is a major red flag for a company's IT department.
- **Sense of Urgency and Threat:** The subject line "URGENT!" and the body text "immediate action is required" and "your account will be locked" are classic social engineering tactics designed to make the recipient panic and click the link without thinking.
- **Generic Greeting:** The email uses a generic salutation, "Hello (insert name)," rather than addressing the recipient by their actual name, which is common in phishing attacks.
- **Mismatched URL:** The text of the link, "Click here to reset your password...", does not match the actual URL provided, which is a Wikipedia page about phishing. A legitimate link would point to a Mastercard-owned domain.

Task 2: Analyze a Phishing Email Sample.

- **Spelling/Grammar Errors:** There is a minor grammatical error where "immediate" is not capitalized after the period in the second sentence.
- **Impersonation:** The email attempts to impersonate "Mastercard IT" to appear as a



Summary of the "Improved" Phishing Email Sample

- **Sender:** Mastercard Staff Rewards
- **Recipient:** employee@email.com
- **Subject:** Your Black Friday Employee reward card

Task 2: Analyze a Phishing Email Sample.

- **Body:**
    - The greeting is personalized with <name>.
    - The email is contextualized to an upcoming Black Friday event.
    - It offers a "gift card" as a "small token of our appreciation" for hard work.
    - It contains a link to "view the balance and activate your employee reward card".

      rewards-support@email.com is provided for questions.
    - The signature is "Staff Reward Services".
    - A "confidentiality disclaimer" is included at the bottom to add legitimacy to the email.

Analysis of Phishing Indicators

Relatable Sender and Context: The sender "Mastercard Staff Rewards" appears more legitimate than a random Gmail address, and the email is contextualized to the Black Friday event to appear more realistic.

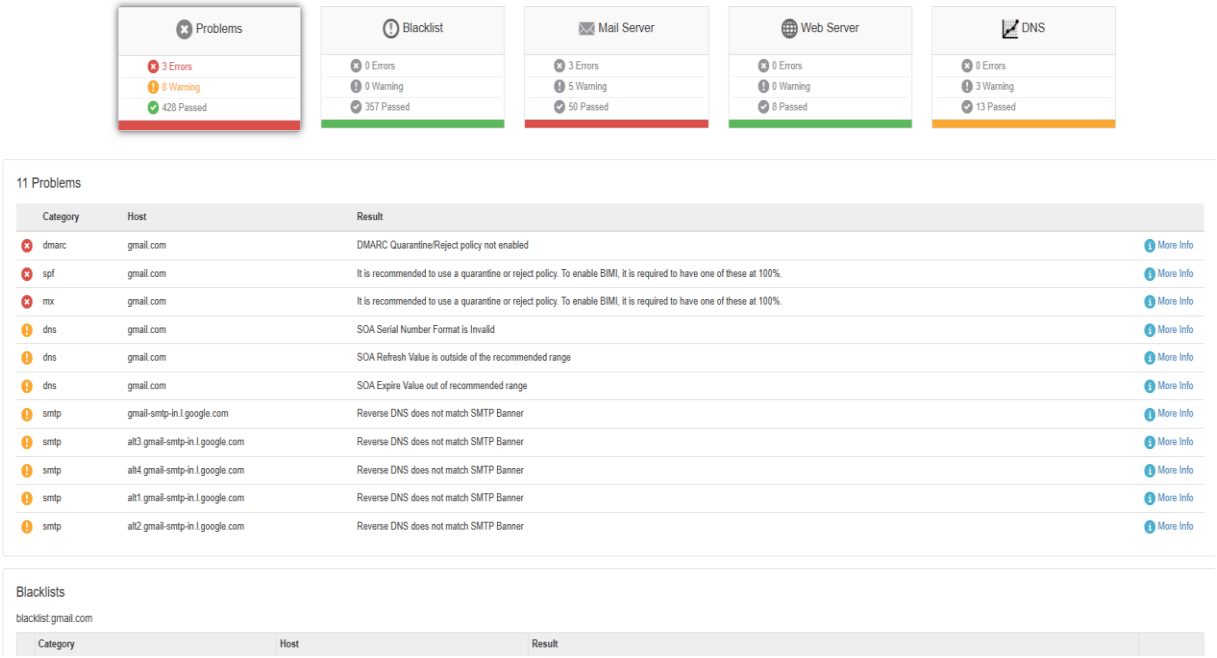
Personalization and Improved Grammar: The email uses a personalized greeting <name> and has no noticeable spelling or grammar errors, making it seem more professional and trustworthy than a typical phishing email.

Link Masking: The link is masked in plaintext with the word "here" to hide the actual phishing link.

Addition of Buffer Text: The email includes "buffer text" and a "confidentiality disclaimer" to increase its legitimacy and make it seem more authentic. This adds to the social engineering aspect of the attack.

- **Implicit Urgency:** While not overtly threatening, the email creates an implicit sense of urgency by offering a limited-time reward tied to a specific event (Black Friday) and prompting the user to "activate" their card.

Task 2: Analyze a Phishing Email Sample.



Summary of the MXToolbox Report

The image displays a report from a tool like MXToolbox that analyzes various aspects of a domain, specifically gmail.com in this case. The report is organized into several sections, with a high-level summary at the top followed by detailed problem listings.

Top-Level Summary:

- **Problems:** There are 3 errors and 0 warnings, with 428 checks passed. This is indicated by a red box.
- **Blacklist:** The domain passed all 357 blacklist checks, indicated by a green box.
- **Mail Server:** There are 3 errors and 5 warnings, with 50 checks passed, shown in a red box.
- **Web Server:** All 8 checks passed, with 0 errors and 0 warnings, in a green box.
- **DNS:** There are 0 errors, 3 warnings, and 13 checks passed, shown in an orange/yellow box.

Detailed Problem List (11 Problems):

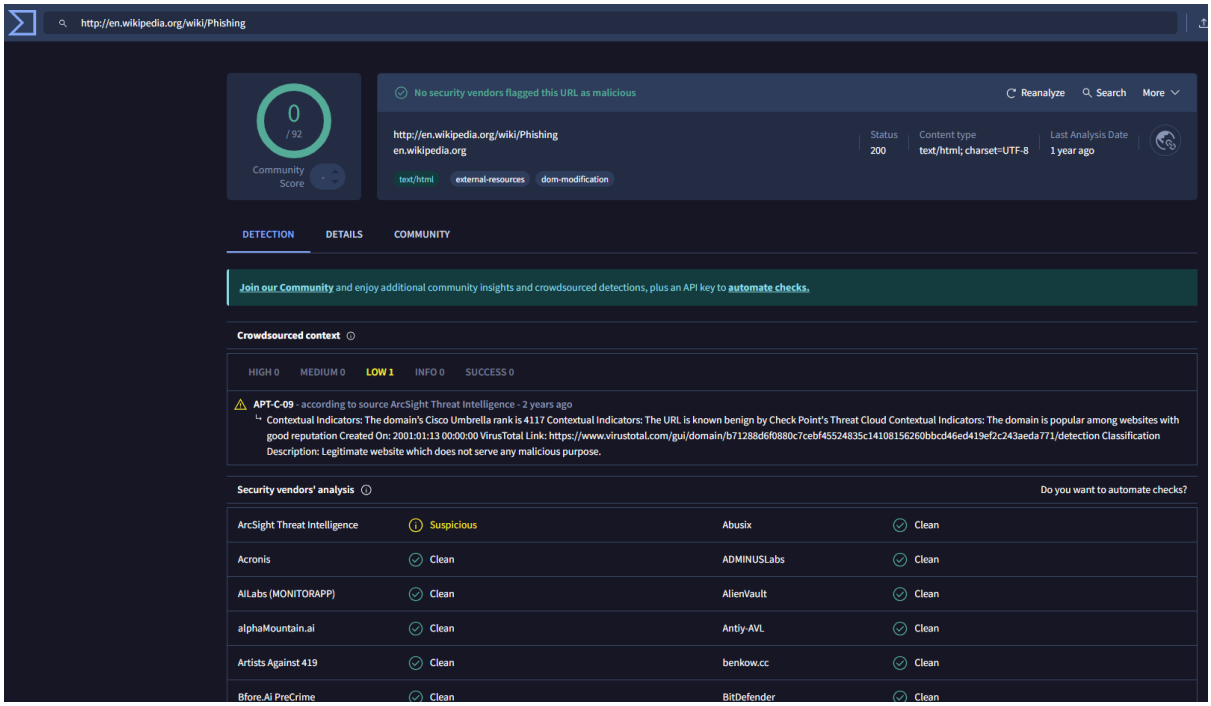
The report lists several specific issues found:

- **DMARC:** The DMARC policy for gmail.com is not set to "Quarantine or Reject," which is recommended.
- **SPF (Sender Policy Framework):** The report recommends a "quarantine or reject" policy for SPF.
- **MX (Mail Exchanger):** Similar to SPF, it recommends a "quarantine or reject" policy for MX.
- **DNS (Domain Name System):**
    - The SOA (Start of Authority) Serial Number format is invalid.
    - The SOA Refresh Value is outside the recommended range.

Task 2: Analyze a Phishing Email Sample.

- The SOA Expire Value is outside the recommended range.

- **SMTP (Simple Mail Transfer Protocol):** Several smtp entries show "Reverse DNS does not match SMTP Banner" for different Google mail servers (gmail-smtp-in.l.google.com, alt3.gmail-smtp-in.l.google.com, alt4.gmail-smtp-in.l.google.com, alt1.gmail-smtp-in.l.google.com, alt2.gmail-smtp-in.l.google.com). This is a common warning where the DNS lookup of the sending IP address does not match the name presented in the SMTP banner.



Summary of the URL Analysis Report

The image displays a security analysis of the URL http://en.wikipedia.org/wiki/Phishing, likely from a threat intelligence or URL scanner tool.

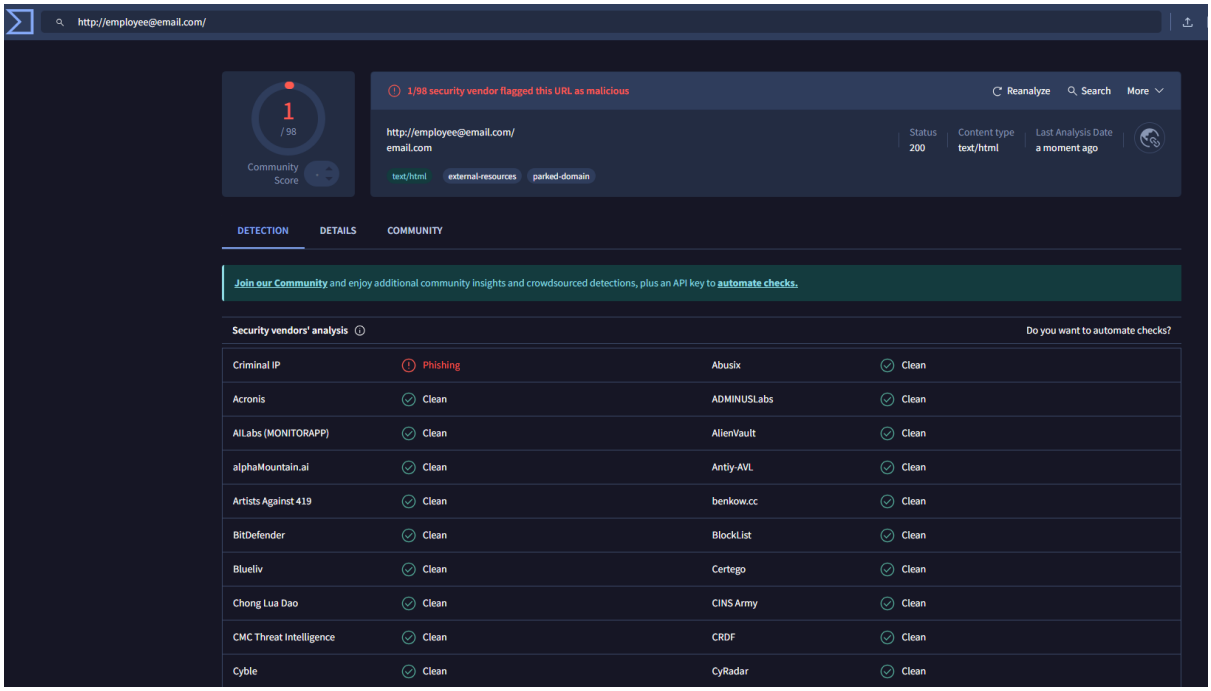
- **Overall Verdict:** The analysis shows a "Community Score" of **0/92**, and a green-colored message states, "No security vendors flagged the URL as malicious." This indicates that the URL is considered safe.

- **URL Details:**
  - **URL:** http://en.wikipedia.org/wiki/Phishing
  - **Domain:** en.wikipedia.org
  - **Status:** 200 (which means "OK")
  - **Content Type:** text/html; charset=UTF-8
  - **Last Analysis Date:** 1 year ago

Task 2: Analyze a Phishing Email Sample.

- **Detection and Community Insights:**
    - The "Detection" tab is selected, showing a high-level overview.
    - Under "Crowdsourced context," there's a specific entry from "APT-C-09 according to source ArcSight Threat Intelligence - 2 years ago".
    - This crowdsourced information notes that the domain cisco Umbrella ranks the URL as a "4.17" and that it's "known benign by Check Point's Threat Cloud Contextual Indicators".
    - It describes the domain as "popular among websites with good reputation" and explicitly states the detection description is a "Legitimate website which does not serve any malicious purpose".
- **Security Vendor Analysis:**
    - A list of various security vendors (e.g., ArcSight Threat Intelligence, Acronis, AllLabs, AlphaMountain.ai, etc.) and their verdicts is shown.
    - Most vendors, including Acronis, AllLabs, and AlphaMountain.ai, classify the URL as "Clean".
    - One vendor, ArcSight Threat Intelligence, has a "Suspicious" flag, but the context box from the same source clarifies that the site itself is legitimate. The overall consensus is that the URL is safe.

Task 2: Analyze a Phishing Email Sample.



The image displays a security analysis of the URL http://employee@email.com, likely from a threat intelligence or URL scanner tool. The report indicates that one security vendor has flagged the URL as malicious, but the overall consensus from other vendors is that it's clean.

- **Overall Verdict:** The analysis shows a "Community Score" of **1/98**, and a red-colored message at the top states, "1/98 security vendor flagged this URL as malicious." This suggests a potential threat, though the majority of checks came back clean.
- **URL Details:**
  - **URL:** http://employee@email.com/
  - **Domain:** email.com
  - **Status:** 200 (which means "OK").
  - **Content Type:** text/html.
  - **Last Analysis Date:** A moment ago.
- **Security Vendor Analysis:**
  - The "Detection" tab is selected, showing a high-level overview of vendor findings.
  - A list of various security vendors (e.g., Criminal IP, Acronis, AllLabs, etc.) and their verdicts is shown.
  - One vendor, **Criminal IP**, has flagged the URL as **"Phishing"**, which is a significant finding.
  - The rest of the vendors listed, including Acronis, AllLabs, AlphaMountain.ai, and others, have classified the URL as **"Clean"**.