Phishing Scams

Sample 1 Phishing Email

Subject: Urgent: Action Required to Avoid Account Suspension

From: `security-update@micros0ft-support.com`

To: you@example.com

Dear Valued Customer,

We have noticed suspicious activity in your Microsoft account. For your security, we have temporarily limited your account access.

To restore full access and avoid permanent suspension, please verify your account within the next 24 hours.

Click here to verify your account

Failure to do so may result in data loss and account termination as per our Terms of Service.

Thank you for your immediate attention.

Sincerely,
Microsoft Security Team
`security-update@micros0ft-support.com`

Attachment: `AccountVerification.docm` *(macro-enabled document)*

Indicators of Phishing

Indicator	Description
Spoofed Sender	Looks like Microsoft, but domain is `micros0ft-support.com` (note the “0” instead of “o”)
Suspicious Link	Text claims to lead to Microsoft, but actual URL is an unknown domain
Urgency	“Verify within 24 hours” creates panic
Poor Grammar	“Failure to do so may result in data loss...” is awkwardly phrased

Dangerous Attachment	`.docm` files can run malicious macros

Sample 2: Fake Bank Alert

Subject: [Action Required] Unusual Activity Detected on Your Account
From: `security-alerts@bankofamerlca.com`

Dear Customer,

We've detected a login attempt from an unknown device. For your protection, we have locked your account temporarily.

Please confirm your identity by logging in below:

Verify Now

Failure to verify within 12 hours will result in permanent account suspension.

Sincerely,
Bank of America Fraud Department
`security-alerts@bankofamerlca.com`

Indicators of phishing :

- Spoofed domain: `bankofamerlca.com` (note the "l" instead of "i")
- Fake urgency: "verify within 12 hours"
- Suspicious link
- No personal salutation

Sample 3: Package Delivery Scam

Subject: Your Package is Held – Address Confirmation Needed
From: `delivery-notice@fedex-tracker.co`

Hello,

We attempted to deliver your parcel today, but no one was available at the address.
Please confirm your delivery address using the link below:

Reschedule Delivery

Note: Your parcel will be returned to the sender within 3 days if unclaimed.

Best regards,
FedEx Support Team
`delivery-notice@fedex-tracker.co`

Indicators of phishing:

- Fake domain: `fedex-tracker.co`
- No tracking number or details
- Threat of return creates urgency
- URL doesn't belong to actual FedEx

Sample 4: Tech Support Refund Scam

Subject: Refund Notification - Action Required
From: `support@tech-assist247.com`

Dear Customer,

You are eligible for a refund of $259.99 due to the termination of our service.
Please fill out the refund form to claim your money:

Claim Refund Now

If we don't receive your confirmation in 48 hours, your refund will be canceled.

Thank you,
TechAssist Billing Team
`support@tech-assist247.com`

Indicators of phishing:

- Refund bait to lure clicks
- Unknown company name
- Fake urgency
- Requests financial information via unsecured site

Header analysis

1. Header Sample

Return-Path: <security-alerts@bankofamerlca.com>

Received: from unknown (HELO mail.bankofamerlca.com) (185.123.45.67)

by mail.example.com with SMTP; Tue, 27 May 2025 09:12:34 +0000

Received-SPF: softfail (example.com: domain of transitioning security-alerts@bankofamerlca.com does not designate 185.123.45.67 as permitted sender)

Authentication-Results: mail.example.com;

dkim=fail reason="signature verification failed" header.d=bankofamerlca.com;

spf=softfail (domain not verified);

dmarc=fail (p=REJECT sp=REJECT dis=NONE) header.from=bankofamerlca.com

From: "Bank of America Alerts" <security-alerts@bankofamerlca.com>

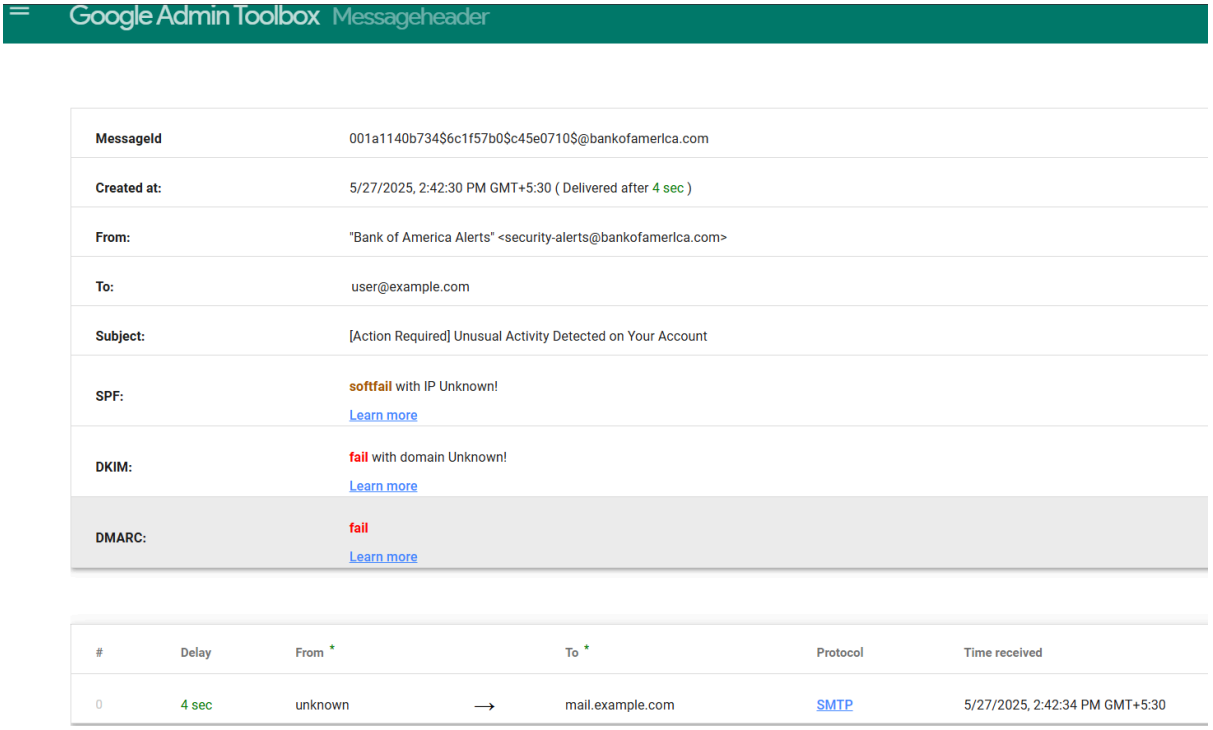
To: user@example.com

Subject: [Action Required] Unusual Activity Detected on Your Account

Date: Tue, 27 May 2025 09:12:30 +0000

Message-ID: <001a1140b734$6c1f57b0$c45e0710$@bankofamerlca.com>

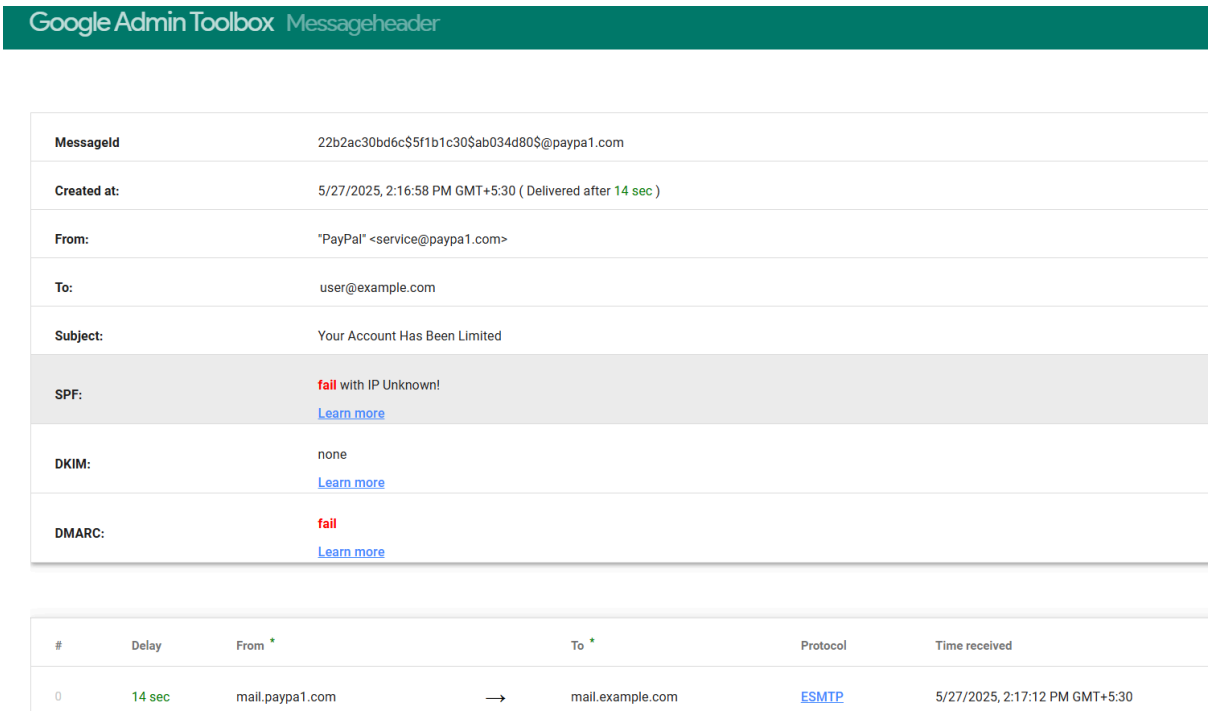
Header analysis result



2. Header Sample (PayPal Notification)

Return-Path: <service@paypa1.com>
Received: from mail.paypa1.com (185.210.91.2)
    by mail.example.com with ESMTP; Mon, 27 May 2025 08:47:12 +0000
Received-SPF: fail (example.com: domain of service@paypa1.com does not designate 185.210.91.2 as permitted sender)
Authentication-Results: mail.example.com;
    spf=fail smtp.mailfrom=service@paypa1.com;
    dkim=none (no signature);
    dmarc=fail (p=REJECT sp=REJECT dis=NONE) header.from=paypa1.com
From: "PayPal" <service@paypa1.com>
To: user@example.com
Subject: Your Account Has Been Limited
Date: Mon, 27 May 2025 08:46:58 +0000
Message-ID: <22b2ac30bd6c$5f1b1c30$ab034d80$@paypa1.com>

Header analysis result



3.Header Sample (Microsoft Security Alert)

Return-Path: <alerts@micr0soft.com>
Received: from unknown.host.com (unknown.host.com. [198.51.100.5])
    by example.com with ESMTPS id abc123
    for <you@example.com>; Mon, 27 May 2025 10:11:00 +0000
Received-SPF: fail (example.com: domain of alerts@micr0soft.com does not designate 198.51.100.5 as permitted sender)
Authentication-Results: example.com;
    dkim=fail (signature did not verify) header.d=micr0soft.com;
    spf=fail (sender IP not authorized);
    dmarc=fail (policy=REJECT) header.from=micr0soft.com
From: Microsoft Security <alerts@micr0soft.com>
To: you@example.com
Subject: Suspicious Sign-In Attempt Detected
Date: Mon, 27 May 2025 10:10:45 +0000
Message-ID: <0a9e8c0e-caf2-4bd2-9eac@micr0soft.com>

Header analysis result