Name: Satya Chaitanya

Task2: Identify phishing characteristics in a suspicious email sample.

Date: 21-10-2025

Tools used: sample email template, Mx toolbox header analyzer

Target email: info@updazz.com

Phishing

Phishing happens when a victim acts on a fraudulent email that demands urgent action. Examples of requested actions in a phishing email include:

- Clicking an attachment
- Enabling macros in a Word document
- Updating a password
- Responding to a social media friend or contact request
- Connecting to a new Wi-Fi hotspot

Every year, cybercriminals become savvier with their phishing tactics, improve their techniques, and try new methods to deceive and steal from unsuspecting people. Now, you can expect phishing through voicemails, texts, and emails.
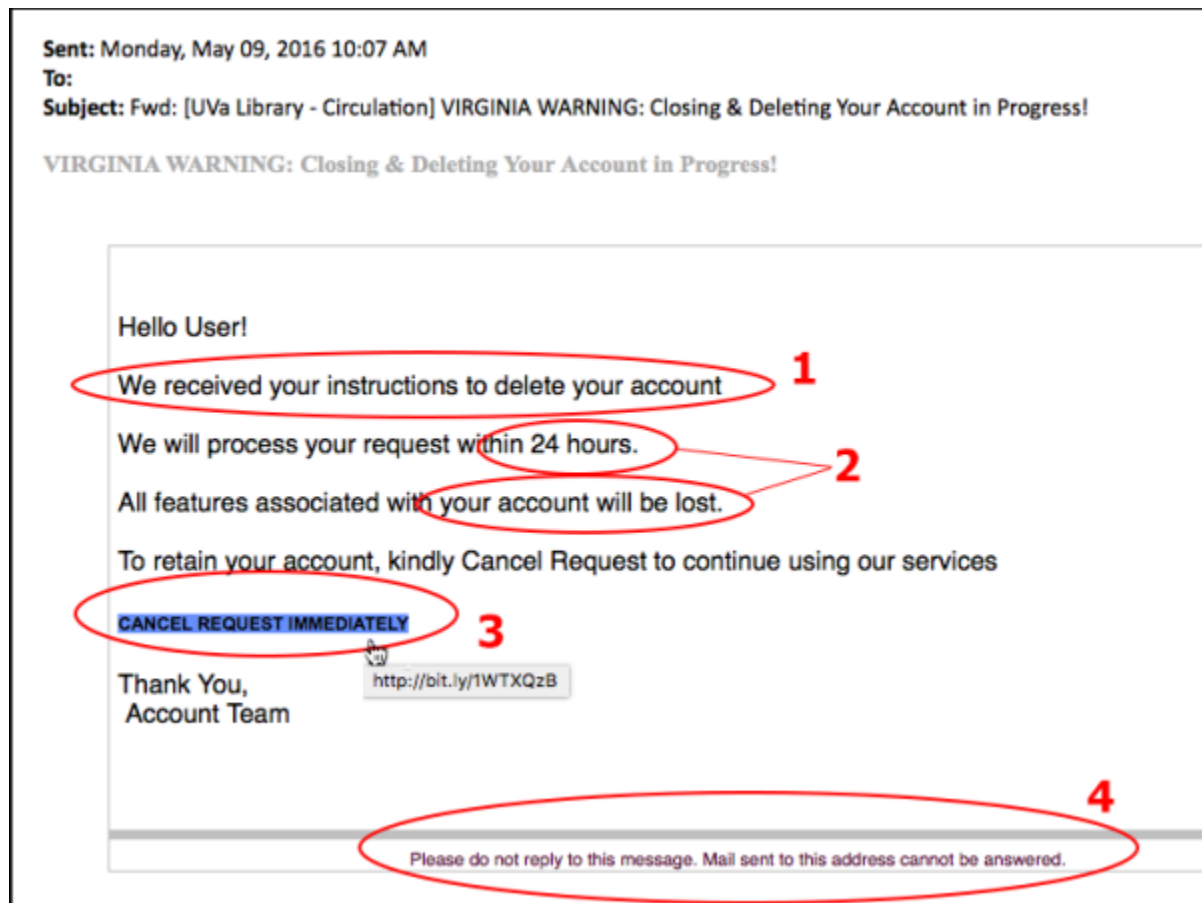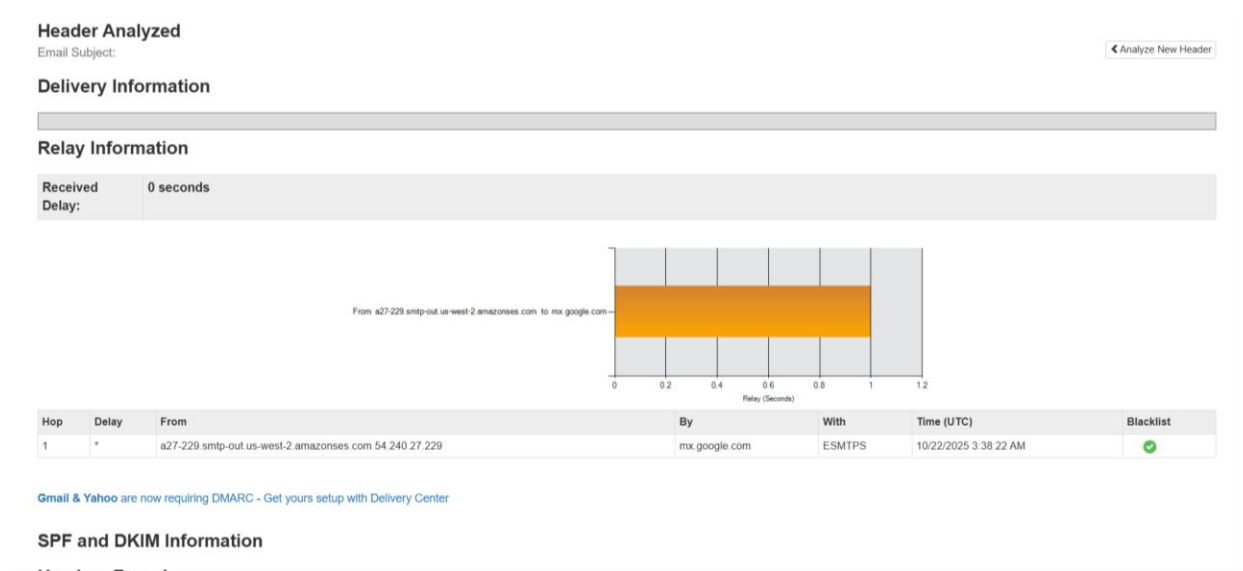
Fig: a sample email template

Header Analyzed
Email Subject:

◄ Analyze New Header

Delivery Information

Relay Information

Received Delay:	0 seconds

From a27-229.smtp-out.us-west-2.amazonses.com to mx.google.com

Relay (Seconds): 0   0.2   0.4   0.6   0.8   1   1.2

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	a27-229.smtp-out.us-west-2.amazonses.com 54.240.27.229	mx.google.com	ESMTPS	10/22/2025 3:38:22 AM	✅

Gmail & Yahoo are now requiring DMARC - Get yours setup with Delivery Center

SPF and DKIM Information

Headers Found

Received-SPF	pass (google.com: domain of 0101019a09ff0e58-21c5bf49-962a-417f-bf10-6dbc4b7e4edc-000000@postmaster.updazz.com designates 54.240.27.229 as permitted sender) client-ip=54.240.27.229;
Authentication-Results	mx.google.com; dkim=pass header.i=@updazz.com header.s=wdrnix7xebnmssgm623u65x4qrxhq6pb header.b=nljyYAPc; dkim=pass header.i=@amazonses.com header.s=gdwg2y3kokkkj5a55z2ilkup5wp5hhxx header.b="n8ar/MzP"; spf=pass (google.com: domain of 0101019a09ff0e58-21c5bf49-962a-417f-bf10-6dbc4b7e4edc-000000@postmaster.updazz.com designates 54.240.27.229 as permitted sender) smtp.mailfrom=0101019a09ff0e58-21c5bf49-962a-417f-bf10-6dbc4b7e4edc-000000@postmaster.updazz.com; dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=updazz.com
DKIM-Signature	v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple; s=wdrnix7xebnmssgm623u65x4qrxhq6pb; d=updazz.com; t=1761104301; h=From:Reply-To:To:Subject:MIME-Version:Content-Type:Message-ID:Date; bh=1njY89JY+OQgJJcjVR+VwuWs8lDl8kgGhF+ddoomrjQ=; b=nljyYAPcMAY+hAXz0VvRhmGCeilXAnYdEWzJHg72n+4VPZ8ftYI0X0yu2ZymI+A dhccUifzKIbz0FrrayGuSvtH1O5WYm6TCE3UqAkJISxx0YIyVL9kZEIAq24kD7uXw8d jHNrQLWO337sQHv9hgXFfK8Znwu39r1dmxr7SkAM=

Received Header

```
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@updazz.com header.s=wdrnix7xebnmssgm623u65x4qrxhq6pb header.b=nljyYAPc;
       dkim=pass header.i=@amazonses.com header.s=gdwg2y3kokkkj5a55z2ilkup5wp5hhxx header.b="n8ar/MzP";
       spf=pass (google.com: domain of 0101019a09ff0e58-21c5bf49-962a-417f-bf10-6dbc4b7e4edc-000000@postmaster.updazz.com designates 54.240.27.229 as permitted sender) smtp.mailfrom=0101019a09ff0e58-21d
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=updazz.com
Return-Path: <0101019a09ff0e58-21c5bf49-962a-417f-bf10-6dbc4b7e4edc-000000@postmaster.updazz.com>
Received: from a27-229.smtp-out.us-west-2.amazonses.com (a27-229.smtp-out.us-west-2.amazonses.com. [54.240.27.229])
       by mx.google.com with ESMTPS id 41be03b00d2f7-b6a76646edasi6390259a12.165.2025.10.21.20.38.21
       for <satyachaitanya21@gmail.com>
       (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128);
       Tue, 21 Oct 2025 20:38:22 -0700 (PDT)
Received-SPF: pass (google.com: domain of 0101019a09ff0e58-21c5bf49-962a-417f-bf10-6dbc4b7e4edc-000000@postmaster.updazz.com designates 54.240.27.229 as permitted sender) client-ip=54.240.27.229;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@updazz.com header.s=wdrnix7xebnmssgm623u65x4qrxhq6pb header.b=nljyYAPc;
       dkim=pass header.i=@amazonses.com header.s=gdwg2y3kokkkj5a55z2ilkup5wp5hhxx header.b="n8ar/MzP";
       spf=pass (google.com: domain of 0101019a09ff0e58-21c5bf49-962a-417f-bf10-6dbc4b7e4edc-000000@postmaster.updazz.com designates 54.240.27.229 as permitted sender) smtp.mailfrom=0101019a09ff0e58-21d
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=updazz.com
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple; s=wdrnix7xebnmssgm623u65x4qrxhq6pb; d=updazz.com; t=1761104301; h=From:Reply-To:To:Subject:MIME-Version:Content-Type:Message-ID:Date; bh=
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple; s=gdwg2y3kokkkj5a55z2ilkup5wp5hhxx; d=amazonses.com; t=1761104301; h=From:Reply-To:To:Subject:MIME-Version:Content-Type:Message-ID:Date:Fd
```