

Sample Spam Email


From: Amazon Support <account-security@amaz0n-alerts.com>
To: user@example.com
Subject: Suspicious Activity Detected on Your Amazon Account

Body:

Hello,

We have detected suspicious login activity on your Amazon account from a new device. For your safety, we have temporarily restricted access to your account.

Please confirm your account ownership by clicking the link below:

 [Confirm Now](#)

If you do not confirm within 24 hours, your account will be permanently suspended.

Thank you for choosing Amazon.

Sincerely,
Amazon Security Team

*After Checking the Email Headers For Discrepancies.

Return-Path: <notices@amaz0n-alerts.com>
Received: from mail.fakehost.ru (fakehost.ru [193.34.56.78])
by mx.example.com with ESMTTP id A1B2C3D4;
Tue, 24 Jun 2025 14:23:01 +0530 (IST)
Received-SPF: Fail (mx.example.com: domain of amaz0n-alerts.com does not designate 193.34.56.78 as permitted sender)
Authentication-Results: mx.example.com;
dkim=fail (bad signature) header.d=amaz0n-alerts.com;
spf=fail (sender IP is 193.34.56.78);
dmarc=fail (p=REJECT)
From: Amazon Support <account-security@amaz0n-alerts.com>
To: user@example.com
Subject: Suspicious Activity Detected on Your Amazon Account
Date: Tue, 24 Jun 2025 14:21:55 +0530
Message-ID: <CAFjQmfke8947238jfh@amaz0n-alerts.com>

Indicator	Suspicious Detail
-----------	-------------------

From Address	`amaz0n-alerts.com` uses "0" instead of "o" – a **lookalike domain
Return-Path	`notices@amaz0n-alerts.com` – not a legitimate Amazon domain
SPF	Fails – IP not authorized to send emails for that domain
DKIM	Fails – email may be **forged or modified** in transit
DMARC	Fails – sender failed domain verification checks
Received from	IP address belongs to a (non-Amazon domain) in Russia (`fakehost.ru`)

Suspicious Links or Attachments

Suspicious link: <http://secure-amazon-check.xyz/login>
The domain is not amazon.com – it's a malicious lookalike.

Mismatched URLs (Hover Test)

Visible link: Confirm Now

Real destination: <http://secure-amazon-check.xyz/login>

Mismatch = high risk.

Spelling or Grammar Errors

Subtle issues:

"confirm your account ownership" – unnatural phrasing

"Thank you for choosing Amazon" – slightly generic, missing personalization

Missing comma after "Hello"

Many phishing emails also use:

"Dear customer" (instead of name)

Poor punctuation or sentence structure

Summary

Trait	Description
spoofed sender	`amaz0n-alerts.com` instead of `amazon.com`
Suspicious link	`secure-amazon-check.xyz` (fake site)
Urgency	Threatens permanent suspension within 24 hours
Mismatched URL	Link text ≠ real destination
Poor grammar	Slightly unnatural wording
Failed SPF/DKIM/DMARC	Header shows authentication failures
Generic greeting	No personalized name, just "Hello"