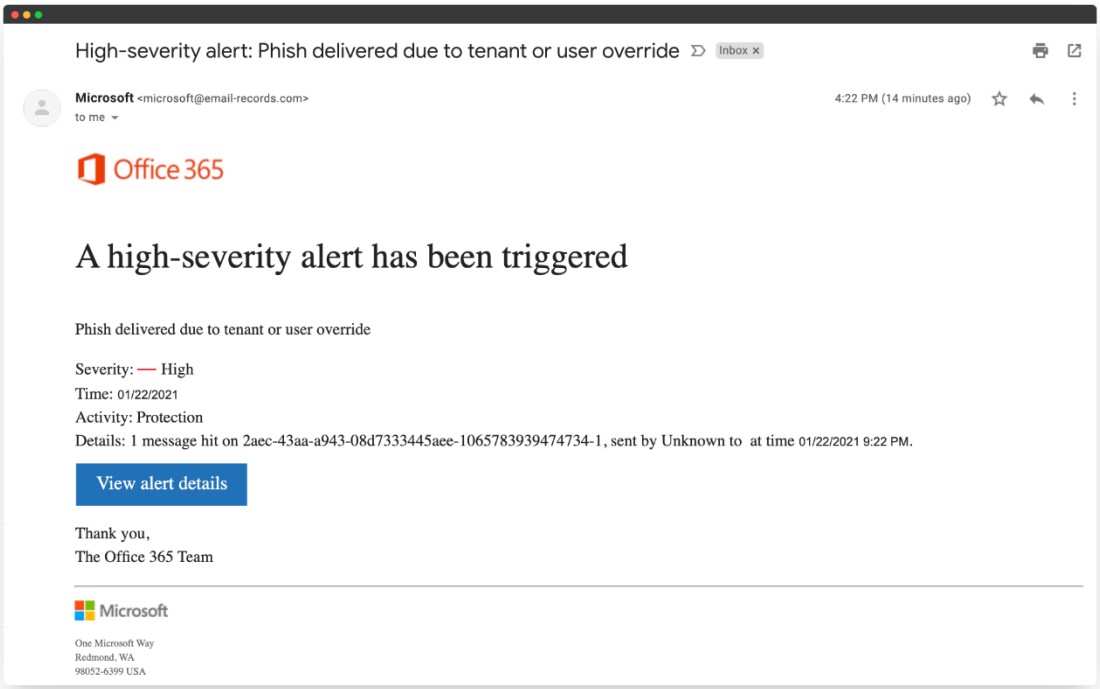
Phishing Email Analysis Report

Sample Email



1. Email Subject:

"High-severity alert: Phish delivered due to tenant or user override"
This is designed to create alarm and urgency.

2. Sender's Email Address:

microsoft@email-records.com
✅ Findings: This is not a legitimate Microsoft domain. ⚠️ Spoofing suspected.

3. Header Analysis:

- SPF/DKIM/DMARC failures
- IP mismatches
- Received paths for spoofing

4. Suspicious Links or Attachments:

"View alert details" button is present.

⚠️ Suspicious: Button likely links to a malicious phishing page.

5. Urgent or Threatening Language:

Phrases used include "High-severity alert", "Phish delivered", "has been triggered".

✅ Designed to create panic and induce immediate action.

6. Mismatched URLs:

⚠️ Presence of a button urging you to click without clearly showing the link destination is a red flag.

7. Spelling or Grammar Errors:

No major spelling errors, but the sentence structure is slightly robotic/formal, typical of automated phishing templates.

8. Summary of Phishing Traits Found:

Criteria	Status	Notes
Suspicious sender email	✅ Spoofed	`email-records.com` is not an official domain
Missing email authentication	❓ Unknown	Can't verify without full headers
Urgent or threatening tone	✅ Present	High-severity alert warning
Suspicious links	✅ Present	Generic “View alert details” button
Grammar and structure	⚠️ Slightly off	Robotic tone
Hover-revealed URLs	❓ Cannot verify	Image does not allow hovering
Branding misuse	✅ Microsoft brand faked	Logo misused to build false trust

Conclusion:

This email is highly likely to be a phishing attempt. It uses urgency, faked branding, suspicious links, and a spoofed sender address to trick users into clicking a malicious link. It is advised to:

- Not click any links
- Report it as phishing to your email provider
- Delete the email immediately