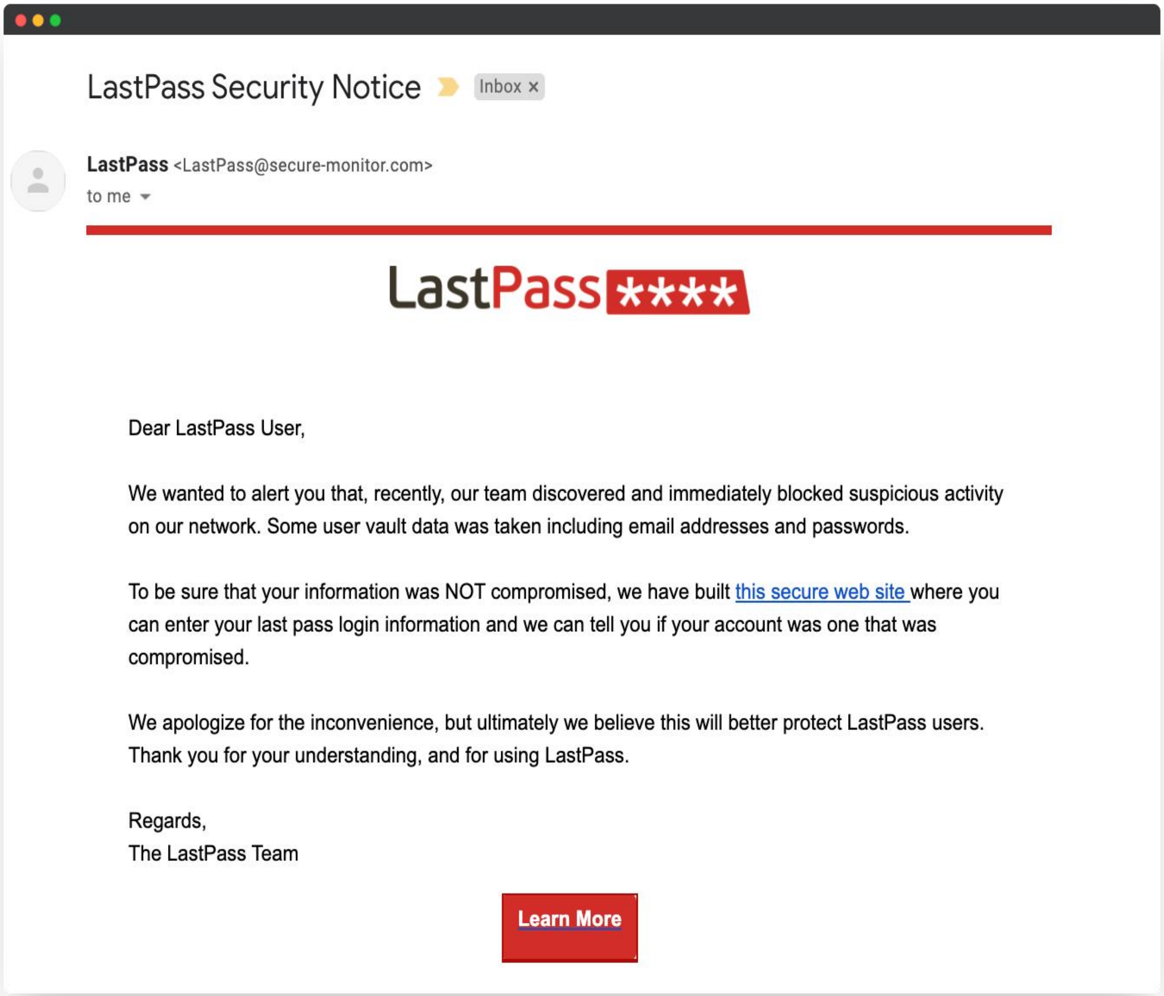
Phishing Email Analysis Report

Report Title: Analysis of Suspicious Email Impersonating LastPass

Date: 10/12/25

Classification: Phishing Attempt – Credential Harvesting



LastPass Security Notice

LastPass <LastPass@secure-monitor.com>

to me

Dear LastPass User,

We wanted to alert you that, recently, our team discovered and immediately blocked suspicious activity on our network. Some user vault data was taken including email addresses and passwords.

To be sure that your information was NOT compromised, we have built this secure web site where you can enter your last pass login information and we can tell you if your account was one that was compromised.

We apologize for the inconvenience, but ultimately we believe this will better protect LastPass users. Thank you for your understanding, and for using LastPass.

Regards,
The LastPass Team

1. Executive Summary

A suspicious email impersonating LastPass was analyzed. The email claimed that suspicious activity occurred on the LastPass network and prompted the recipient to verify their login credentials on a “secure website.” Multiple indicators confirm that this is a credential-harvesting phishing attack designed to steal LastPass account credentials.

2. Email Details (From Provided Sample)

- Subject: LastPass Security Notice

- Sender Display Name: LastPass

- Sender Address: LastPass@secure-monitor.com

- Recipient: User

- Attachments: None

- Embedded Links: Present (“this secure web site”, “Learn More”)

3. Sender Verification & Spoofing Analysis

- The domain secure-monitor.com does not belong to LastPass.

- Official LastPass emails originate from @lastpass.com.

- Use of deceptive display name (“LastPass”) is consistent with email spoofing tactics.

- The mismatched domain strongly suggests unauthorized impersonation.

Assessment: High-confidence indicator of phishing.

4. Header Analysis (Conceptual Indicators)

While full headers were not provided, expected red flags include:

- SPF/DKIM/DMARC failures

- Mismatch between 'From' and 'Return-Path'

- IP address not tied to LastPass infrastructure

- Use of non-standard mail relays

5. Content Analysis

5.1 Urgency & Fear Tactics

The email states:

- “suspicious activity on our network”

- “some user vault data was taken”

- urges the user to immediately verify credentials

5.2 Suspicious Links

The phrases:

- “this secure web site”

- “Learn More”

indicate embedded hyperlinks likely leading to a fraudulent LastPass login portal.

5.3 Credential Harvesting Attempt

The email asks the user to enter their LastPass login information. Legitimate companies never ask for passwords via email.

5.4 Grammar & Formatting Issues

Contains awkward phrasing, unnecessary commas, and unprofessional tone.

6. Indicators of Compromise (IOCs)

- Sender Domain: secure-monitor.com

- Display Name: “LastPass”

- Suspicious Links: “this secure web site”, “Learn More”

- Content: Claims of data compromise

- Behavior: Requests login credentials

7. Phishing Characteristics Identified

- Spoofed sender domain

- Generic and vague security alert

- Urgent language inducing fear

- Request for sensitive credentials

- Suspicious hyperlinks

- Grammar errors

- Unusual domain unrelated to LastPass

8. Attack Type Classification

Threat Category: Social Engineering → Phishing

Attack Objective: Credential Harvesting

Risk Level: High

9. Recommended Actions

For End Users:

- Do NOT click links or enter credentials.

- Delete or report the email.

- Reset LastPass credentials through official channels if interacted.

For Security Team:

- Block sender domain.

- Add URLs to deny-list.

- Conduct user awareness training.

- Monitor for suspicious login attempts.

10. Conclusion

The analyzed email is a fraudulent phishing attempt designed to impersonate LastPass and steal user credentials. Indicators strongly confirm malicious intent.