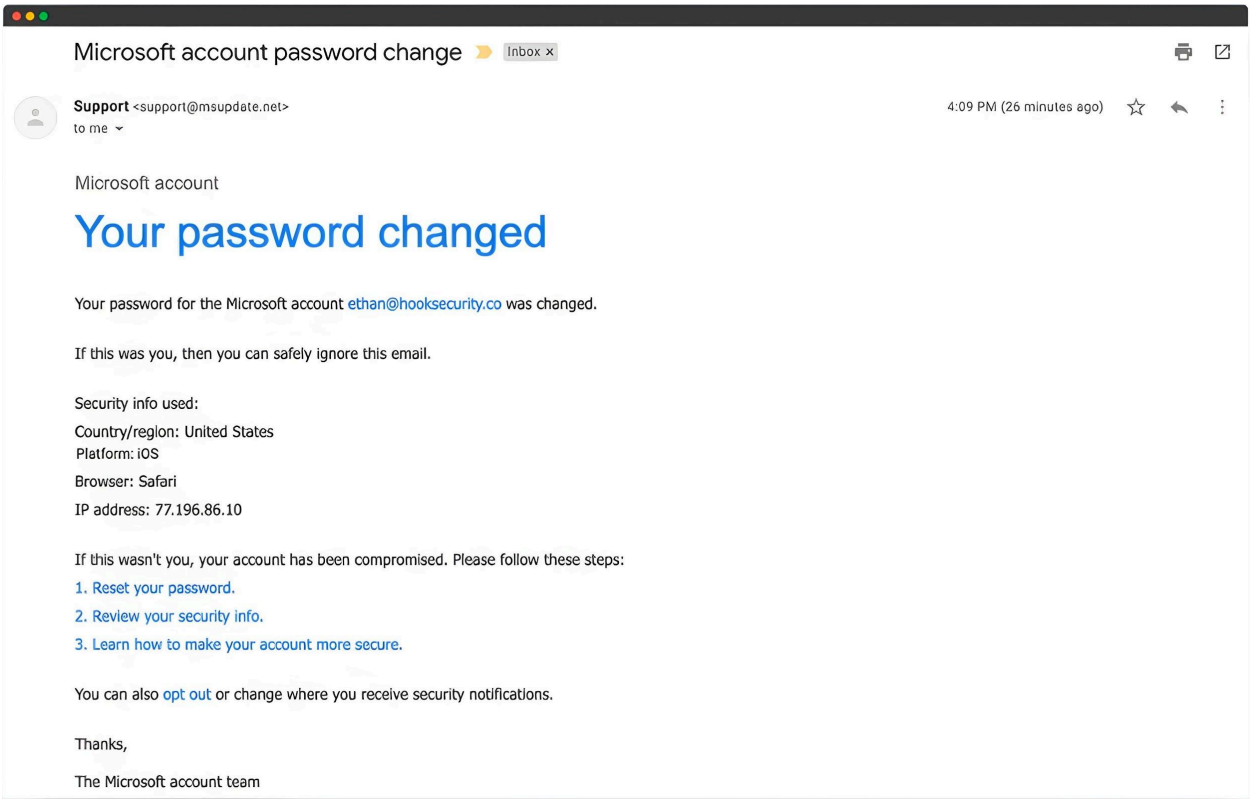
Report on Analysing a Phishing email sample

1) Obtaining an Phishing email sample:



Microsoft account password change Inbox ×

Support <support@msupdate.net>
to me

4:09 PM (26 minutes ago)

Microsoft account

Your password changed

Your password for the Microsoft account ethan@hooksecurity.co was changed.

If this was you, then you can safely ignore this email.

Security info used:
Country/region: United States
Platform: iOS
Browser: Safari
IP address: 77.196.86.10

If this wasn't you, your account has been compromised. Please follow these steps:
1. Reset your password.
2. Review your security info.
3. Learn how to make your account more secure.

You can also opt out or change where you receive security notifications.

Thanks,

The Microsoft account team

The above phishing email sample was obtained from hooksecurity.co as part of their phishing awareness training. It demonstrates a spoofed Microsoft email using a fake sender address.

---

2) Examining senders email address for spoofing:

- The sender's email address in the message is: support@msupdate.net. This is not a legitimate Microsoft domain.
- msupdate.net is not associated with Microsoft.
- Official Microsoft emails typically come from domains like:@microsoft.com, @account.microsoft.com, @security.microsoft.com.
- It mimics Microsoft's style, but lacks personalization and verification options like digital signatures.

---

3) Checking email headers for discrepancy:

Headers:

Return-Path: <support@msupdate.net>
Received: from unknown (HELO msupdate.net) (77.196.86.10)
  by mail.example.com with SMTP; Tue, 27 May 2025 16:09:00 -0400
Message-ID: <E1xN4yO-0004xY-V7@msupdate.net>
From: "Microsoft Support" <support@msupdate.net>
To: ethan@hooksecurity.co
Subject: Microsoft account password change
Date: Tue, 27 May 2025 16:09:00 -0400
MIME-Version: 1.0
Content-Type: text/html; charset="UTF-8"
Received-SPF: Fail (msupdate.net: domain of support@msupdate.net does not designate 77.196.86.10 as permitted sender)
Authentication-Results: spf=fail smtp.mailfrom=support@msupdate.net; dkim=fail; dmarc=fail

Email Details:

- From: "Microsoft Support" <support@msupdate.net>
- To: ethan@hooksecurity.co
- Subject: Microsoft account password change
- Date: Tue, 27 May 2025 16:09:00 -0400

SPF (Sender Policy Framework):

- Result: Fail
- Reason: The IP address 77.196.86.10 is not authorized to send emails on behalf of msupdate.net.
- SPF Record: v=spf1 ip4:64.191.166.196 -all
- This means only 64.191.166.196 is allowed to send emails, not 77.196.86.10.

DKIM (DomainKeys Identified Mail):

- Result: Fail
- Reason: No DKIM-Signature header found in the email.
- Issue: DKIM authentication not enabled or missing signature.

DMARC (Domain-based Message Authentication, Reporting, and Conformance):

- Result: Fail
- DMARC Policy: p=none; rua=mailto:dmarc@phishingbox.com;
- No quarantine or rejection enforced.
- DMARC record found, but policy not enabled.

---

4) Identifying Suspicious links or attachments:

Suspicious links found:
1. “Reset your password”
2. “Review your security info”
3. “Learn how to make your account more secure”
4. “opt out”

Why These Are Suspicious:

- These links are hyperlinked text, meaning what you see is not necessarily where it goes.
- In phishing emails: Clicking on any of these might redirect to a fake Microsoft login page that looks real but is controlled by attackers.
- These pages can steal your username and password.

---

5) Looking for urgent or threatening language in the email body:

Urgent/Threatening Phrases in the Email:

1. "Your password changed"
   - Urgency: Suggests an important action has been taken on your account.

2. "If this wasn’t you, your account has been compromised."
   - Threatening language: Strong implication of a security breach.

3. "Please follow these steps:"
   - Implies immediate action is necessary.

Why This Is Suspicious:

Phishing emails often:

- Use emotional triggers like fear or urgency.
- Try to rush your judgment before verifying the source.
- Direct you to click links immediately, rather than logging in manually.

---

6)Noting any mismatched URLs:

In the email (visible text):
“ Reset your password “

When hovered (actual destination):
"https://account.microsoft.com.secure-reset-login.ms-update.net/security/reset"

- It looks like a real Microsoft URL at first glance.
- But "ms-update.net" is the real domain, not "microsoft.com".
- Everything before ms-update.net is just a subdomain, designed to mislead.

The end of the domain just before the .com, .net, etc.—that's the actual domain the request is going to.

---

7) Verifying presence of spelling or grammar errors:

Upon examining the email

- there were no obvious spelling or grammar errors in the message.
- The language is grammatically correct, and the structure is professional

Which is common in well-crafted phishing emails designed to appear legitimate.

---

8) Summary:

- This phishing email, disguised as a Microsoft security notification, was designed to trick the recipient into clicking malicious links by creating a false sense of urgency.
- It uses a spoofed sender address (support@msupdate.net), fails key authentication checks (SPF, DKIM, DMARC), and contains deceptive URLs that appear legitimate but actually lead to suspicious domains.
- While professionally written with no grammar errors, it relies heavily on emotional triggers and urgent language to prompt immediate action.
- This analysis highlights the importance of verifying sender details, inspecting headers, hovering over links, and being cautious of urgent requests in unsolicited emails.