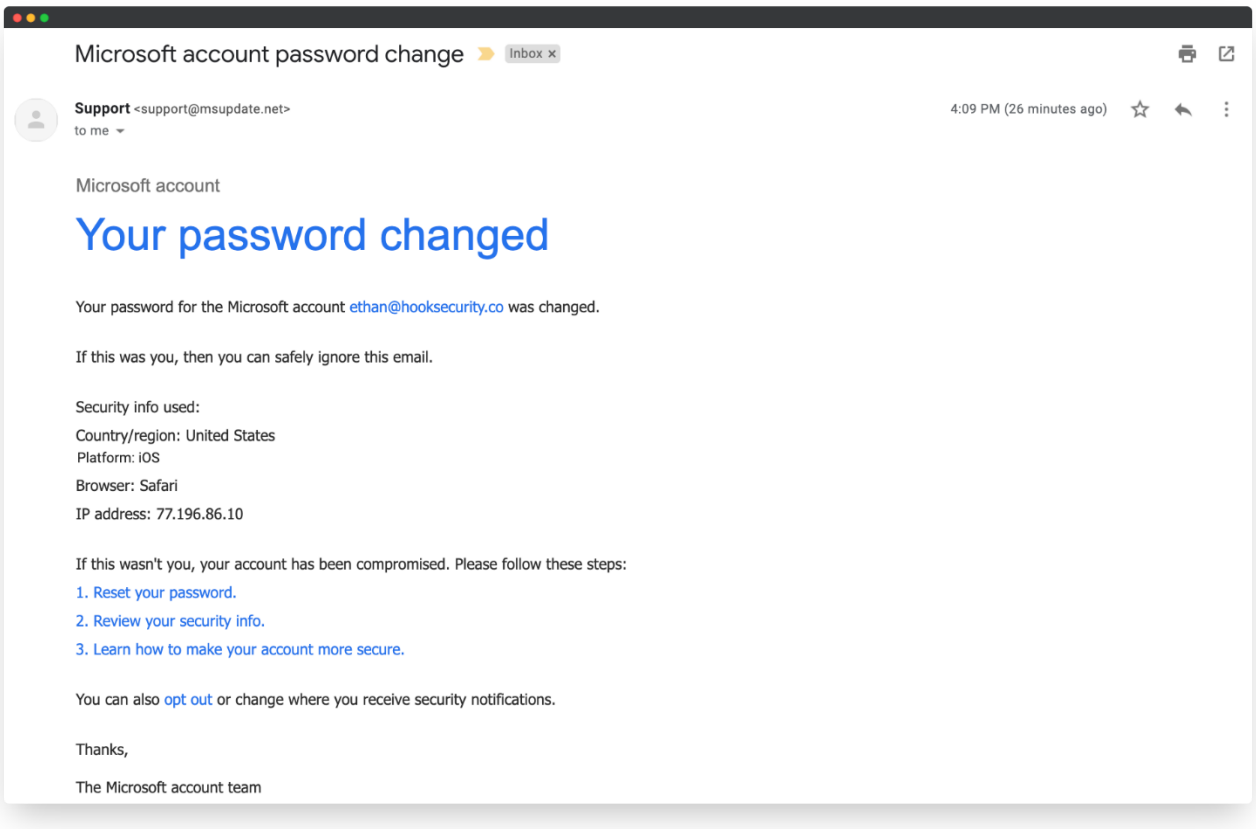
Task 2

Phishing Email



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

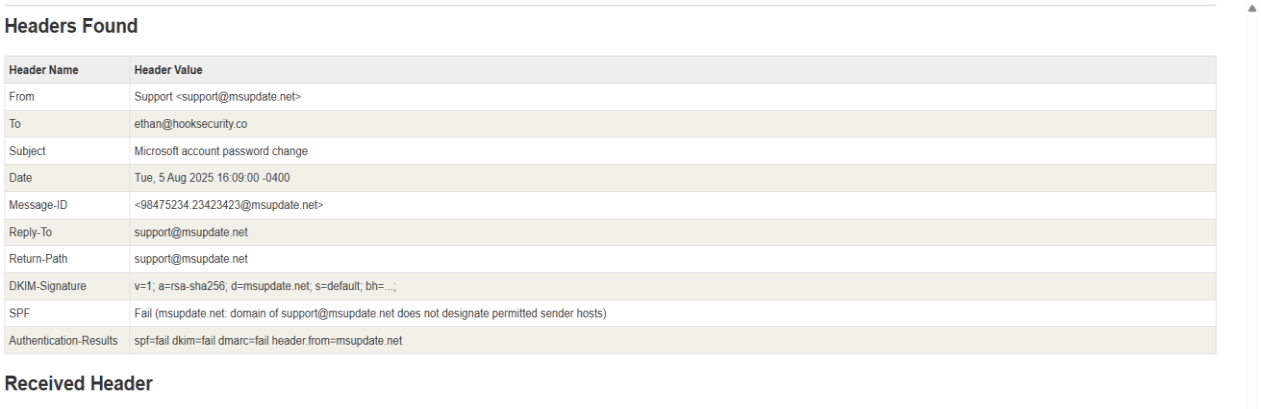
If this wasn't you, your account has been compromised. Please follow these steps:
1. Reset your password.
2. Review your security info.
3. Learn how to make your account more secure.

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

Thanks,

The Microsoft account team

Email Hader Analyser



Headers Found

Header Name	Header Value
From	Support <support@msupdate.net>
To	ethan@hooksecurity.co
Subject	Microsoft account password change
Date	Tue, 5 Aug 2025 16:09:00 -0400
Message-ID	<98475234.23423423@msupdate.net>
Reply-To	support@msupdate.net
Return-Path	support@msupdate.net
DKIM-Signature	v=1; a=rsa-sha256; d=msupdate.net; s=default; bh=...;
SPF	Fail (msupdate.net: domain of support@msupdate.net does not designate permitted sender hosts)
Authentication-Results	spf=fail dkim=fail dmarc=fail header.from=msupdate.net

Received Header

How does this phishing email

1 Suspicious Sender Email Address

The "From" field shows Support <support@msupdate.net>.

The email address does not use the official Microsoft domain (@microsoft.com or a verified subdomain like @account.microsoft.com). Instead, it uses a similar-looking but fake domain, msupdate.net, which is a classic tactic to deceive users.

2. Recipient's Email Address

The email states, "Your password for the Microsoft account ethan@hooksecurity.co was changed."

This is a crucial detail. The email is addressed to the recipient, but it claims to be about an account that belongs to ethan@hooksecurity.co. This is a clear sign that the email is not genuinely from Microsoft about the recipient's account. It's a template designed to confuse a user into thinking a different account was compromised, leading them to panic and click the links.

3. Malicious Links:

The email provides three links:

1. Reset your password.
2. Review your security info.
3. Learn how to make your account more secure.

While I cannot see the actual URLs that these links point to, in a phishing email, they would lead to a fake website that mimics the Microsoft login page. The goal is to trick you into entering your real password on the fake site, which the attackers can then steal. The use of phrases like "Reset your password" and "Review your security info" is a social engineering tactic to create a sense of urgency and direct you to the malicious site.

4. Social Engineering and Urgency

The email's subject is "Microsoft account password change," and the body implies that if the user did not make this change, their account has been "compromised."

This is designed to create a sense of panic. The email gives you a simple choice: "If this was you, then you can safely ignore this email. If this wasn't you, your account has been compromised." This framing pushes the user to believe their account is in danger, making them more likely to click the malicious links to "fix" the problem without thinking critically.

5. Lack of Personalization:

The email uses a generic greeting and refers to an account with a different email address.

A legitimate security notification from a company like Microsoft would be highly personalized, addressing you by name and providing specific details about your account, not a different one. The lack of personalization is a common red flag in mass phishing campaigns.

6. Grammatical Errors/Awkward Phrasing:

The grammar and phrasing are mostly correct, but the overall structure and flow feel slightly unnatural for a major corporation. The email is a bit brief and lacks the polished, professional tone you would expect from a company like Microsoft.