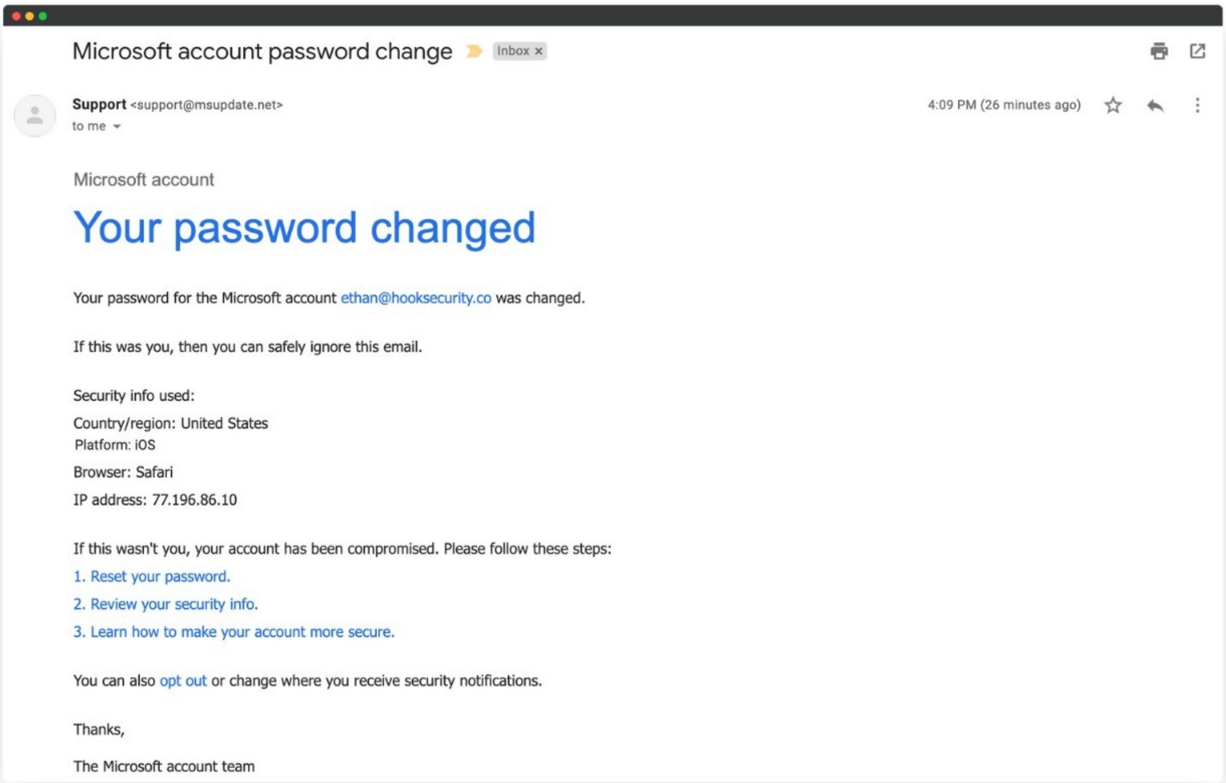

Microsoft account password change

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

Phishing Email Analysis Report

1. Overview

This document details the analysis of a phishing email impersonating Microsoft. The goal is to identify common phishing indicators and document them for educational and security awareness purposes.

2. Email Subject and Sender

Subject: "Microsoft account password change"

Sender Name: "Support"

Sender Email Address: support@msupdate.net

Analysis:
The subject line is designed to create a sense of urgency and alarm, prompting the recipient to take immediate action. The sender's name "Support" is generic and meant to appear official. The sender's email address, support@msupdate.net, is a significant red flag. While it uses "msupdate," it does not originate from a legitimate Microsoft domain (e.g., microsoft.com, accountprotection.microsoft.com). This is a classic tactic to deceive users who may not scrutinize the full email address.

3. Email Body and Content

Greeting: "Microsoft account" (generic, no personalization)

Key Message: "Your password changed"

Account Mentioned: ethan@hooksecurity.co

Analysis:
The email body lacks personalization, which is common in mass-sent phishing campaigns. A legitimate notification would likely address the user by name. The message aims to create panic by stating the password has been changed, even though the recipient did not initiate the change. This is a social engineering tactic to make the user click on the provided links. The email also mentions a specific email address, ethan@hooksecurity.co, which may be a legitimate account used by the attacker or a decoy.

4. Phishing Indicators

The email contains several key indicators of a phishing attempt:

Sender Domain Mismatch: The sender's email (msupdate.net) does not match the official domain of the impersonated company (Microsoft).

Urgency and Threat: The subject and body create a false sense of urgency and threat ("Your password changed," "your account has been compromised").

Generic Salutation: The lack of a personalized greeting (e.g., "Dear [User Name]") is a common red flag.

Suspicious Links: The email contains three links:

Reset your password.

Review your security info.

Learn how to make your account more secure.

Hypothesis: These links, if clicked, would not lead to the legitimate Microsoft website. Instead, they would likely direct the user to a fake login page designed to steal credentials. The opt out link at the bottom is also a tactic to add a veneer of legitimacy while potentially leading to another malicious page or a non-functional link.

Unusual "Security Info" details: The email provides "Security info used," including a Country/region, Platform, Browser, and IP address.

IP Address: 77.196.86.10

Analysis: Attackers often include this type of information to make the email seem more credible and specific. A quick search of the provided IP address may reveal its origin, which is often inconsistent with the purported location (e.g., the IP address may be from a different country than the "United States" claimed in the email).

5. Summary of Red Flags

Indicator	Details
Sender Email	support@msupdate.net (not a legitimate Microsoft domain)
Subject Line	Creates a sense of urgency and alarm
Body Content	Impersonal and designed to trigger an emotional response
Call to Action	Asks the user to click on suspicious links
Provided Information	The "Security info used" section is likely fabricated to appear legitimate

6. Mitigation and Best Practices

Do not click on any links.

Do not reply to the email.

Do not download any attachments.

Report the email as a phishing attempt.

Navigate directly to the official Microsoft website (e.g., https://account.microsoft.com) through a web browser to check account activity or change your password.

Be vigilant. Always verify the sender's email address and hover over links to check the destination URL before clicking.

Enable Multi-Factor Authentication (MFA) on all your accounts to add a crucial layer of security, even if your password is compromised.