Phishing email analysis

Phishing emails are fraudulent messages designed to trick recipients into providing personal information or downloading malware. They often mimic legitimate companies or services to appear trustworthy. Phishing emails are becoming more and more common. They can be very convincing for even the most experienced Internet users. Phishers use various techniques to fool people into clicking on links or opening attachments that could lead to viruses or malware downloads onto your system, while at the same time stealing personal information like passwords and credit card numbers which they then use for their own purposes such as identity theft or money.

How to identify phishing emails

Phishing emails often:

- Seem to be from legitimate companies like banks, internet service providers, credit card companies, etc.

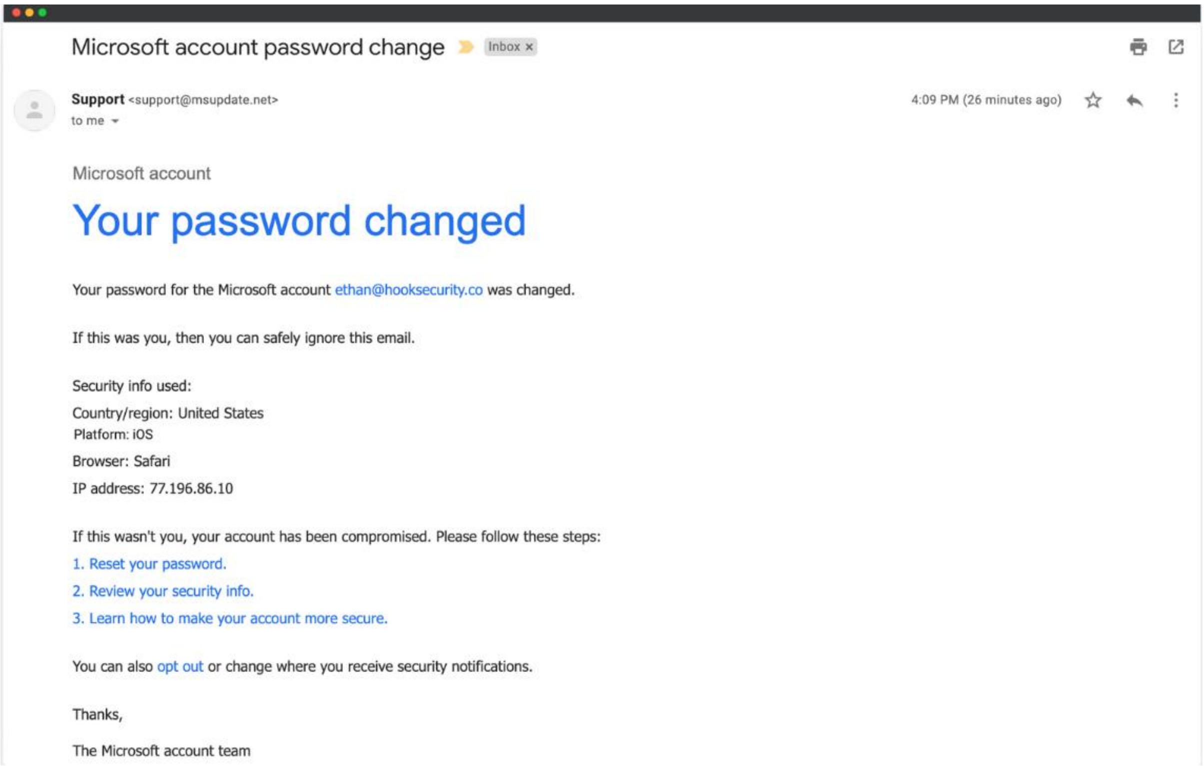
- Are unsolicited (you didn't ask for it; they just sent it to you)

- Ask for things like usernames, passwords, account numbers, etc.

- Offer something seemingly valuable, like a prize or discount - Use poor spelling and grammar

- Have strange email addresses or typos in the email address - Have crazy titles

#Example



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

From the sample mail above :

- We could see the mail sender is support@msupdate.net , Microsoft will never use a domain like msupdate.net. They use:@microsoft.com or @account.microsoft.com
- Phishing emails often create panic to trick you into clicking , here they say that you changed your password when you actually didn’t.
- Multiple links are provided; these are likely fake links. If you **hover your mouse** (don’t click), you may see that the link doesn't go to a real Microsoft domain.
- No personal greeting (e.g., “Hi Ethan” or “Dear Ethan”)
- No official Microsoft branding (e.g., logos, security seals)
- Poor structure and basic text styling

What You Should Do

1. Do not click any links in the email.
2. Report it as phishing in your email provider (Gmail, Outlook, etc.).
3. If it concerns your real Microsoft account:
   - Go directly to https://account.microsoft.com
   - Log in manually and check recent activity and security settings.
4. Change your password immediately if you think your credentials were compromised.