

Phishing Assessment

Module 3.1: Spot Phishing Email

Table of Contents

1. Demonstration

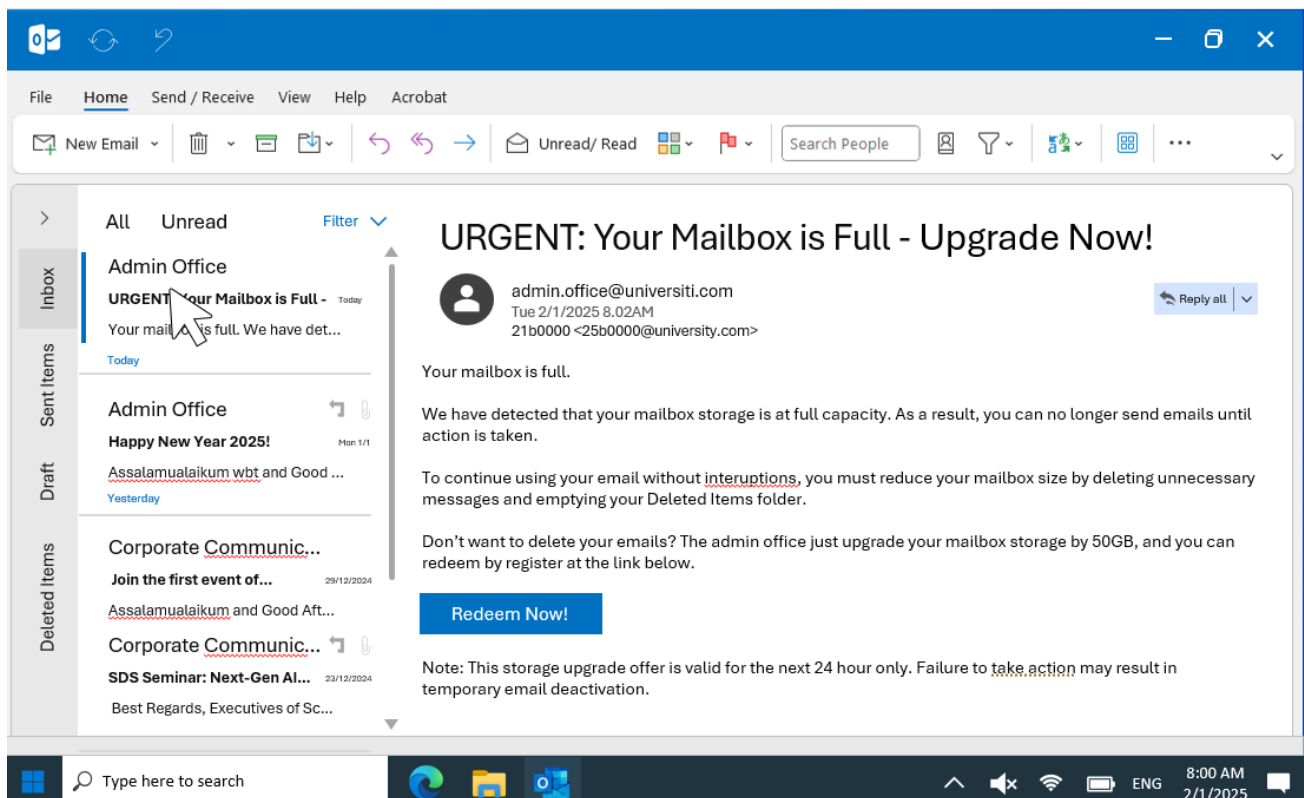
2. Countermeasure

1. Demonstration

Receiving a Suspicious Email

You're sitting at your desk, about to check your Outlook inbox. Suddenly, you receive a new email from **admin.office@universiti.com**.

The email content:



The email contains **phishing characteristics**:

- Suspicious Sender Address

The sender address looks official, but it's slightly different from the real domain — The domain should be university with letter Y not I, and Also, official emails usually display a proper name, like "Admin Office," not a full, unusual email address. The domain appears similar to a legitimate one but is fraudulent.

- Urgency & Threats

The email claims the mailbox is full and threatens service interruption. The email pressures you to act fast, saying your account will be deactivated within 24 hours. This is a classic phishing tactic—attackers want you to panic and click without thinking.

- Poor Grammar & Spelling Errors

There is awkward wording and typos. The email contains spelling errors and awkward grammar, another clue that this email isn't from a real administrator.

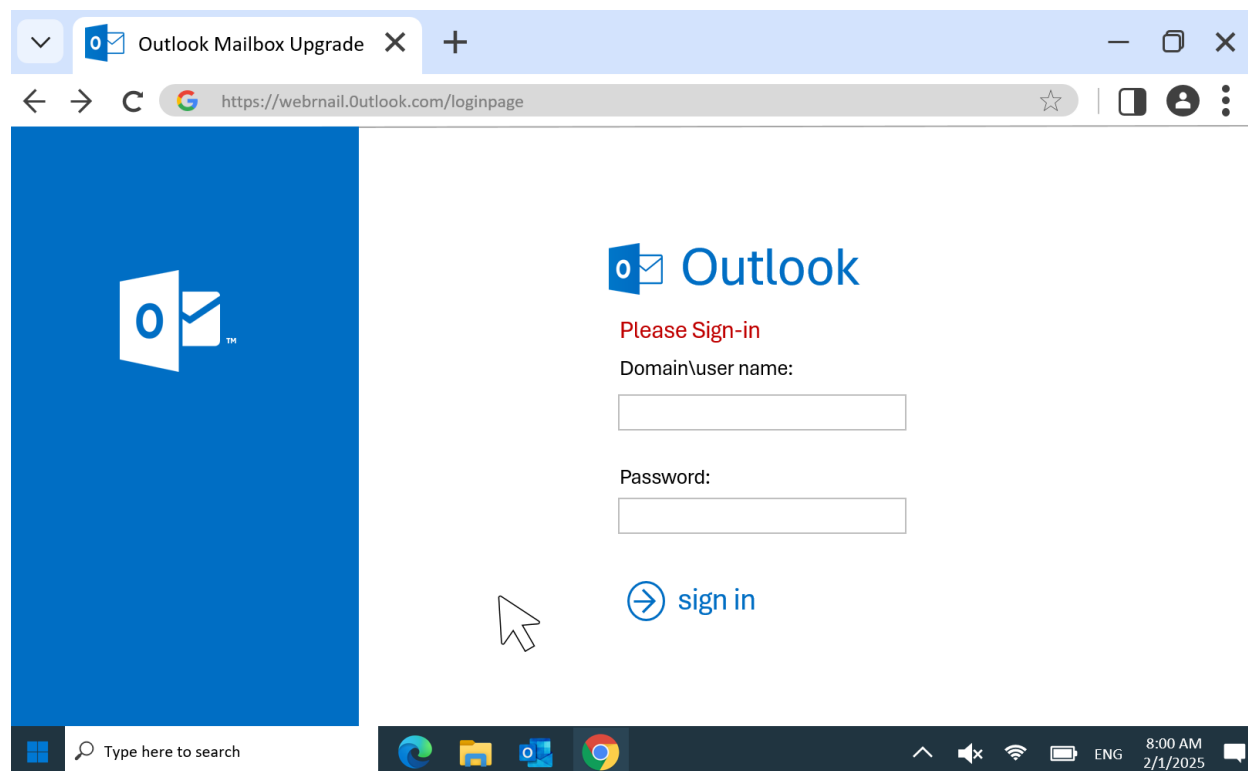
- Fake Links

The email offers a misleading link to increase storage. This looks suspicious.

Clicking on the Phishing Link

The browser opens a page: <https://webnail.Outlook.com/loginpage>.

the website design:



It mimics a legitimate Microsoft Outlook login page. The web page design mimics Microsoft Outlook but notice the subtle difference in the URL—it's not an official Microsoft domain. "webnail" is not associated with Outlook domain. The correct domain is "outlook.com".

The "o" in outlook is replaced with a "0". This is a very common trick used in phishing attacks.

While legitimate websites may have login pages, the explicit use of "loginpage" in the URL, especially combined with the other red flags, is suspicious.

Entering Credentials

Entering email and password on the fake login page. Then, clicking the "Sign In" button.

The page redirects to a fake registration form asking for additional sensitive details: full name, identity number, date of birth, nationality, phone number, home address, and personal email:

The registration form page:

Outlook Mailbox Upgrade

https://webmail.Outlook.com/registerpage

Outlook

Please Register

Full name :

Date of birth : Home address :

IC No. :

Nationality : Personal email :

Phone No. :

Register

Type here to search

8:00 AM 2/1/2025

This is another red flag—real login pages don't ask for extra personal details after signing in.

***The moment you enter your credentials, they are sent directly to the attacker.**

Consequences of Entering Credentials

PAST

Demonstration

Module 3.1
Spot Phishing Email

By falling for this email phishing, what happens next?



Captures Login Credentials



Send More Phishing Emails



The Dark Web

Page 4 of 6

Captures Login Credentials: The attacker immediately captures your login credentials. They log into your email, change your password, and lock you out. They also have access your personal and professional emails, contacts, and data stored in your email.

Send More Phishing Emails: They can use your account to send more phishing emails and trick others into falling victim. Because emails come from a trusted source (you), your friends, colleagues, or clients are more likely to fall for the scam. They might impersonate you and ask for sensitive data, financial transactions, or spread malware.

The Dark Web: Your stolen personal details can be sold on the dark web. Hackers trade and sell login details in bulk, allowing other cybercriminals to exploit them.





2. Countermeasure

PAST

Countermeasure

Module 3.1
Spot Phishing Email

What to do next?

Disconnect Immediately

Change Your Password ASAP

Monitor Your Accounts

Report Phishing Attack

Page 5 of 6

What to Do If You've Been Phished: Damage Control

- Disconnect Immediately**

If you clicked on a phishing link and entered your credentials, disconnect from the internet (especially if you're on a company network). This prevents further unauthorized access to your device.

- Change Your Password ASAP**

If you entered your credentials on a phishing site, change your password immediately. Use a strong, unique password that isn't used for other accounts.

- Monitor Your Accounts for Suspicious Activity**

If your email is linked to banking or social media, watch for unusual login attempts or unauthorized transactions. Check your email for unauthorized access and set up alerts for suspicious activity in your email and banking apps.

- **Report the Phishing Attack**

If you are at work, report it to your IT/security team immediately.

If the email is on your personal email, report the phishing email to:

- If Microsoft: reportphishing@office365.microsoft.com
- If Google: reportphishing@google.com
- Or Your email provider's "Report Phishing" feature.
- Police or Cybersecurity agencies.

Summary

Phishing attacks don't break into systems; they trick people into opening the door. Hackers don't need to break in if they can trick you into letting them in. Stay alert and stay secure.

- END -