MOS USER SECURITY GUIDE

Guide #003

Spot a Phishing Email

How to identify suspicious emails and protect company data

Phishing emails try to trick you into giving away your password, clicking dangerous links, or downloading malware. This guide teaches you the warning signs and what to do when you spot one.

Jean Claude Munyakazi | IT Systems Administrator | Magister Operis Systems

munyakazi.org

🏢 COMPANY POLICY

MOS Email Security Policy §4.1:

- Never click links in unexpected emails without verifying the sender
- Never open attachments you were not expecting
- Report suspicious emails to IT within 1 hour
- Do NOT forward suspicious emails to colleagues
- If in doubt, delete it and contact IT

Violating this policy may result in a security incident report.

⚠ WHY THIS MATTERS

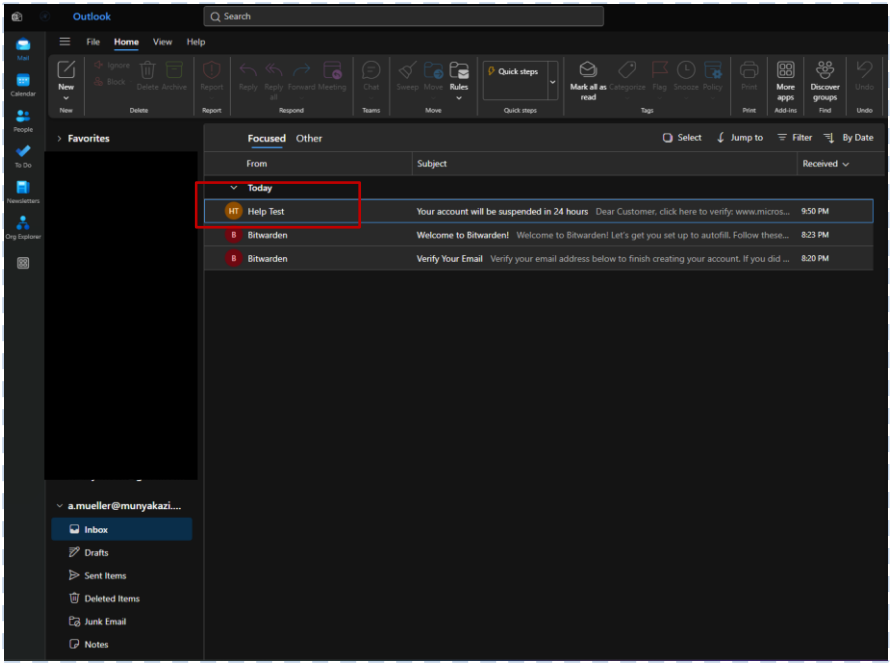
Phishing is responsible for 90% of all cyberattacks. One click on a malicious link can:

- Give attackers full access to your account
- Install malware on your computer and the company network
- Lead to a data breach affecting clients and colleagues

IT security tools help but CANNOT catch everything. You are the last line of defence.

STEP 1

Check the Sender's Email Address



INSTRUCTIONS

Before opening any email, look at the FULL email address, not just the display name:

✅ Real: support@microsoft.com
❌ Fake: support@micros0ft-help.com
❌ Fake: microsoft.support@gmail.com
❌ Fake: htest054@gmail.com

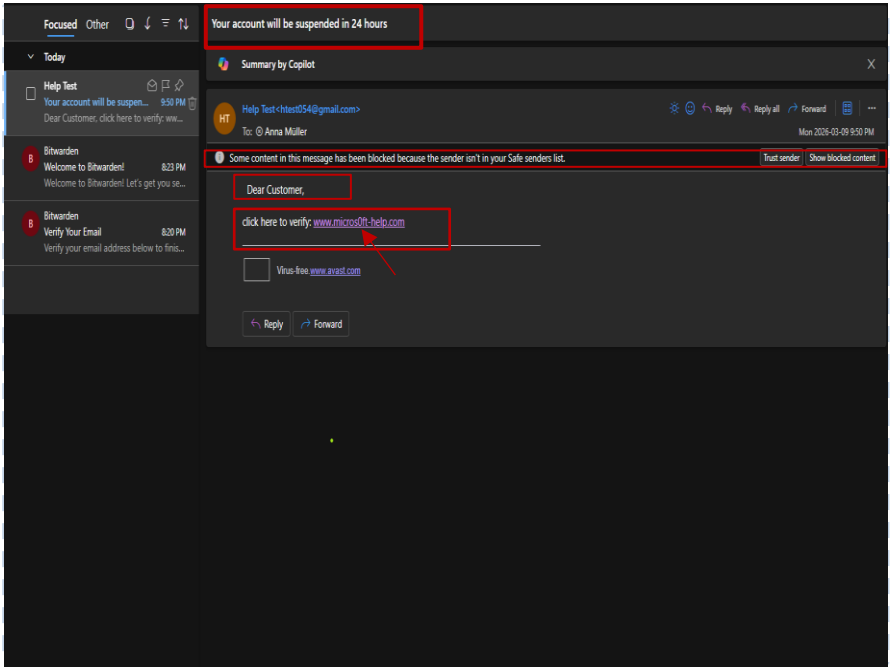
Attackers use:

- Misspelled domains (micros0ft, arnazon)
- Extra words added (microsoft-security-alert.com)
- Legitimate-looking names with fake domains

→ If the domain looks wrong, do not click anything

STEP 2

Look for These Red Flags in the Email



INSTRUCTIONS

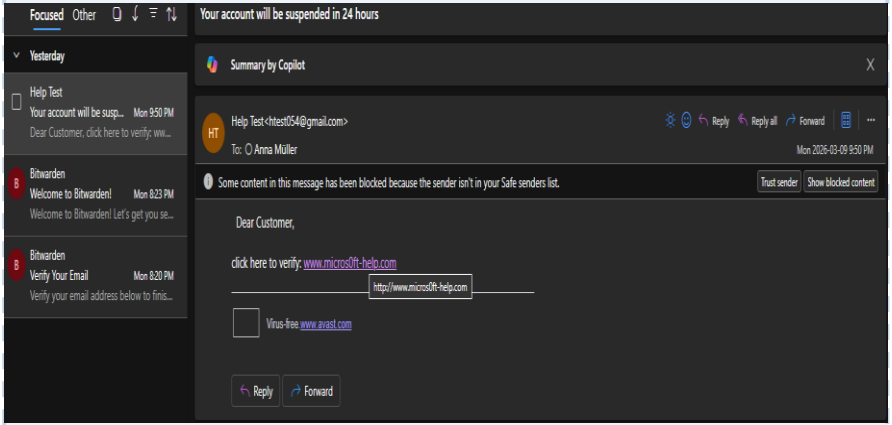
Warning signs to look for:

- 🚨 Urgent language: 'Your account will be suspended in 24 hours!'
- 🚨 Unexpected requests: 'Click here to verify your password'
- 🚨 Generic greeting: 'Dear User' or 'Dear Customer'
- 🚨 Grammar mistakes and unusual phrasing
- 🚨 Links that don't match the company they claim to be from
- 🚨 Unexpected attachments: .zip, .exe, .docm files

→ Legitimate companies never ask for passwords by email

STEP 3

Check Links Before Clicking



INSTRUCTIONS

BEFORE clicking any link in an email:

1. Hover your mouse over the link (don't click)

2. Look at the URL shown at the bottom of your browser

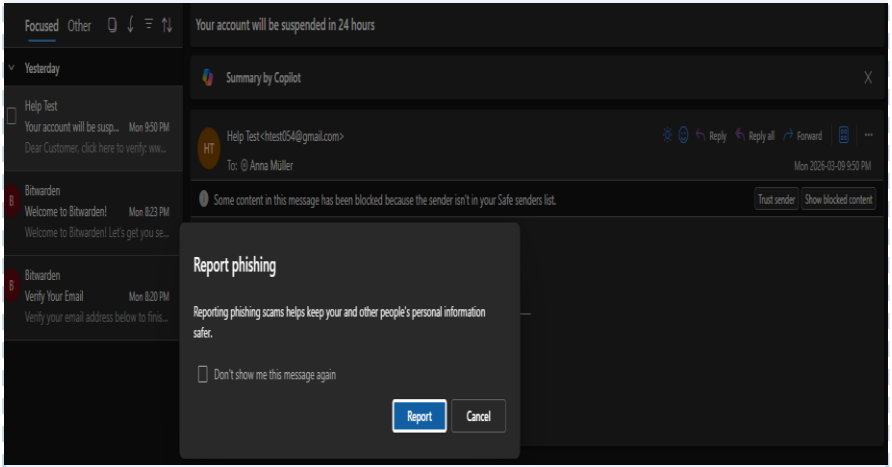
3. Ask yourself: does this match the company?
✅ microsoft.com/account
❌ www.micros0ft-help.com

4. If you are unsure, go directly to the website by typing the address yourself

→ Never copy/paste links from suspicious emails

STEP 4

Report a Suspicious Email to IT



INSTRUCTIONS

If you receive a suspicious email:

1. Do NOT click any links or open attachments

2. Do NOT reply to the email

3. In Outlook: click the three dots (...) menu

4. Select: Report → Report phishing
   OR forward as attachment to: itsupport@munyakazi.org

5. Delete the email from your inbox

→ Reporting helps IT block the sender for everyone at MOS

What NOT To Do

Don't click links to 'verify your account'

Legitimate services will never email you asking to verify your password or account via a link.

Don't ignore it and just delete without reporting

Reporting suspicious emails to IT helps protect all 23 MOS users, not just yourself.

Don't open unexpected attachments

Even from people you know, their account may have been compromised. Confirm by phone if unsure.

Don't forward the suspicious email to colleagues

This spreads the threat. Report to IT only, never share suspicious content with other staff.

Don't enter passwords on pages reached via email

Always go directly to the website by typing the address. Never follow email links to login pages.

Don't trust the display name alone

The name shown ('Microsoft Support') can be faked. Always check the actual email address behind it.

Need Help? Contact IT

IT Helpdesk Chat

Teams → MOS IT Support
Channel: Incidents

Email Support

itsupport@munyakazi.org
Response within 4 hours

Urgent Security Issue

Call your manager immediately
Do NOT wait for email response

Remember: IT will NEVER ask for your password over email, chat, or phone.

✅ Quick Summary

Spot a Phishing Email

1. Always check the FULL email address, not just the display name
2. Look for urgency, grammar mistakes, generic greetings, and suspicious links
3. Hover over links before clicking to see the real destination URL
4. Never enter your password on a page you reached by clicking an email link
5. Report suspicious emails via Outlook → Report → Report phishing
6. When in doubt, delete and contact IT. Better safe than sorry.