



PHISHING AWARENESS & EMAIL SECURITY

A PRACTICAL GUIDE TO IDENTIFYING AND AVOIDING PHISHING THREATS.

“CLICK SMART, STAY SAFE”

📌 **Prepared By:** Akarsh Gautam

📌 **Internship Project:** Phishing Link Detector Tool & Awareness Training.

INTRODUCTION

Phishing is one of the most common and dangerous forms of cybercrime. It involves tricking individuals into revealing sensitive information, such as **passwords, banking details, or personal data**, through **deceptive emails, fake websites, or malicious links**.

Why This Matters:

1. **91%** of cyberattacks start with a phishing email.
2. Phishing causes billions in financial losses annually.
3. Even a single click on a malicious link can compromise an entire organization's network.
4. This training will help you **recognize, avoid, and report phishing attempts** effectively.

WHAT IS PHISHING?

Phishing is a **fraudulent attempt** to obtain confidential information by disguising as a **trustworthy entity**.

Common Forms:

- 1.Email Phishing** – Fake emails claiming to be from banks, companies, or services.
- 2.Spear Phishing** – Targeted attacks on specific individuals or organizations.
- 3.Smishing** – Phishing via SMS messages.
- 4.Vishing** – Phishing via phone calls.
- 5.Clone Phishing** – A legitimate email is copied and resent with a malicious link.

Example Fake Email:

From: PayPal Security <support@paypai.com>

Subject: Urgent – Your account is on hold

Message: Click here to verify your account immediately.

(Note: “paypai.com” instead of “paypal.com” is a classic sign of a phishing domain.)

HOW TO RECOGNIZE PHISHING EMAILS

Key Warning Signs:

- **Suspicious Sender:** The email address is slightly misspelled or from an unknown domain.
- **Generic Greeting:** “Dear Customer” instead of using your name.
- **Urgency or Threats:** “Your account will be suspended in 24 hours!”
- **Links to Fake Websites:** Hover over links to check the real URL.
- **Poor Grammar & Spelling:** Many phishing messages have noticeable language mistakes.
- **Unexpected Attachments:** Could contain malware.

Example:

A fake Microsoft email asking to “reset password” with a suspicious link to

microsoft-support-login.com

REAL-WORLD EXAMPLE

Spam Email Example:

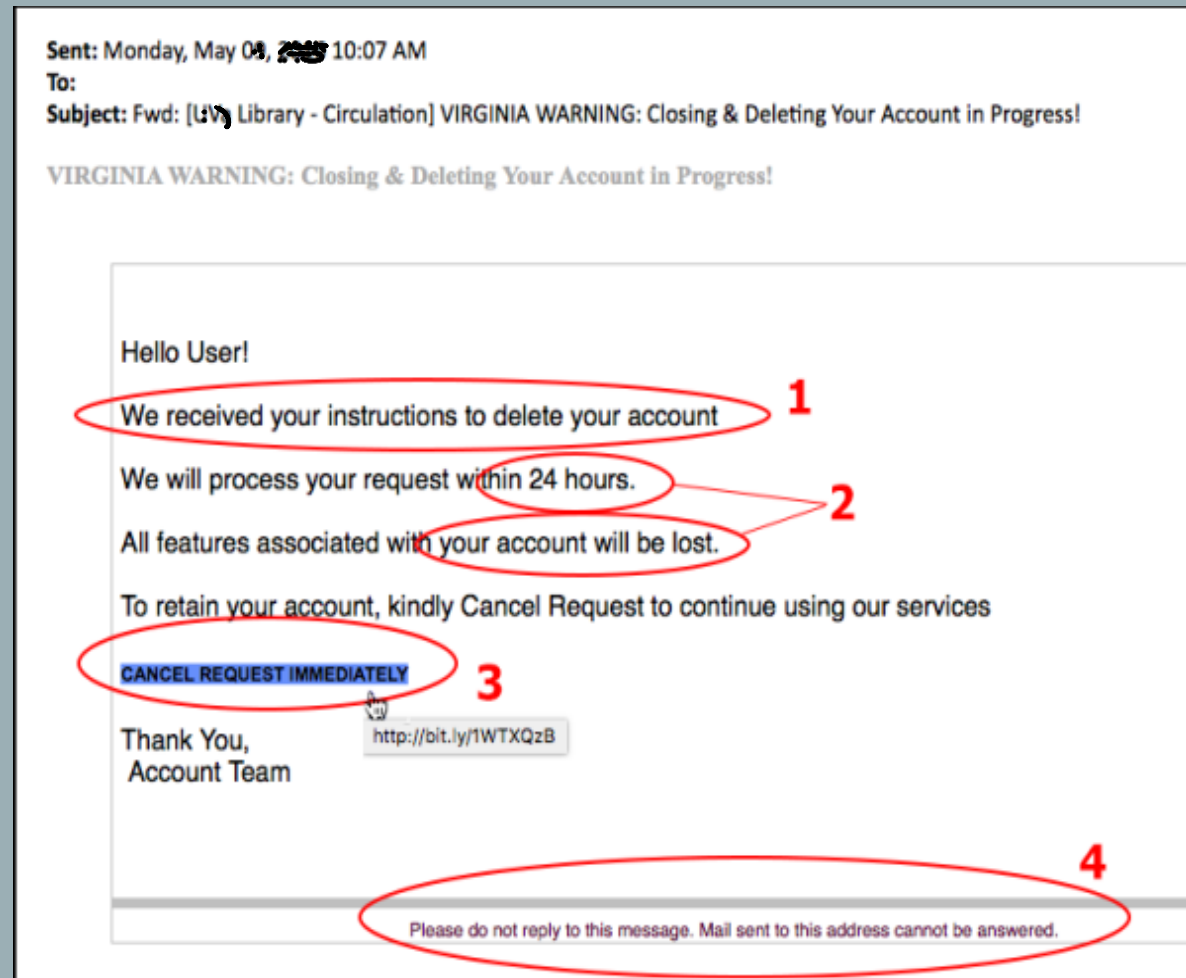
Subject: “Security Alert – Your Account Has Been Compromised!”

Body:

“Your account has been accessed from an unknown location.

To secure your account, click the link below and verify your details immediately.”

Link leads to **secure-login-verify-account.xyz** instead of the official website.



FAKE WEBSITE INDICATORS

When you click a phishing link, it often leads to a fake login page.

How to Spot Them:

- **URL Mismatch:** Domain name is misspelled or unusual.
- **No HTTPS:** Missing the padlock icon.
- **Poor Design:** Low-quality logos or mismatched fonts.
- **Requests for Sensitive Data:** Asking for full password, card details, or OTP.

Example:

A fake Google login page with URL

accounts.google.support-login.com

instead of accounts.google.com

LINK MANIPULATION

Phishing links often mimic a real websites but might include variations like misspellings, non-Latin characters, and shortened URLs.

Manipulating the links for example

www.faceb00k.com

Instead of

www.facebook.com

Real Link

<https://au.norton.com/>

Phishing Link

<https://au.noorton.com/>

SOCIAL ENGINEERING IN PHISHING

Phishing is more than just fake links — it's **psychological manipulation**.

Tactics Used:

1. **Urgency**: “Act now or lose access.”
2. **Fear**: “Your account will be blocked.”
3. **Greed**: “You have won a prize.”
4. **Curiosity**: “See this confidential document.”

Example:

An email saying “*Invoice attached – urgent payment needed*” to trick finance teams.

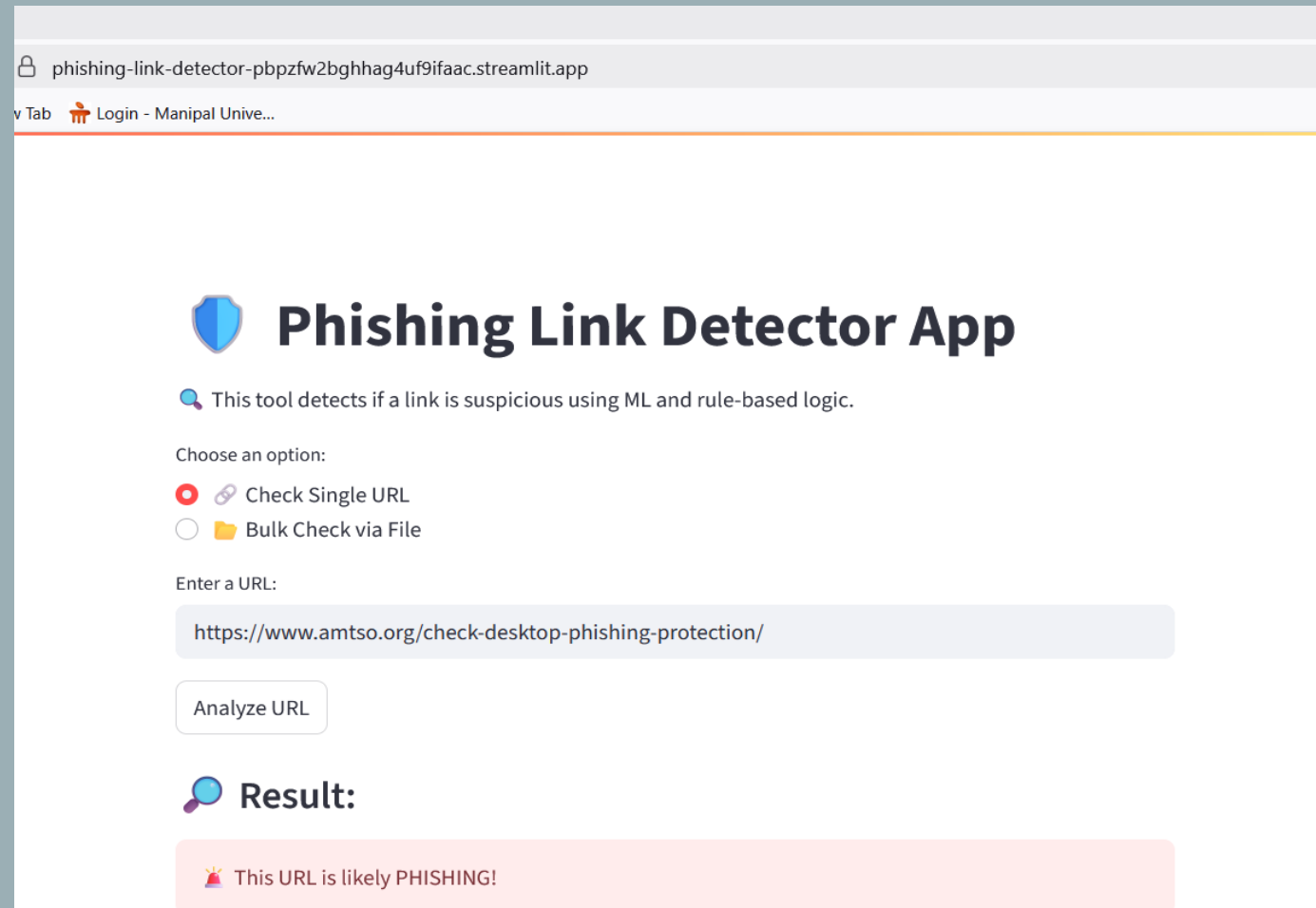
BEST PRACTICES TO AVOID PHISHING

- ✓ Verify the sender's email address before clicking links.
- ✓ Hover over links to check the real URL before clicking.
- ✓ Do not open unexpected attachments from unknown sources.
- ✓ Use multi-factor authentication (MFA) for extra security.
- ✓ Report suspicious emails to your IT/security team.
- ✓ Keep your browser and antivirus software updated

MY LIVE PROJECT: PHISHING LINK DETECTOR

As part of my internship, I developed a **Phishing Link Detector** tool that:

1. **Analyzes URLs in real time**
2. **Checks against threat intelligence databases**
3. **Identifies suspicious/malicious domains**
4. **Provides an instant “Safe” or “Phishing” status**




The screenshot shows a web browser window with the address bar displaying 'phishing-link-detector-pbpzfw2bgghag4uf9ifaac.streamlit.app'. The browser tab is labeled 'v Tab' and 'Login - Manipal Unive...'. The main content area features a blue shield icon with a white checkmark, followed by the title 'Phishing Link Detector App'. Below the title, a magnifying glass icon is followed by the text 'This tool detects if a link is suspicious using ML and rule-based logic.' Underneath, the text 'Choose an option:' is followed by two radio button options: 'Check Single URL' (selected) and 'Bulk Check via File'. Below these options, the text 'Enter a URL:' is followed by a text input field containing the URL 'https://www.amtso.org/check-desktop-phishing-protection/'. A button labeled 'Analyze URL' is positioned below the input field. The results section, titled 'Result:' with a magnifying glass icon, shows a red alert icon followed by the text 'This URL is likely PHISHING!'.


phishing-link-detector-pbpzfw2bgghag4uf9ifaac.streamlit.app


v Tab Login - Manipal Unive...

Phishing Link Detector App

 This tool detects if a link is suspicious using ML and rule-based logic.


Choose an option:


☒  Check Single URL

☐  Bulk Check via File

Enter a URL:

Analyze URL

 **Result:**

 This URL is likely PHISHING!

CONCLUSION

Phishing remains one of the **biggest cybersecurity threats** today, but with awareness and the right tools, we can prevent most attacks.

Key Takeaways:

1. Always **verify before you click**
2. Awareness is your **first line of defense**
3. Tools like **Phishing Link Detector** can provide extra protection



Remember: It only takes one careless click to cause a major security breach.

CONTACT & ACKNOWLEDGMENTS

Prepared By: Akarsh Gautam

Project: Phishing Link Detector & awareness Training

LinkedIn: <https://www.linkedin.com/in/akarsh-gautam-ba62292a3>

GitHub: <https://github.com/Akarsh-gautam24>

Project Link: <https://phishing-link-detector-pbpzfw2bghhag4uf9ifaac.streamlit.app/>