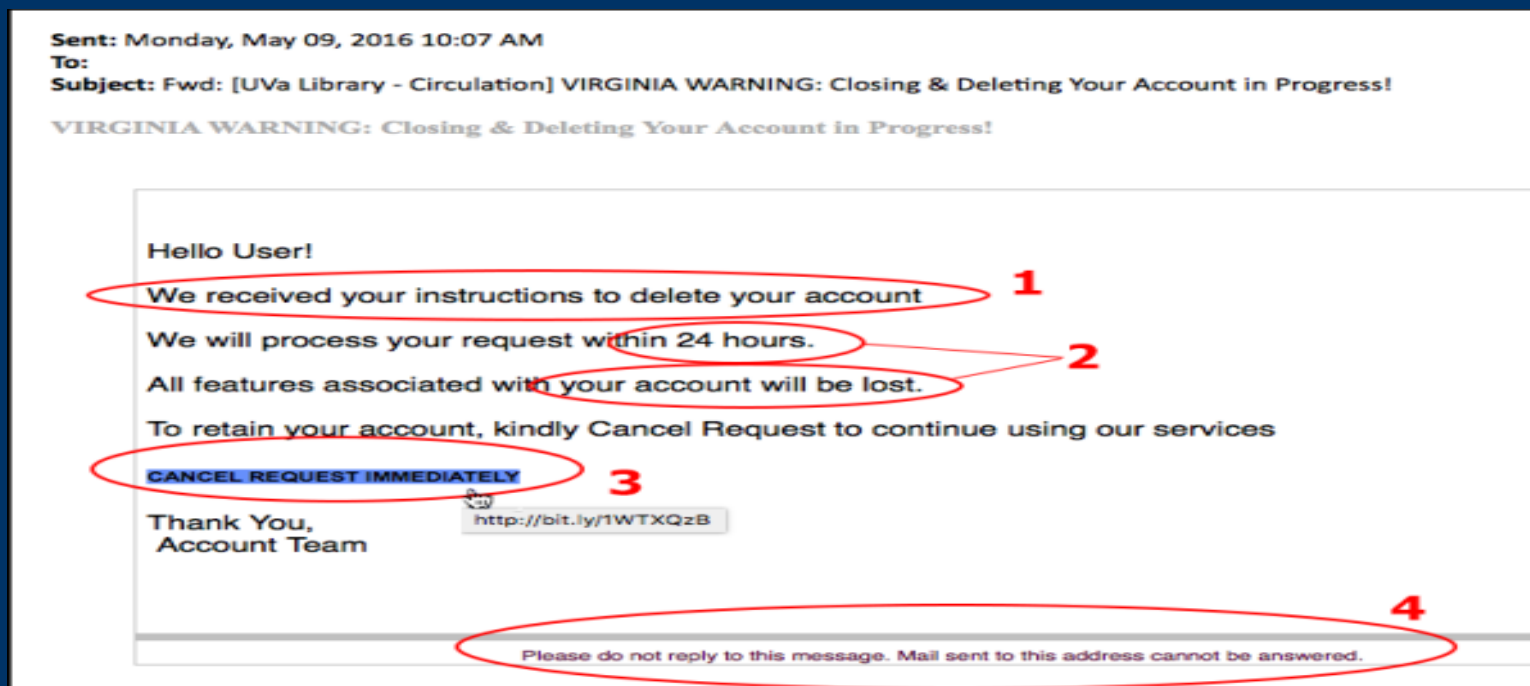


Understanding and Preventing Phishing Attacks

- Learn how to identify, avoid, and defend against phishing attacks and social engineering tactics.

Recognizing Phishing Emails

- - Suspicious sender addresses
- - Generic greetings like 'Dear user'
- - Urgent or threatening language
- - Unexpected attachments or links



Identifying Fake Websites

- - Look-alike URLs (e.g., g00gle.com)
- - No HTTPS
- - Typos or poor design
- - Check domain registration

The image shows a screenshot of a web browser displaying a fake Amazon login page. The page layout mimics the real Amazon site, including the Amazon logo, a 'Your Account | Help' link, and a 'Sign In' section. The 'Sign In' section asks for an email address and a password, with options for new customers or existing users. A 'Sign In Help' section is also present. At the bottom, there is a footer with links to 'Conditions of Use' and 'Privacy Notice', and a copyright notice for 1996-2014, Amazon.com, Inc. or its affiliates. The browser's developer tools are open on the right, showing the HTML structure. Red circles highlight the 'Footer Section' and 'Copyright Section' in the footer. The developer tools show the HTML for the footer, including the copyright notice and links to 'Conditions of Use' and 'Privacy Notice'. The copyright notice is highlighted with a green box, and the links are highlighted with red boxes.

amazon Your Account | Help

Sign In

What is your e-mail address?

My e-mail address is:

Do you have an Amazon.com password?

☐ No, I am a new customer.

☒ Yes, I have a password: [Forgot your password?](#)

[Sign in using our secure server](#)

Sign In Help

Forgot your password? [Get password help.](#)

Has your e-mail address changed? [Update it here.](#)

Footer Section

[Conditions of Use](#) [Privacy Notice](#) © 1996-2014, Amazon.com, Inc. or its affiliates

Copyright Section

```
"ap_privacy_footer">
  <p class="tiny" align="center">
    <a onclick="return amz_js_PopWin('#');" target="AmazonHelp" href="#">Conditions of Use</a>
    <a onclick="return amz_js_PopWin('#');" target="AmazonHelp" href="#">Privacy Notice</a>
  </p>
</div>
```

Social Engineering Tactics

- - Impersonation of trusted entities
- - Pretexting and baiting
- - Scareware and urgency
- - Emotional manipulation

Best Practices & Tips

- - Never click unknown links
- - Use two-factor authentication
- - Regularly update passwords
- - Verify requests via trusted sources

Real-World Examples

- - 2020 Twitter bitcoin scam
- - Fake bank emails
- - Corporate credential phishing attacks

Interactive Quiz - Sample Questions

- 1. Which of these is a phishing indicator?
- 2. What should you do if you suspect a phishing email?
- 3. Which URL is likely fake?

Final Tips & Resources

- - Visit trusted cybersecurity sites
- - Contact internal IT for help
- - Use tools like VirusTotal, URLVoid