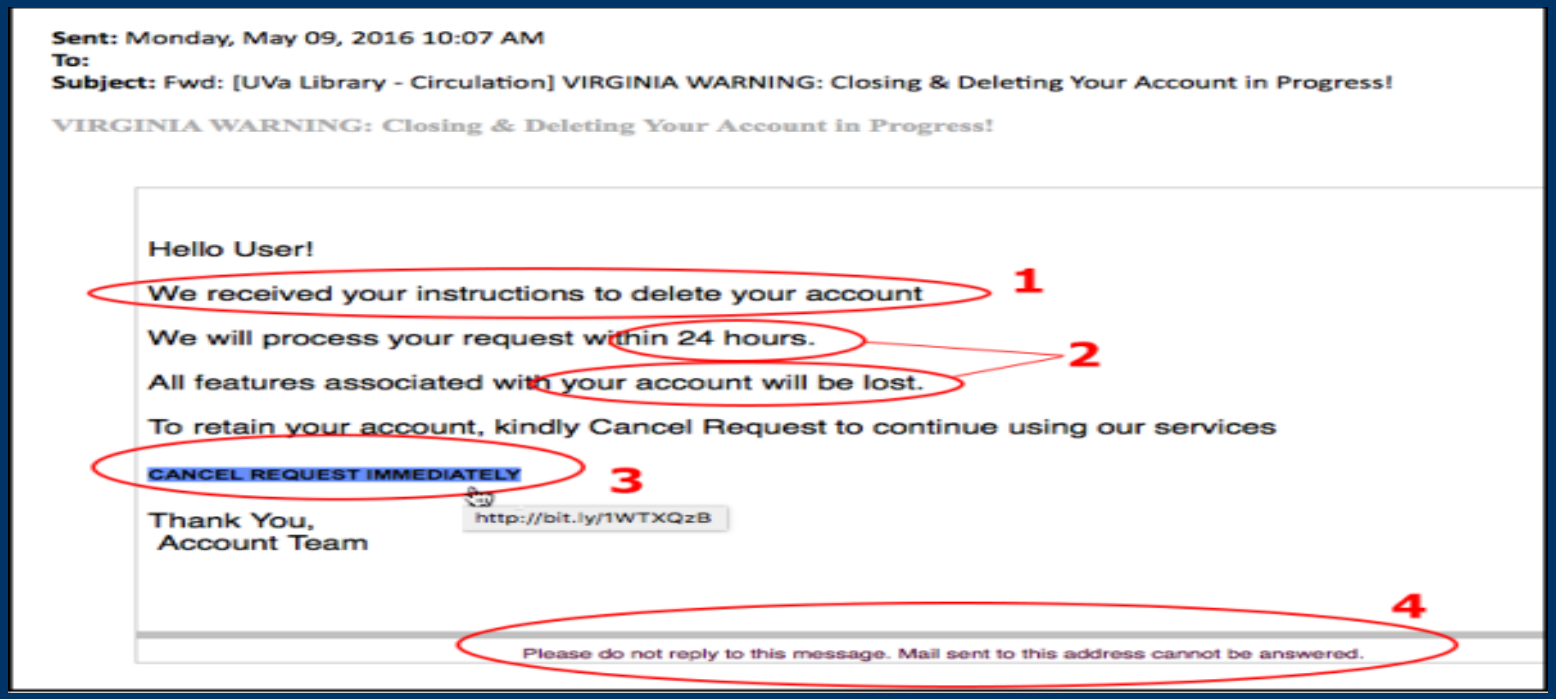
Understanding and Preventing Phishing Attacks

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

Prepared by Sparsh Agarwal

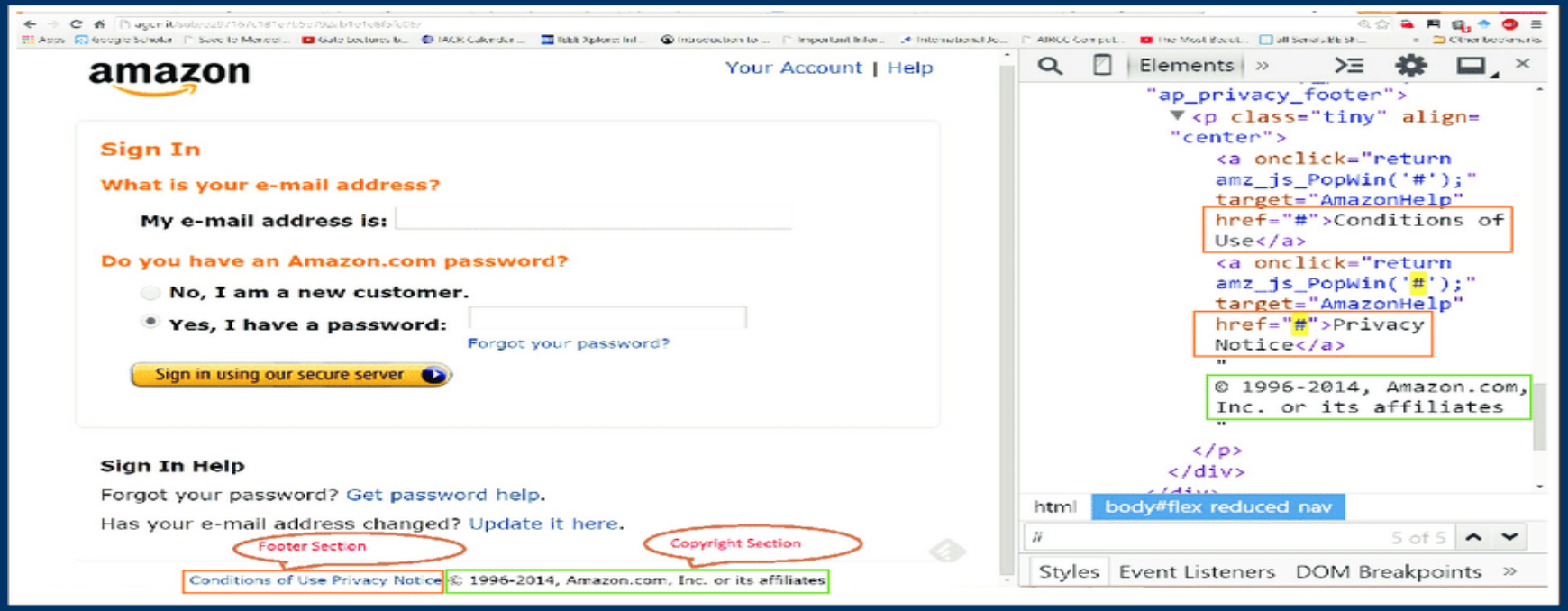
Recognizing Phishing Emails

- - 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



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