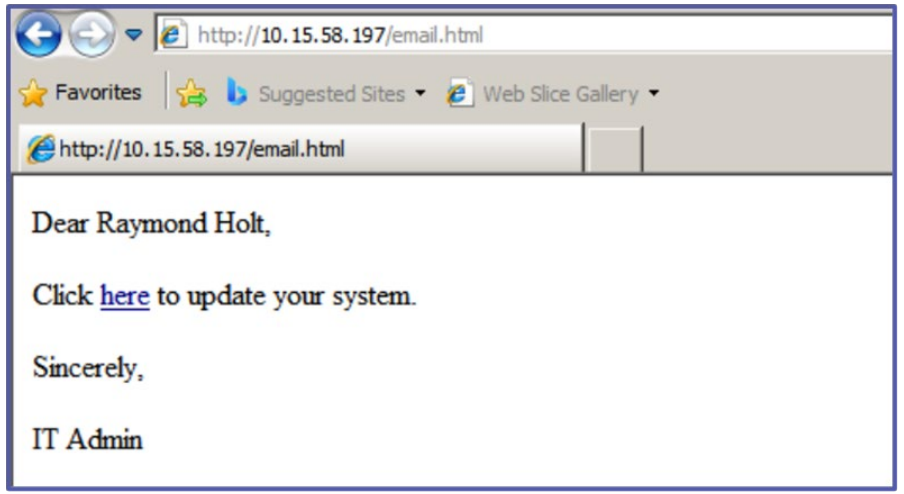
Cybersecurity

5.6.1 - Phishing Awareness

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Phishing

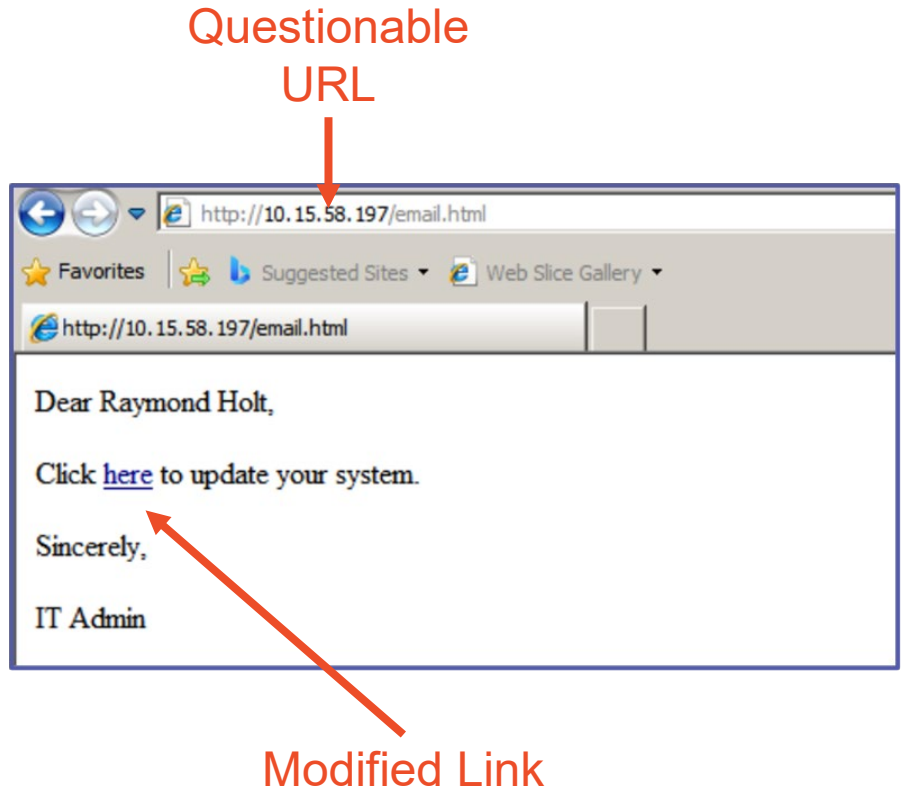
- A cybercrime tactic used by malicious actors to deceive individuals into providing sensitive information
  - Usernames
  - Passwords
  - Finance or other personal information
- Phishing campaigns can involve mass emails, text messages, or phone calls that appear legitimate at a glance, but they are intended to gain confidential information or download malicious software.



Phishing Example

Recognizing Phishing

- Be on the look out for:
  - Deceptive email addresses
  - Misspellings, grammatical errors, or other typos
  - Unusual domain names
  - A sense of urgency or threat of immediate action or consequences
- Ways to mitigate phishing
  - Hover over links to check URLs
  - Avoid clicking on unrecognized emails and attachments as they can redirect to or install malicious programs
  - Be wary of emails requesting personal information as most legitimate companies will communicate through specific channels



Response to Suspicious Messages

- Don’t respond to the original message, click any links, or download attachments!
- Forward suspected phishing schemes to your IT or security team for analysis and report phishing attempts.
- Share experienced phishing tactics to aid in detecting and raising awareness among colleagues, friends, and family.
- If you did fall victim to phishing, immediately change passwords for affected accounts and enable multi-factor authentication where possible.