Anatomy of a Phishing Email

Phishing is an attempt by a malicious actor pretending to be a legitimate enterprise for the purpose of stealing private information, such as usernames, passwords, social security numbers (SSN), and other sensitive data. More often than not, phishing messages have distinguishing characteristics, making them easy to identify if you know what to look for. Here's a look at the anatomy of a typical phishing email…

Don A Cook
Wed 2/15, 4:58 PM

Subject: **TECHNICAL URGENT UPGRADE**

Your account has been temporally suspended, and this means that you will not be able to send and receive new email messages. This is because of the on-going yearly maintenance and deleting of inactive accounts. **You are then requested to verify your account here for upgrading.**

Click Or **Open** this link to **VERIFY** your Account:
CLICK HERE

Security Alert Office.

Urgency / Fear
Phishing emails often try to create a sense of fear and urgency in subject lines, hoping that users will comply.

Poor grammar
Grammatical errors are common

Bad Links
Always review the link prior to clicking, and in the event the link has been clicked, please review the destination website for confirmation that the URL is accurate and valid. When possible, opt to go directly to a site through your browser instead of clicking a link in an email.

Random Capitalization
Random use of ALL CAPS

For more information about phishing, visit **www.lsu.edu/phishing**

LSU | Information Technology Services