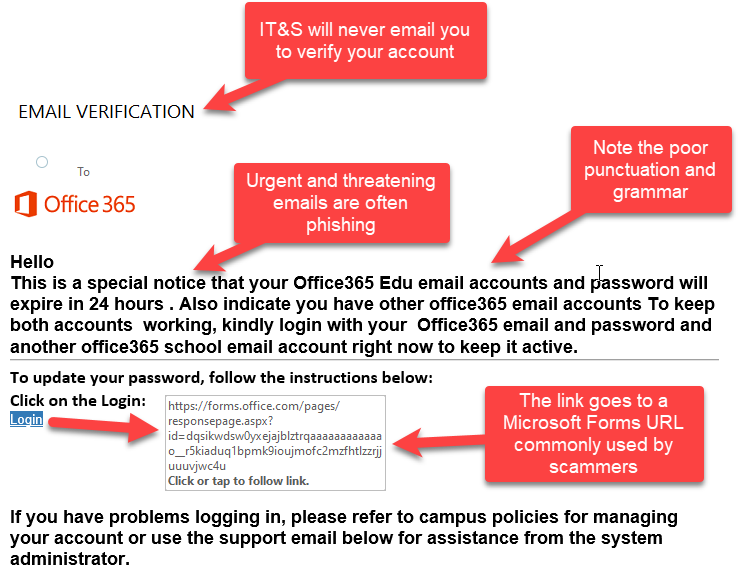
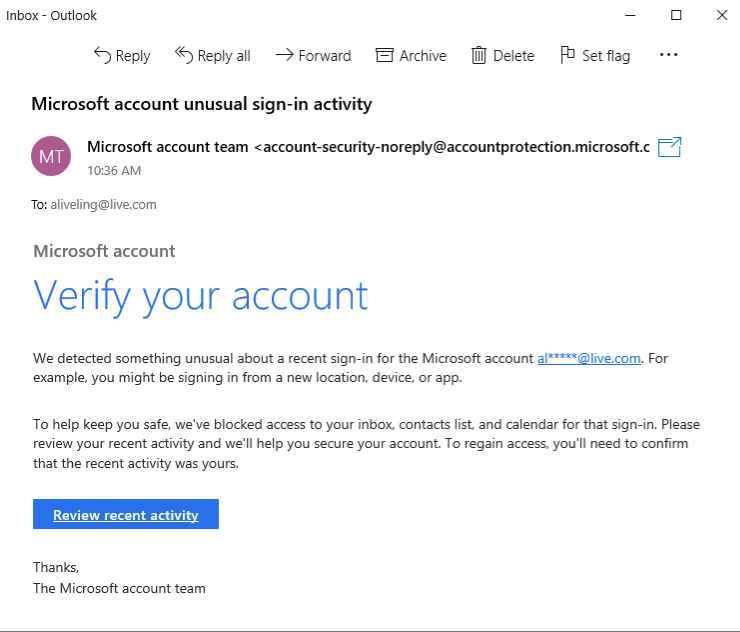
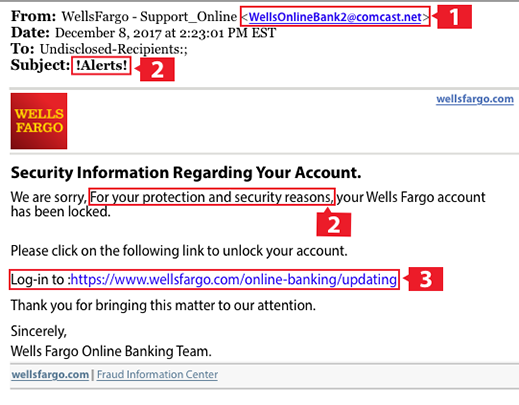
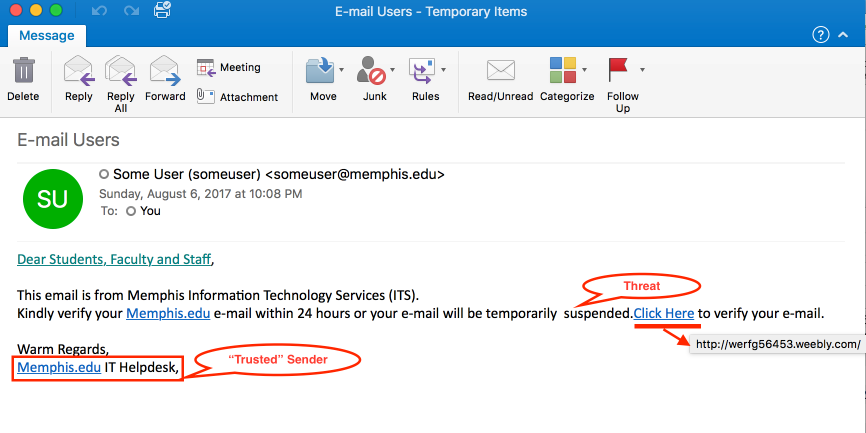
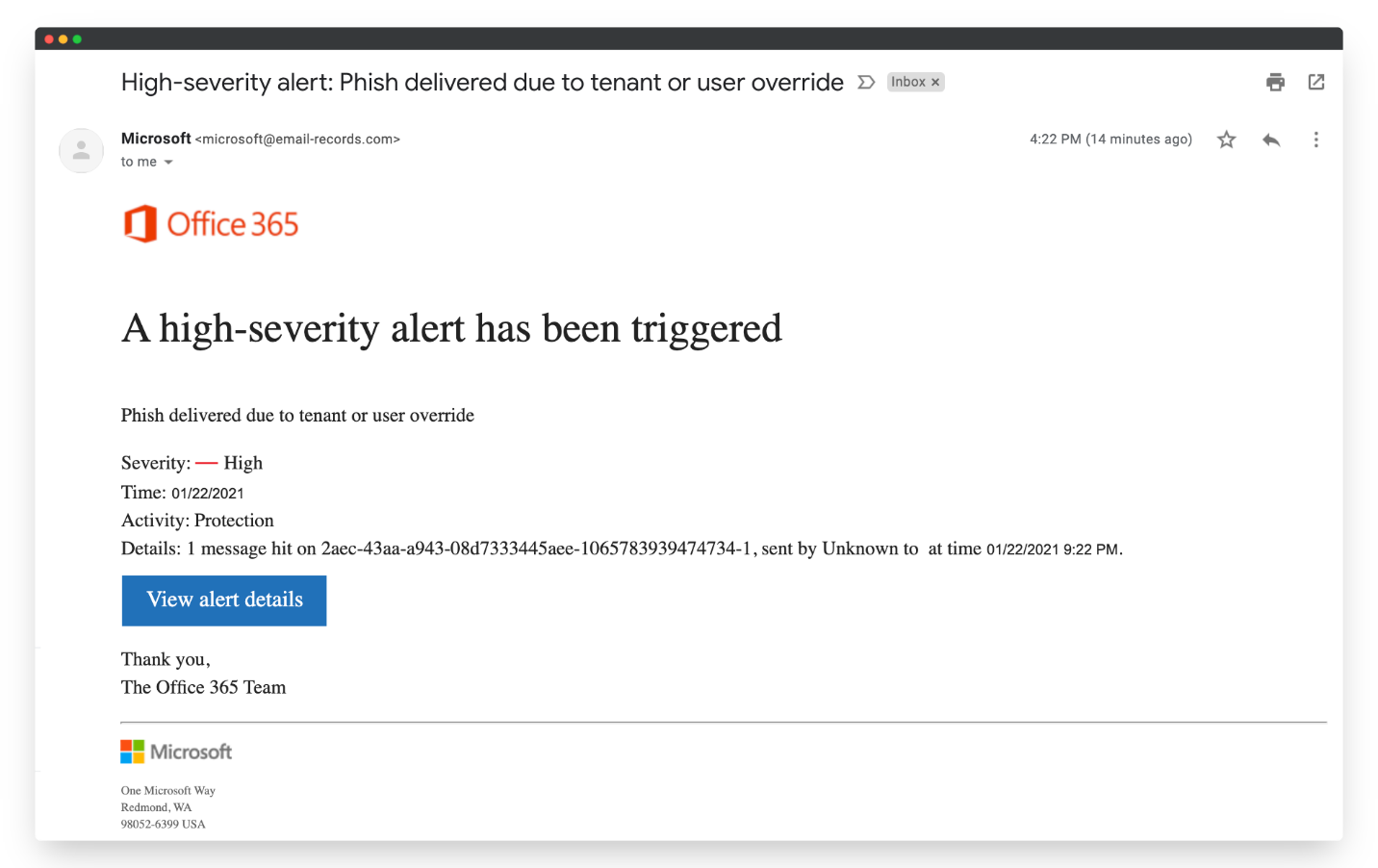
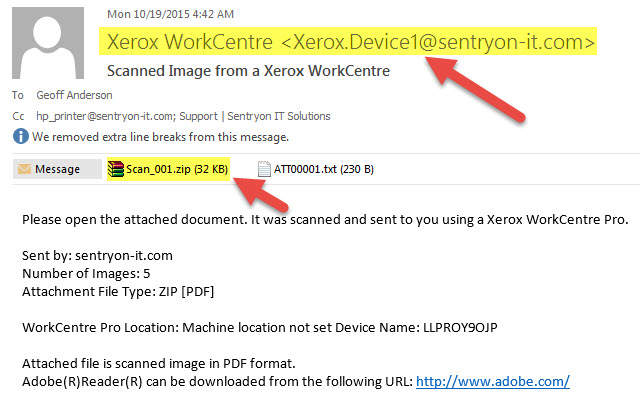
Task 2 – elevate Labs Cyber Security Internship

Ahmad Ghraieb

* Phishing email samples:





s

Phishing emails often display a combination of indicators that distinguish them from legitimate communication. A common characteristic is the use of spoofed sender addresses, where attackers manipulate domains to closely resemble authentic organizations. Examination of email headers typically reveals further inconsistencies, such as messages originating from servers unrelated to the claimed source. Additionally, phishing emails frequently contain suspicious links or attachments, which may redirect recipients to fraudulent websites or deliver malicious software. The body of the message is often written in an urgent or threatening tone, pressuring the recipient into immediate action. Hovering over embedded URLs commonly exposes mismatches between the displayed text and the actual destination, reinforcing their deceptive intent. Finally, spelling and grammatical errors are prevalent, diminishing the professionalism of the communication. Collectively, these traits—spoofed sender details, anomalous headers, malicious links or attachments, urgency, mismatched URLs, and poor language quality—serve as reliable indicators for identifying phishing attempts.

To avoid falling victim to phishing, users should verify sender addresses carefully, inspect email headers, and hover over links before clicking to confirm their legitimacy. They should avoid opening unsolicited attachments, remain cautious of urgent or threatening requests, and report suspicious emails to their organization’s IT or security team. Technical countermeasures include implementing email filters, enabling multi-factor authentication, and maintaining up-to-date antivirus and security patches, all of which reduce the risk and impact of phishing attacks.