**Phishing Email Analysis (2)** 16 Feb 2024

The phishing email analyzed in the provided image is an example of an email impersonating Microsoft to deceive the recipient to change their password. This aligns with the MITRE ATT&CK framework's T1566 phishing technique where threat actors use social engineering tactics to trick users into revealing sensitive information or downloading malicious content.

Three key indicators suggest that this email is a phishing attempt. First the sender's email address, "[support@msupdate.net](mailto:support@msupdate.net)" is not an official Microsoft domain, instead Microsoft uses "@microsoft.com" or related verified domains for security related communications. Second, the email contains a sense of urgency that instructs the recipient to reset their password immediately if they did not make the change, since attackers often use urgency to manipulate victims into making bad decisions. Third, the embedded links in the email, such as those for resetting the password or reviewing security info, could lead to a malicious website designed to steal login credentials.

To mitigate phishing attempts like this, organizations and individuals can implement several strategies. First, Network intrusion prevention systems can be used to scan and remove malicious email attachments or links (M1031). Second, training users to recognize phishing attempts through security awareness programs helps individuals spot suspicious emails and identify social engineering phishing techniques (M1017). Finally, companies should deploy antivirus and anti malware solutions to detect and block malicious messages and automatically quarantine them before they reach inboxes (M1049).

Personally, I have encountered an phishing email attempting to impersonate my bank, it claimed there was an urgent issue with my account that required immediate verification. The email contained a link to a fake login page that closely resembled my bank’s website. However, upon closer inspection, the URL was incorrect, and the email contained grammatical errors. I ignored the email and deleted it.

