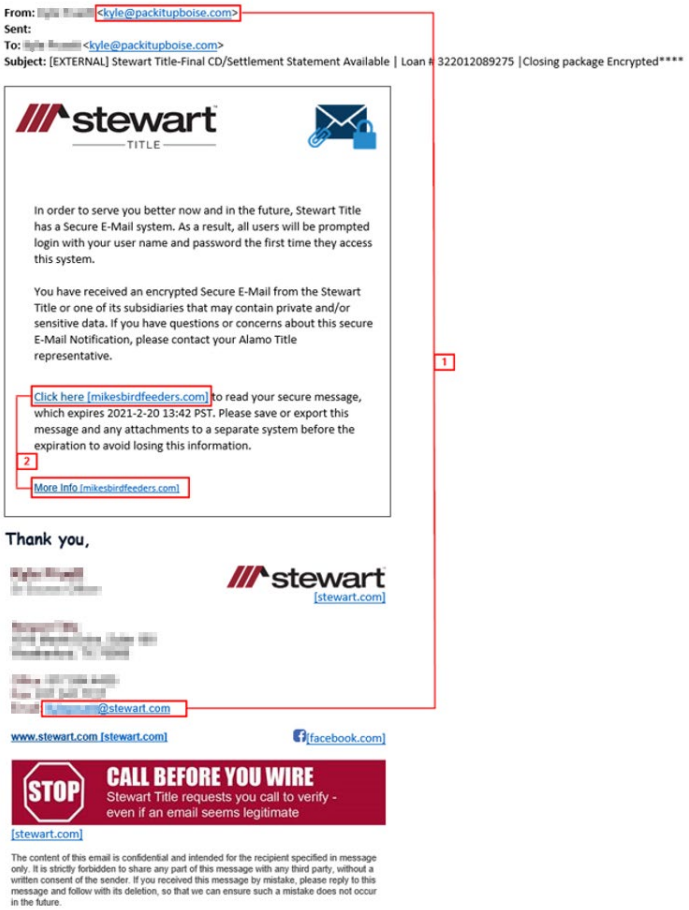
This Month's Tip: How to Recognize and Avoid Targeted Phishing Attacks

Phishing continues to be the most common online threat to Supreme Lending employees, so it's important to spot tell-tale signs and know what to do when you encounter a malicious email message. This month, we will break down a "sample" phishing email received by a Supreme Lending employee:

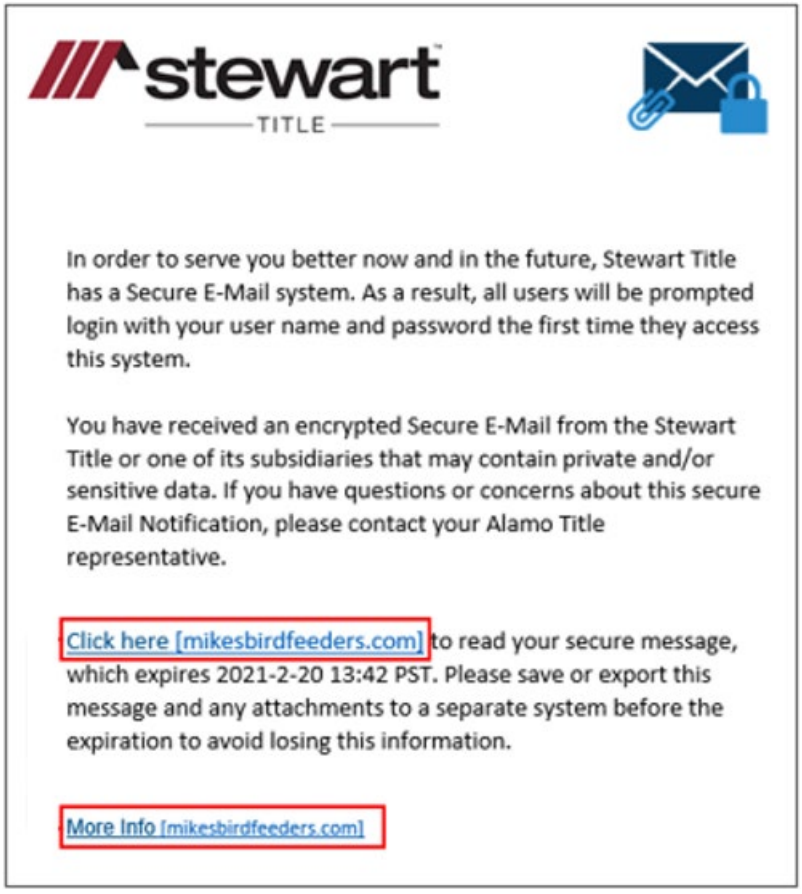


1. Conflicting Contact Information

The from address does not match the alleged sender. In the signature, we can see a legitimate @stewart[.]com address, but this email was sent from @packitupboise[.]com. This is our first red flag, and the email should be reported by using the “Report Phish” button.

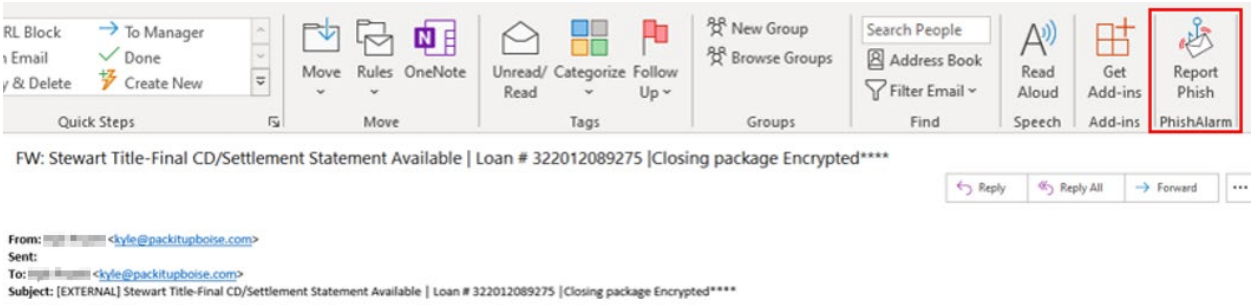
2. Malicious URL

Our second red flag comes from the URL in the body of the email. You can spot a malicious URL if the destination address does not match the context of the email. When an email is sent by Stewart Title, you should expect the link to direct you towards an address related to their company. In this case, the URL is taking us to hxxp://[mikesbirdfeeders[.]com]. Many legitimate and scam emails hide the destination address in a button or clickable link, but Proofpoint makes the destination domain visible. Always check the destination domain before clicking on any link.



3. What to Do If You Receive a Phishing Email

Be suspicious of any unsolicited email you receive from someone you do not recognize. Scammers are often very clever at disguising a phishing scam as a legitimate email from a reputable organization. If you feel something is not quite right, always report the email to Supreme's Information Security by highlighting the phishing email in your inbox and clicking the "Report Phish" button.



If you have any questions regarding this policy, please contact Information Security via Mark.Nagiel@SupremeLending.com. Thanks for participating in the Information Security effort!