NMLS Advisory

How to Respond to Spam or Phishing Emails

This advisory is being provided to reinforce the message that all email notifications you receive from NMLS are sent from NMLS_Notifications@NmlsNotifications.com.

Notifications are generated to inform you of an action you completed or need to take in NMLS. Email notices will never contain sensitive information, ask for your personal information, or include links to any site other than NMLS. When receiving notices, it is best if you navigate to NMLS and log in to determine what you need to do.

If you receive an email that is NOT from the NMLS email address listed above:

- Notify the IT security team within your organization. If your organization does not have an IT security team, proceed with the steps below.
- Forward the suspected email to security@csbs.org and add the word "PHISHING" to the beginning of the subject line.
- Delete the email after you have forwarded it to security@csbs.org.
- Do not reply to the email.

The phishing email could be an attempt by an illegitimate party attempting to gain access to your personal information (e.g., social security number, account numbers, passwords). These emails often threaten to close your account if you do not respond. Do not be tricked into opening or responding to a phishing email.