Fraudulent Email Notifications

In support of the Agency's paperless initiative, FDOT began use of an electronic signature application in August 2016, for purposes of executing contract documents. While new technology offers opportunities for process improvements, it may inevitably also present opportunities for phishing scams.

Email notifications requesting a vendor to electronically review and sign an FDOT contract document will originate from FDOT's DocuSign account. A few simple techniques can help you spot the difference between a spoof DocuSign email vs. the real thing:

- Email notifications originating from FDOT's electronic signature account will contain a picture of the FDOT logo.
- Hover over the link – URLs to view or sign DocuSign documents contain "docusign.net/" and should always start with https.
- Access your documents directly from www.docusign.com by entering the unique security code, which is included at the bottom of every DocuSign email.
- Do NOT open unknown or suspicious attachments.
- Look for misspellings, poor grammar, generic greetings, and a false sense of urgency.
- Delete any emails with the subject line, "Completed: [domain name] – Wire transfer for recipient-name Document Ready for Signature" and "Completed [domain name/email address] – Accounting Invoice [Number] Document Ready for Signature". These emails are not from DocuSign. They were sent by a malicious third party and contain a link to malware spam.
- Delete any suspicious emails from your computer. They may appear suspicious because you don't recognize the sender, contain misspellings (like "docusgn.com" without an 'i' or @docus.com), or direct you to a link that starts with anything other than https://www.docusign.com or https://www.docusign.net
- Contact the sender offline to verify the email's authenticity, if you're still suspicious.
- Report any suspicious DocuSign emails to related to DocuSign to spam@docusign.com and then delete them from your computer.
- For more information, please refer to the following link: https://trust.docusign.com/en-us/personal-safeguards/fraudulent-email-websites/