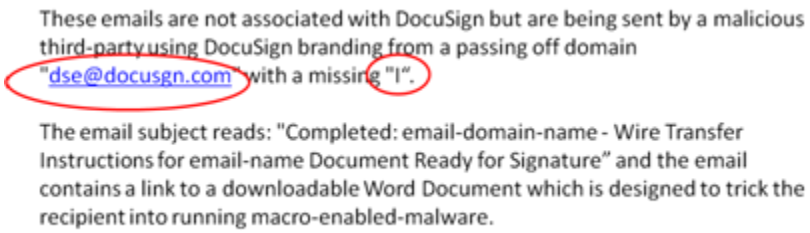
**WEBSITE MESSAGE - DOCUSIGN**

**Note: New Phishing scam**
DocuSign has observed a new phishing campaign that began the morning of May 16 (Pacific Time). The email comes from "dse@dousign.com" with the subject *"Legal acknowledgement for <person> Document is Ready for Signature"* and it contains a link to a malicious, macro-enabled Word document. We suggest you do not open this email, but rather delete it immediately.

Their investigations have revealed that only people with a DocuSign account were impacted by this incident – those who signed a document without a DocuSign account were not among the list of email addresses that were accessed maliciously. That said, even though an employee or customer of yours would not be on the list unless they had an account with DocuSign, we would still encourage you to be vigilant and aware of this phishing tactic.
Example:


These emails are not associated with DocuSign but are being sent by a malicious third-party using DocuSign branding from a passing off domain "dse@docusgn.com" with a missing "l".

The email subject reads: "Completed: email-domain-name - Wire Transfer Instructions for email-name Document Ready for Signature" and the email contains a link to a downloadable Word Document which is designed to trick the recipient into running macro-enabled-malware.

**If you do get a report of such an email please have it forwarded to spam@docusign.com and copied to partners@appositech.com and deleted.**

As part of that process, DocuSign has published an update on the trust and security section of the DocuSign website regarding advice on additional awareness tips.

**With DocuSign our top tips are:**

- All URLs to view or sign DocuSign documents will contain "docusign.net/" and will always start with https.
- All legitimate DocuSign envelopes include a unique security code at the bottom of notification emails
- If you don't recognise or expect a transaction from the sender, to query you can see the advice note at https://trust.docusign.com/en-us/personal-safeguards

**SAFEGUARD IDS & PASSWORDS**

- Keep your user IDs and passwords safe by following these tips.
- Use a strong password that is difficult for others to guess and avoid birthdays, names, and pet's names.
- Never write down your password or share it with others.
- Never provide your DocuSign account login or password, credit card number, or other personal information via email or to unknown parties.

**Note:** DocuSign will never ask you for your password via email.

Exercise caution using public computers: Public web browsers can cache personal data and store login details. Always log off of web sites and clear the browser cache to protect your personal information, passwords, and accounts.