Nascoga Federal Credit Union Member Alert: DocuSign E-Mail Incident

DocuSign recently confirmed that an unauthorized third party had gained entry to a portion of its system responsible for storing customer information on service announcements. Nascoga Federal Credit Union uses DocuSign's eSignature application to send loan documents, as well as other information, to its members upon their request. Going forward, Nascoga Federal Credit Union will telephone its members before sending an e-mail asking members to use DocuSign's eSignature system.

Nascoga Federal Credit Union's systems have not been impacted by this incident and none of our member's sensitive information has been known to be affected.

According to a statement by DocuSign, "A complete forensic analysis has confirmed that only a list of email addresses were accessed; no names, physical addresses, passwords, social security numbers, credit card data or other information was accessed. No content or any customer documents sent through DocuSign's eSignature system was accessed; DocuSign's core eSignature service, envelopes and customer documents and data remain secure." (https://trust.docusign.com/en-us/personal-safeguards/#updates).

The information that was obtained from DocuSign allowed attackers to craft specially targeted e-mail campaigns at users featuring doctored branding and headers that make messages appear to contain legitimate DocuSign attachments. These e-mails are not from DocuSign, but originate from a malicious third party, using DocuSign branding in the headers and body of the e-mail. The e-mails are sent from non-DocuSign-related domains including dse@docus.com and @docusgn.com (missing i). DocuSign has stated that legitimate DocuSign signing emails come from @docusign.com or @docusign.net email addresses.

Many of the phishing e-mails contain the following in the headers: "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." The e-mail message contains a link to a downloadable Microsoft Word document that, when clicked, installs malicious software.

DocuSign recommends that users be particularly cautious of any e-mail requesting them to sign or view a Document they are not expecting. DocuSign recommends that if you receive a suspicious e-mail that appears to have been sent from DocuSign, that you DO NOT RESPOND TO THE E-MAIL OR OPEN ANY ATTACHMENTS. Instead, DocuSign is recommending that you forward the e-mail to DocuSign at spam@docusign.com and immediately delete the message. DocuSign also recommends that users take this opportunity to make sure that their antivirus software is running and up to date.

When in doubt, access your documents directly by visiting docusign.com, and entering the unique security code included at the bottom of a legitimate DocuSign e-mail. DocuSign has stated that it will not ask recipients to open a PDF, Office document or ZIP file in an e-mail.

Further information regarding this incident at DocuSign can be found at https://trust.docusign.com/en-us/personal-safeguards/#updates.