SHELL EMPLOYEES' CREDIT UNION LIMITED

Dear members,

We have recently been advised that DocuSign, a third-party provider that Shell Employees' Credit Union uses for electronic document signing, has been the victim of a data breach that has led to massive phishing attacks which used stolen DocuSign information. Below is an excerpt for DocuSign's communication regarding the breach:

"During the week of May 8 and again the week of May 15, DocuSign detected an increase in phishing emails sent to some of our customers and users – and we posted alerts on the DocuSign Trust Site and in social media. The emails "spoofed" the DocuSign brand in an attempt to trick recipients into opening an attached Word document that, when clicked, installs malicious software. As part of our process in response to phishing incidents, we confirmed that DocuSign's core eSignature service, envelopes and customer documents remain secure.

However, as part of our ongoing investigation, we confirmed that a malicious third party had gained temporary access to that non-core system. A complete forensic analysis has confirmed that only 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; and DocuSign's core eSignature service, envelopes and customer documents and data remain secure.

We can confirm 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.

Please know we continue to work with various Law Enforcement officials and will provide additional updates as we complete the investigation.

For the latest information on this incident, please visit http://trust.docusign.com."

If you think you've been affected, here's what you need to know:

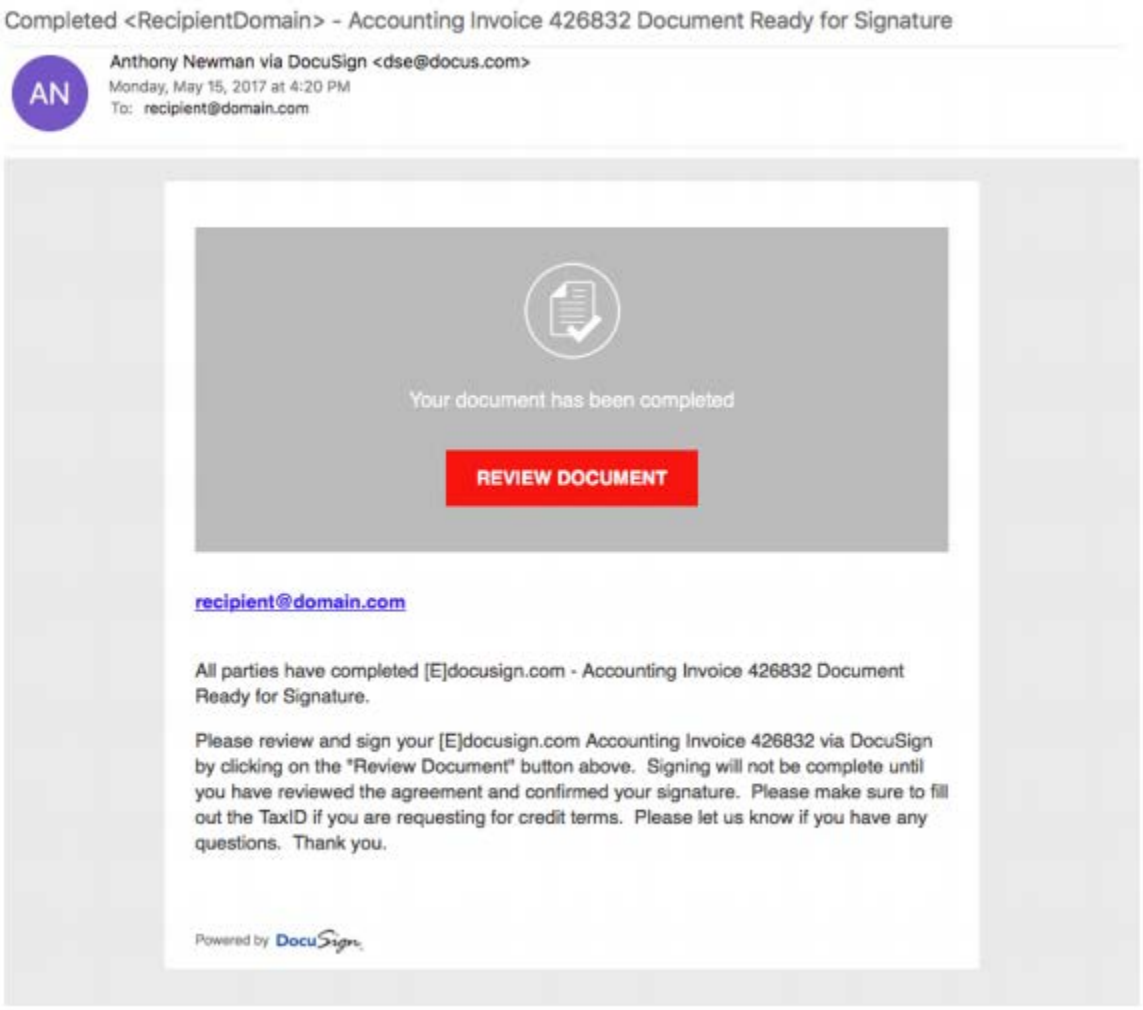
- Affected members will have received an email from Bruce Wilson, SECU Manager of Risk and Compliance, on May 29, 2017 advising them of the breach. This is a legitimate email.

- Members are instructed to filter or delete any emails with subject lines like:

- *Completed: [domain name] – "Wire transfer for recipient-name Document Ready for Signature"*
- *Completed [domain name/email address] – "Accounting Invoice [Number] Document Ready for Signature"*
- *Subject: "Legal acknowledgement for [recipient username] Document is Ready for Signature"*

These phishing emails will have Word docs as attachments, and use social engineering to trick users into activating Word's macro feature, which will download and install malware on the user's workstation. *DocuSign warned that highly likely there will be more campaigns in the future*.

Below is an example of the fake phishing email:



If you have any questions or concerns, please do not hesitate to contact us.