DocuSign®

Malicious Email Campaign FAQ – as of 5/18/2017

As an update on the malicious phishing incident, we wanted to share some of the most frequent questions that we have been receiving. We will continue to update the Trust Center with new information as it becomes available. As always, please continue to email service@docusign.com or call +1-800-379-9973 with any additional questions.

Q: What actually happened?

A:

- Last week and again on Monday, 5/15/2017, DocuSign detected an increase in phishing emails sent to some of our customers and users – and we posted alerts on the DocuSign Trust Center 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 routine 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, yesterday we confirmed that a malicious third party had gained temporary access to a separate, non-core system used for service-related announcements.
- 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.

Q: Is my DocuSign envelope and data secure?

A: As part of our process in response to phishing incidents, we confirmed that DocuSign's core eSignature service, envelopes and customer documents remain secure.

Q: Has my instance of DocuSign been impacted?

A: We have no evidence that there is any impact to any instance of DocuSign, and as part of our process in response to phishing incidents, we confirmed that DocuSign's core eSignature service, envelopes and customer documents remain secure.

Q: What information was impacted?

A: It was a list of email addresses stored in a separate, non-core system used for service-related announcements.

Q: Have the email addresses of my employees, customers or customers' customers been exposed as part of this incident?

A: As part of our ongoing investigation, we can now confirm that no signers were on the list of email addresses that was accessed maliciously unless they had signed up for a DocuSign account. That could include direct DocuSign customers; someone who signed a document and elected to open a DocuSign account; or someone who signed up for a DocuSign freemium account – via docusign.com, through a partner integration, or via the DocuSign mobile client.

Q: Do I need to communicate to all of them?

A: We would encourage you to utilize the existing materials on the DocuSign Trust Center to help your employees, customers or customers' customers protect themselves from phishing attacks.

Q: How many people were affected? How many email addresses compromised?

A: Right now we are still acting on the results of our ongoing investigation and cannot comment on those details.

Q: What systems were impacted?

A: As part of our ongoing investigation, we confirmed that a malicious third party had gained temporary access to a separate, non-core system used for service-related announcements.

Q: Why did we have to hear about it via social media?

A: We have been actively communicating via the DocuSign Trust Center since last week when we first discovered the increase in phishing emails to customers and users. Then as soon as we saw the increase on Monday this week (5/15/2017), we updated the Trust Center and posted updates across our Web site and social media channels. We are also working on direct customer outreach.

Q: Was any other information impacted outside of my email address?

A: 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.

Q: How are you so sure only my email address was impacted?

A: 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.

Q: What should I do about this?

A: We recommend taking the following steps to ensure the security of your email and systems:

- Delete any emails with the subject line, "*Completed: [domain name] – Wire transfer for recipient-name Document Ready for Signature*", "*Completed [domain name/email address] – Accounting Invoice*

[Number] Document Ready for Signature” and *“Legal acknowledgement for <person> Document is Ready for Signature”*. These emails are not from DocuSign. They were sent by a malicious third party and contain a link to malware spam.

- Forward any suspicious emails related to DocuSign to spam@docusign.com, and then delete them from your computer. They may appear suspicious because you don’t recognize the sender, weren’t expecting a document to sign, contain misspellings (like ‘@docusgn.com’ without an ‘i’ or @docus.com), contain an attachment, or direct you to a link that starts with anything other than https://www.docusign.com or https://www.docusign.net.

- Ensure your anti-virus software is enabled and up to date.

- Review our whitepaper on phishing available at https://trust.docusign.com/static/downloads/Combating_Phishing_WP_05082017.pdf

Q: I/one of my employees opened a suspicious email, what should I do?

A: If possible ensure that they do not click the link and/or install malicious code. We would also recommend continual education and content updates to your internal teams in terms of best practices around phishing. And we recommend taking the following steps to ensure the security of your email and systems:

- Delete any emails with the subject line, *“Completed: [domain name] – Wire transfer for recipient-name Document Ready for Signature”*, *“Completed [domain name/email address] – Accounting Invoice [Number] Document Ready for Signature”* and *“Legal acknowledgement for <person> Document is Ready for Signature”*. These emails are not from DocuSign. They were sent by a malicious third party and contain a link to malware spam.

- Forward any suspicious emails related to DocuSign to spam@docusign.com, and then delete them from your computer. They may appear suspicious because you don’t recognize the sender, weren’t expecting a document to sign, contain misspellings (like ‘@docusgn.com’ without an ‘i’, @docus.com or ‘dse@dousign.com’ without a ‘c’), contain an attachment, or direct you to a link that starts with anything other than https://www.docusign.com or https://www.docusign.net.

- Ensure your anti-virus software is enabled and up to date.

- Review our whitepaper on phishing available at https://trust.docusign.com/static/downloads/Combating_Phishing_WP_05082017.pdf

Q: What additional steps is DocuSign taking to address this issue?

A: We have taken immediate action to prohibit unauthorized access to this system, we have put further security controls in place, and are working with law enforcement agencies.

Q: Is this related to the global ransomware attack of late last week?

A: No.