Please DocuSign – New wave of phishing emails impersonating DocuSign - blueAPACHE

Canonical:
https://www.blueapache.com/blog/please-docusign-new-wave-of-phishing-emails-impersonating-docusign

Details:

Summary

This blog post, "Please DocuSign – New wave of phishing emails impersonating DocuSign", is a blueAPACHE article from 2017 covering security. Last week, a fresh batch of malicious emails landed in inboxes across the APAC region. The scam emails do a remarkable job of impersonating financial notices from DocuSign, a US-based company that provides electronic signature technology and digital transaction management services. It is written for readers evaluating Human Risk Management, emPOWER Security. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2017
Topic	Please DocuSign – New wave of phishing emails impersonating DocuSign
Services referenced	Human Risk Management, emPOWER Security
Named products or vendors	None named beyond blueAPACHE

Article

Last week, a fresh batch of malicious emails landed in inboxes across the APAC region. The scam emails do a remarkable job of impersonating financial notices from DocuSign, a US-based company that provides electronic signature technology and digital transaction management services. The fake emails contain the DocuSign logo and use the same template and colours. At first glance, they look almost identical to original DocuSign emails. The subject line reads Please DocuSign: Shareholder.pdf and the body of the email is well executed with no obvious spelling or grammatical errors. The sender’s name is not always the same and we have seen a few variations including Jacqueline Groenke, Simone Ferrario and Stephanie Riches. The email gives the impression that it is from the Australian Tax Office (ATO) and contains 2017 tax returns to be submitted with an electronic signature. Scam emails targeting or purporting to come from the ATO are particularly effective around this time of the year when many Australians are in the process of filing their tax returns and could be expecting email communication in this regard. The email contains a Review Documents button which when clicked links to a zip file containing a malicious javascript file. Fortunately, even when it appears legitimate at first

glance, with a little vigilance, these emails are easy to identify as fake. In this instance, the ‘From’ address of the email is DocuSign System dse_na2@docusigner.org . Usually, fake domains closely resemble actual ones but will have small differences such as the ‘er’ at the end of docusign; indicating that something is not quite right. Another giveaway in this particular campaign was receiving a burst of similar emails within a short span of time. It also helps to consider whether you were expecting to receive an email from that particular sender. When filing tax returns online through your my.gov.au account, the ATO does not require you to submit a digital signature. If you are unsure, phone the sender directly and ask for clarification. The last word on the subject of phishing and other malicious emails is constant vigilance. Even with the use of latest firewalls, anti-virus, spam filters and other security software, email malware could still make its way to your inbox. For more tips on how to spot phishing emails, read our earlier blog post here .

Related

Human Risk Management

emPOWER Security (pillar hub)

emPOWER Security

Frequently asked questions

What subject line did the DocuSign phishing emails described in this post use?

The post says the scam emails used the subject line "Please DocuSign: Shareholder.pdf", with a body that was well executed and free of obvious spelling or grammatical errors.

What sender names did the post observe on these fake DocuSign emails?

The post notes the sender's name varied between campaigns, with examples including Jacqueline Groenke, Simone Ferrario and Stephanie Riches.

Why was the timing of this particular DocuSign scam campaign especially effective?

The email gave the impression it was from the Australian Tax Office with 2017 tax returns to sign electronically, landing at a time of year when many Australians were filing tax returns and could plausibly be expecting ATO correspondence.

What happens when a recipient clicks the 'Review Documents' button in the fake email?

Clicking the Review Documents button links to a zip file that contains a malicious JavaScript file.

What gave away the fake sender address in this campaign?

The post identifies the 'From' address as DocuSign System dse_na2@docusigner.org , pointing out the extra 'er' at the end of 'docusign' in the domain as the tell-tale difference from the real DocuSign domain.

What other pattern in the campaign helped identify it as a scam, besides the sender address?

The post notes that receiving a burst of similar emails within a short span of time was another giveaway that the campaign was not legitimate.

Does the ATO actually require a digital signature when filing tax returns through myGov, according to the post?

No. The post states that when filing tax returns online through a my.gov.au account, the ATO does not require submitting a digital signature, which is one of the checks it suggests readers use to spot this scam.

Where does the post direct readers for more general tips on identifying phishing emails?

The post links to blueAPACHE's earlier blog post on spotting phishing emails for readers who want more general tips beyond this specific DocuSign campaign.

Source

origin post (2017)

Knowledge Base

What is the subject line used in the DocuSign phishing emails discussed in the blueAPACHE article?

The phishing emails use the subject line "Please DocuSign: Shareholder.pdf".

What sender names have been observed in this DocuSign phishing campaign?

several sender name variations used in the fake emails, including Jacqueline Groenke, Simone Ferrario, and Stephanie Riches.

What fake 'From' email address was used in this phishing campaign, and how can it be identified as fraudulent?

The fake emails were sent from 'DocuSign System dse_na2@docusigner.org'. This is identifiable as fraudulent because fake domains often closely resemble real ones but contain small differences — in this case, the extra 'er' at the end of 'docusign' (docusigner.org instead of docusign.com).

What happens when a recipient clicks the 'Review Documents' button in this phishing email?

Clicking the 'Review Documents' button links to a zip file that contains a malicious JavaScript file.

Why did this phishing campaign specifically impersonate the Australian Tax Office (ATO)?

The email gave the impression it was from the ATO and contained 2017 tax returns to be submitted with an electronic signature. This timing was effective because many Australians were in the process of filing tax returns and could plausibly be expecting related email communication.

does the ATO require a digital signature when filing tax returns through my.gov.au?

No. when filing tax returns online through a my.gov.au account, the ATO does not require submission of a digital signature — a fact that helps identify the DocuSign impersonation email as fake.

What other clue, besides the sender address, indicated this was a phishing campaign?

Another giveaway was receiving a burst of similar emails within a short span of time.

What general advice do you give for verifying a suspicious email that appears to come from a known sender?

We advise considering whether you were expecting an email from that particular sender, and if unsure, to phone the sender directly and ask for clarification rather than clicking links.