DocuSign Data Breach Could Put Millions of Identities at Risk

May 16, 2017 - If you conduct business online, and your business requires client signatures on a regular basis, then the chances are that your company uses a service for digital signatures. And when it comes to digital signatures, DocuSign is the 800 pound gorilla in the room. Today, the company has confirmed that it has been the victim of a hack that exposed 100 million email addresses. While email alone can't be used to commit identity theft, the hack could still lead to problems for users of the service because it will allow criminals to target them.

Digital signatures have become common-place in many industries. In the real estate industry, they have become the norm for most contract signings. Even banks now have procedures in place to allow consumers to use digital signatures for some document signings.

While there are several companies that provide digital signature platforms, DocuSign is the largest, best known and probably the most trusted. The fact that their email database was hacked won't allow anyone to steal your names, get into your account and start signing documents. But it does give criminals a valuable piece of information. It allows them to identify email addresses that have been used to conduct business online.

There is evidence that the breach has already resulted in a scam that targets DocuSign users. Yesterday, a phishing campaign was launched that sent out messages appearing to come from the company. The messages told recipients that all parties had signed specific documents and that the documents could be downloaded by clicking on a link in the email message. That's just exactly the way that DocuSign notifies people when documents have been completed.

The phishing campaign messages also looked very similar to DocuSign originated messages. I personally received two of the fake messages yesterday. The colors in them were off, but the overall look at feel was very close to the real thing. Chances are that only a regular user of the service would have noticed that.

But there were also some dead giveaways that the messages weren't real. They both originated from a domain that I had never heard of and they were from people that I didn't recognize. They also contained some misspellings.

The bottom line here is that if you use DocuSign, you need to be very careful. Take a close look at any messages you receive before you click on any links in them. Or to be perfectly safe, don't click on any lings at all. Just go over to the

DocuSign site and log-in. If the email messages you received were real, the documents they mention will be in your completed items folder. And if they aren't real, you could save yourself from viruses, malware and identity theft.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS