



 [Subscribe to RSS](#)

 [Follow me on Twitter](#)

 [Join me on Facebook](#)



**SECURITY VISIBILITY  
MADE SIMPLE**



CLOUD SECURITY  
DONE RIGHT  
IS EVIDENT

[Get Started](#)

# Krebs on Security

In-depth security news and investigation



- [About the Author](#)
- [Blog Advertising](#)

15  
May 17

## Breach at DocuSign Led to Targeted Email Malware Campaign

**DocuSign**, a major provider of electronic signature technology, acknowledged today that a series of recent malware phishing attacks targeting its customers and users was the result of a data breach at one of its computer systems. The company stresses that the data stolen was limited to customer and user email addresses, but the incident is especially dangerous because it allows attackers to target users who may already be expecting to click on links in emails from DocuSign.

San Francisco-based DocuSign warned on May 9 that it was tracking a malicious email campaign where the subject line reads, “Completed: docusign.com – Wire Transfer Instructions for recipient-name Document Ready for Signature.” The missives contained a link to a downloadable **Microsoft Word** document that harbored malware.

Please review and sign your document



**From:**  **Michael Strickland (michael.strickland@docusign.com)**  
DocuSign

Hello Phillip Buckingham,  
Please review the documents and sign immediately.  
Best,  
Michael

[View Documents](#) ►

Alternately, you can access these documents by visiting [docusign.com](https://docusign.com), clicking the "Access Document" link, and using this security code:

8A5A4DDADBA5490AAC0D358ED675F \*\*\*\*

DocuSign. The fastest way to get a signature.®

This message was sent to you by Michael Strickland who is using the DocuSign Electronic Signature Service. If you would rather not receive email from this sender you may contact the sender with your request.

A typical DocuSign email. Image: DocuSign.

The company said at the time that the messages were not associated with DocuSign, and that they were sent from a malicious third-party using DocuSign branding in the headers and body of the email. But in [an update](#) late Monday, DocuSign confirmed that this malicious third party was able to send the messages to customers and users because it had broken in and stolen DocuSign’s list of customers and users.

“As part of our ongoing investigation, today we confirmed that a malicious third party had gained temporary access to a separate, non-core system that allows us to communicate service-related announcements to users via email,” DocuSign wrote in an alert posted to its site. “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.”

The company is asking people to forward any suspicious emails related to DocuSign to [spam@docusign.com](mailto:spam@docusign.com), and then to delete the missives.

“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>,” reads the advisory.

If you have reason to expect a DocuSign document via email, don’t respond to an email that looks like it’s from DocuSign by clicking a link in the message. When in doubt, access your documents directly by visiting [docusign.com](https://docusign.com), and entering the unique security code included at the bottom of every legitimate DocuSign email. DocuSign says it will never ask recipients to open a PDF, Office document or ZIP file in an email.

DocuSign was already a perennial target for phishers and malware writers, but this incident is likely to intensify attacks against its users and customers. DocuSign says it has more than 100 million users, and it seems all but certain that the criminals who stole the company’s customer email list are going to be putting it to nefarious use for some time to come.

Tags: [DocuSign breach](#), [DocuSign phishing](#), [macro exploit](#), [Microsoft Word](#)

This entry was posted on Monday, May 15th, 2017 at 11:34 pm and is filed under [Other](#). You can follow any comments to this entry through the [RSS 2.0](#) feed. You can skip to the end and leave a comment. Pinging is currently not allowed.

### 30 comments

-  *a*  
[May 16, 2017 at 12:03 am](#)

I have used DocuSign a few times to make long-distance real estate offers (that were rejected) and was dismayed at how little was required to

use a site that might have committed me to pay hundreds of thousands of dollars.


[Reply](#)



[May 16, 2017 at 1:52 am](#)


It's true that what you do with the site can have big consequences, but all it really allows you to do is sign a document; it serves the same function as a pen. I don't think there's any reason for requiring more from users of the site to sign things.

[Reply](#)

2.  *Bodda Rajendra*  
[May 16, 2017 at 12:23 am](#)

I received few mails, as per above information I tried to send same to [spam@docusign.com](mailto:spam@docusign.com). But this mail id id rejecting mails.

[Reply](#)

3.  *Loïc*  
[May 16, 2017 at 1:23 am](#)

Please send this to me : loic dot houssier at docusign dot com

Thanks for your help  
Loïc

[Reply](#)

4.  *Kag*  
[May 16, 2017 at 1:42 am](#)

From what i heard from users, DocuSign do attach files to their emails.

Makes this statement kind of useless thou i know it is from a DocuSign statement from here  
[https://trust.docusign.com/static/downloads/Combating\\_Phishing\\_WP\\_05082017.pdf](https://trust.docusign.com/static/downloads/Combating_Phishing_WP_05082017.pdf)

DocuSign says it will never ask recipients to open a PDF, Office document or ZIP file in an email.

[Reply](#)

-  *Rocky*  
[May 16, 2017 at 11:38 am](#)


DocuSign doesn't require you to open any attachments. When signing a document, their emails provide a secure link to the encrypted .pdf that is housed in their cloud. When the document has been completed by all signers, the option to have a .pdf copy of the completed document(s) delivered via email is available. This is what the hack exploited. The emails were made to appear like the recipient had received a wire transfer, and the completed documentation was attached to the email for their review.

[Reply](#)

-  *Eliel Joseph*  
[May 16, 2017 at 11:58 am](#)

Yes! after the documents are signed the recipients received a copy to download.

[Reply](#)

5.  *J*  
[May 16, 2017 at 3:29 am](#)

This is a serious breach. I helped someone defend against the phishing attack described in the article.

It's hard to train users to look at URLs for phishiness. The one I saw had a top-level domain of an African country.

[Reply](#)

-  *parabarbarian*  
[May 16, 2017 at 1:24 pm](#)

This is especially bad when punycode URL can looks virtually identical to a “normal” URL. Some browsers will display this:

<https://www.xn--80ak6aa92e.com/>

as this:

<https://www.apple.com/>

See here for how it works:


<https://www.xudongz.com/blog/2017/idn-phishing/>

[Reply](#)

6.  *IRS iTunes Card*  
[May 16, 2017 at 7:16 am](#)

Time to get rid of the use of email for good.

[Reply](#)

-  *JimV*  
[May 16, 2017 at 10:33 am](#)

And do what instead? Go back to chisels and stone tablets, or snail mail and FedEx?

[Reply](#)

-  *W from FL*  
[May 16, 2017 at 11:49 am](#)

rofl... agreed.

[Reply](#)

7.  *Thaumatechnician*  
[May 16, 2017 at 7:35 am](#)

Some months ago, my employer wanted us to acknowledge receipt and reading of the employee handbook by using DocuSign.

After the initial shock from reading the documentation on their website, I did a little research and found that other people (some of them lawyers) also had concerns about DocuSign’s ‘digital signatures’.

I checked what the Canadian government considered to be acceptable digital signatures (hint: they’re bang on!). I referred the HR dept. (located in the ‘States) to the relevant Canadian government documentation, pointing out that what Docusign does has no legal standing in Canada. I refused to Docusign. They didn’t push it.

And, oh look!, I’m protected from this phishing attack.

[Reply](#)

-  *S*  
[May 16, 2017 at 9:45 am](#)

This is not true. Digital signature are legal in Canada


[Reply](#)

-  *Jon*  
[May 16, 2017 at 12:24 pm](#)

What are the concerns about Docusign’s digital signatures?

I just got a document to sign yesterday (had no experience with Docusign) and I didn’t have to set up a digital signature using PKI. So basically anybody with access to my e-mail could have signed. Is that what the concern is?

[Reply](#)

8.  *Nobby Nobbs*



[May 16, 2017 at 9:13 am](#)

The delayed trickle of acknowledgements is enough to make me not want to trust this company.

There is already a proper way to digitally “sign” something: with a GPG key. When someone imitates a proven technology to dumb it down, that’s strike two.

Not securing your customers’ information, even on an marketing server? Strike three, thanks for playing.

[Reply](#)



o *JimV*

[May 16, 2017 at 10:40 am](#)

PGP (i.e. Pretty Good Privacy)?

[Reply](#)



■ *Nobby Nobbs*

[May 16, 2017 at 11:32 am](#)

Well, that’s an option, too.

The open-source implementation is Gnu Privacy Guard, GPG. They have versions for Windows, OSX, Android, Linux, etc.

<https://gnupg.org/>

[Reply](#)



9. *Blake*

[May 16, 2017 at 9:16 am](#)

I saw several of these recently, but they linked to an Office365 login page, not a Word document.

[Reply](#)



10. *Matt*

[May 16, 2017 at 9:18 am](#)

If you live in the UK also submit a report to Action Fraud. This is set up by the City of London Police to handle cyber crime/phishing.

[http://www.actionfraud.police.uk/report\\_fraud](http://www.actionfraud.police.uk/report_fraud)

[Reply](#)



11. *Matt*

[May 16, 2017 at 9:53 am](#)

In the USA you can use – <https://www.ic3.gov/complaint/default.aspx>

Matt

[Reply](#)



12. *D Haiz*

[May 16, 2017 at 10:02 am](#)

Our domain users are receiving targeted emails on this today. If anyone including DocuSign has lingering Malware or gets infected from this point forward I’d suggest using Malwarebytes Breach Remediation Tool (MBBR). Works great and not expensive at all.

[Reply](#)



13. *Nik*

[May 16, 2017 at 10:49 am](#)

Well, yesterday’s phishing campaign posing as DocuSign that sent over 1,000 targeted emails against my company (have to run a report to get the actual number) now makes sense as to where they had obtained the email addresses from. Luckily, our email filter stopped all of the emails from reaching the recipient this time.

[Reply](#)

14.  *vb*

[May 16, 2017 at 11:04 am](#)

It doesn't help that DocuSign sends out marketing emails, thus getting user complacent about getting email from DocuSign. I finally unsubscribed to DocuSign marketing emails.

I never want an unsolicited email from most companies. Especially companies dealing with financial transactions.

[Reply](#)

15.  *Anon*

[May 16, 2017 at 11:12 am](#)

I am a docuSign user. I was affected by this noticed the suspicious email and immediately tweeted them and forwarded the email to their abuse department.

[Reply](#)

16.  *Elie Joseph*

[May 16, 2017 at 11:27 am](#)

I alerted docuSign and arstechnica on the 8th of this bug, not sure docuSign took it seriously at first.

[Reply](#)

17.  *Silemess*

[May 16, 2017 at 11:42 am](#)

Typo: "On San Francisco-based DocuSign warned on May 9"

Looks like it's supposed to be either "On May 9th San Francisco..." or just "San Francisco-based..."

Once again, this seems to be a solid push for using DKIM and SPF. Identifying if the emails actually do come from DocuSign (or any other expected and semi-trusted party) would be a good step towards establishing the bona fides of the received email.

From there maybe we can move on to not sending attachments except when explicitly stated in a communication ahead of time from a trusted party.

Then the best fun, making sure that links actually go where they say they go and never trusting a shortened one.

Still loads of flaws in these approaches, but they do reduce some risk. That said, they also increase the communication barrier and historically we've never appreciated or approved of things that do that. DKIM and SPF are the best in that they don't cause the user to have extra work, and their work can be done in the background silently.

[Reply](#)

o  *Nik*

[May 16, 2017 at 1:02 pm](#)

For their one domain, docuSign.net, they do have DMARC configured for 100% reject. For their other domain though, docuSign.com, they only have DMARC configured for reporting.

[Reply](#)

o  *vb*

[May 16, 2017 at 1:16 pm](#)

"making sure that links actually go where they say they go"

Even if the links go where they should, this check does not always work. I've seen links in spam with domain or sub-domain names that make perfect sense for the legitimate company.

And I've seen I've seen links in legitimate company email. with domain or sub-domain names that look like spam links.

[Reply](#)

18.  *LessThanObvious*  
[May 16, 2017 at 12:31 pm](#)

I hate DocuSign, I really hope this prompts employers not to use this for employee offer letters and applications. I should not be forced to trust my personal info to some third party with little accountability just to accept a job offer.

[Reply](#)

**Leave a comment**

Name (required)

Email (required)

Website

Comment

**Advertisement**

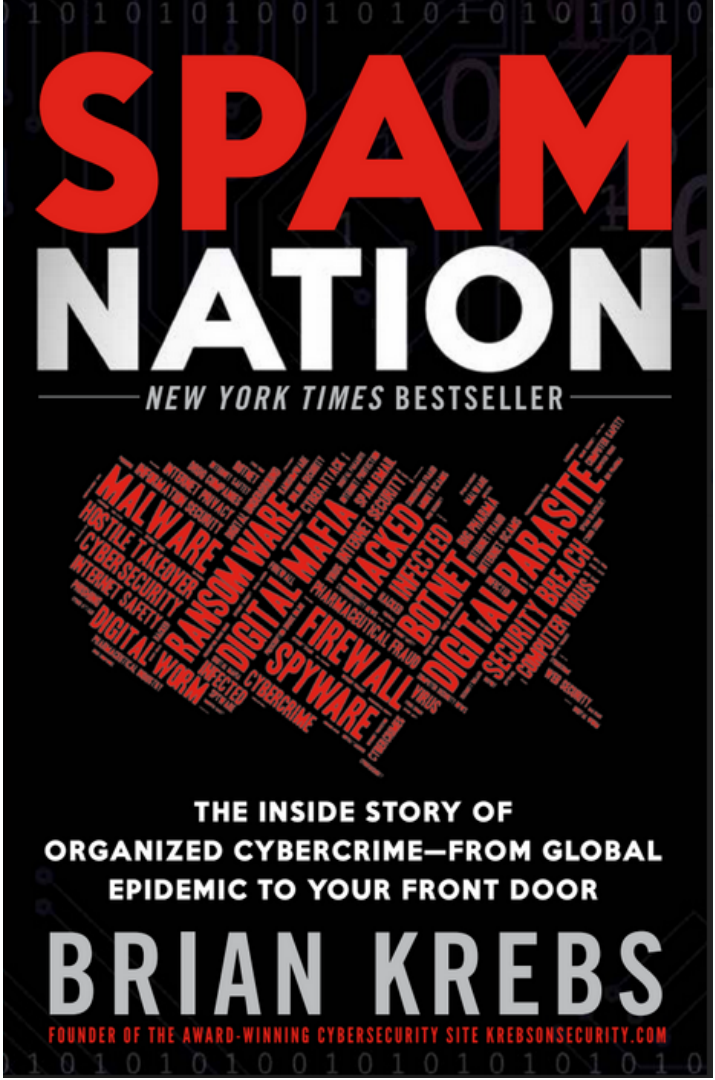


On-demand, automated security & compliance in any environment

LEARN MORE

•  

• **My New Book!**



A New York Times Bestseller!



- ## Recent Posts

- [Breach at DocuSign Led to Targeted Email Malware Campaign](#)
  - [Global ‘Wana’ Ransomware Outbreak Earned Perpetrators \\$26,000 So Far](#)
  - [Microsoft Issues WanaCrypt Patch for Windows 8, XP](#)
  - [U.K. Hospitals Hit in Widespread Ransomware Attack](#)
  - [SSA.GOV To Require Stronger Authentication](#)

- ## Subscribe by email

Please use your primary mailbox address, not a forwarded address.

Your email:

- ## All About Skimmers





Click image for my skimmer series.

• The Value of a Hacked PC



Badguy uses for your PC

• Tools for a Safer PC



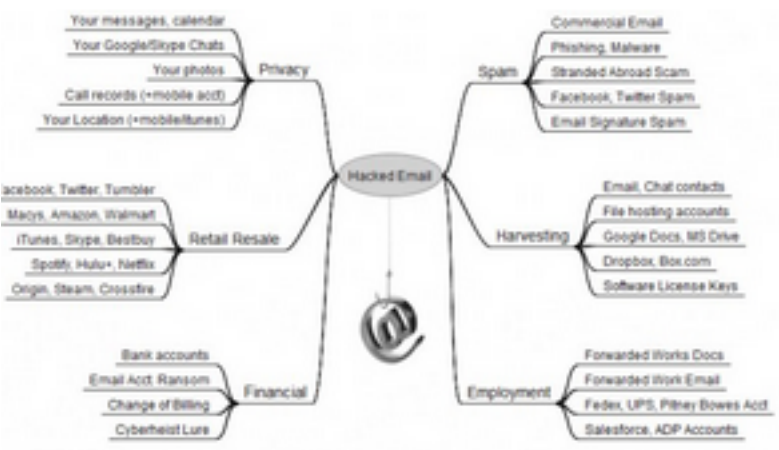
Tools for a Safer PC

• The Pharma Wars



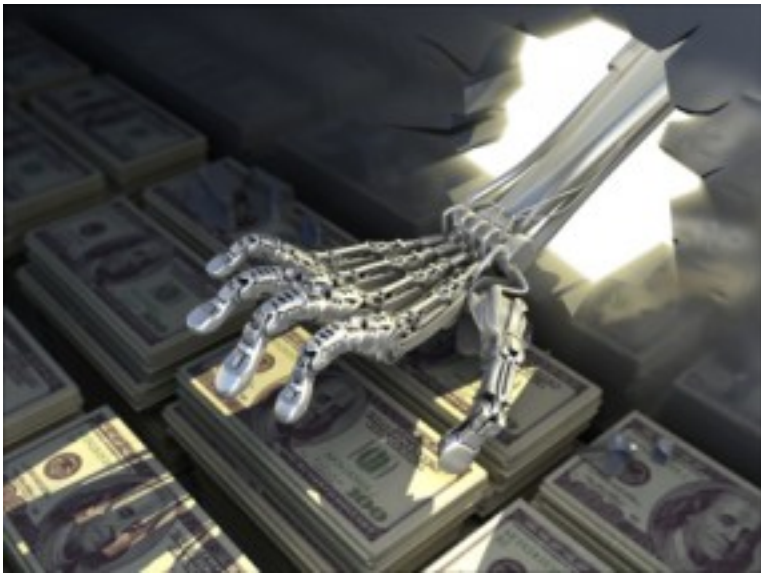
Spammers Duke it Out

• Badguy Uses for Your Email



Your email account may be worth far more than you imagine.

## • eBanking Best Practices



eBanking Best Practices for Businesses

## • Most Popular Posts

- [Online Cheating Site AshleyMadison Hacked](#) (798)
- [Sources: Target Investigating Data Breach](#) (620)
- [Cards Stolen in Target Breach Flood Underground Markets](#) (445)
- [Reports: Liberty Reserve Founder Arrested, Site Shuttered](#) (416)
- [Was the Ashley Madison Database Leaked?](#) (376)
- [True Goodbye: 'Using TrueCrypt Is Not Secure'](#) (363)
- [Who Hacked Ashley Madison?](#) (360)
- [Following the Money, ePassporte Edition](#) (353)
- [U.S. Government Seizes LibertyReserve.com](#) (315)
- [Extortionists Target Ashley Madison Users](#) (310)

## • Category: Web Fraud 2.0



Innovations from the Underground

- 

ID Protection Services Examined

- **Is Antivirus Dead?**



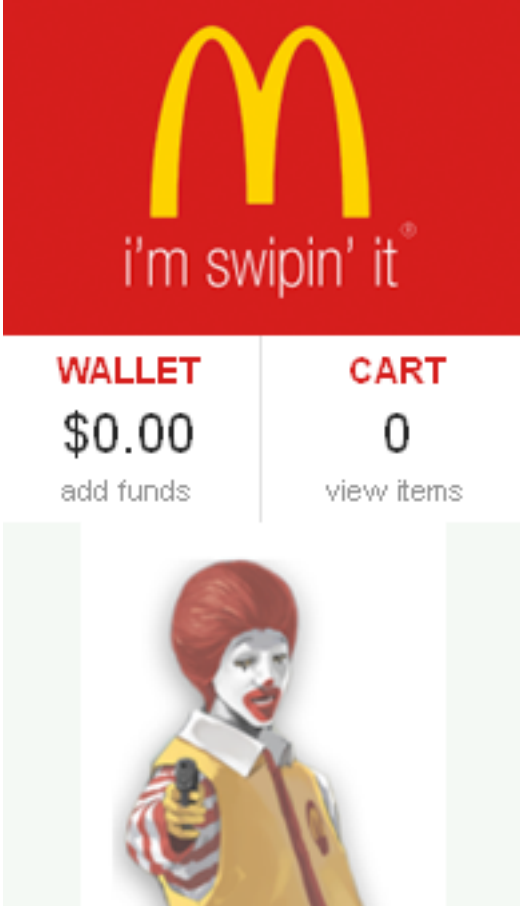
The reasons for its decline

- **The Growing Tax Fraud Menace**



File 'em Before the Bad Guys Can

- **Inside a Carding Shop**



A crash course in carding.

• Beware Social Security Fraud



Sign up, or Be Signed Up!

• How Was Your Card Stolen?



Finding out is not so easy.

• Krebs's 3 Rules...





...For Online Safety.