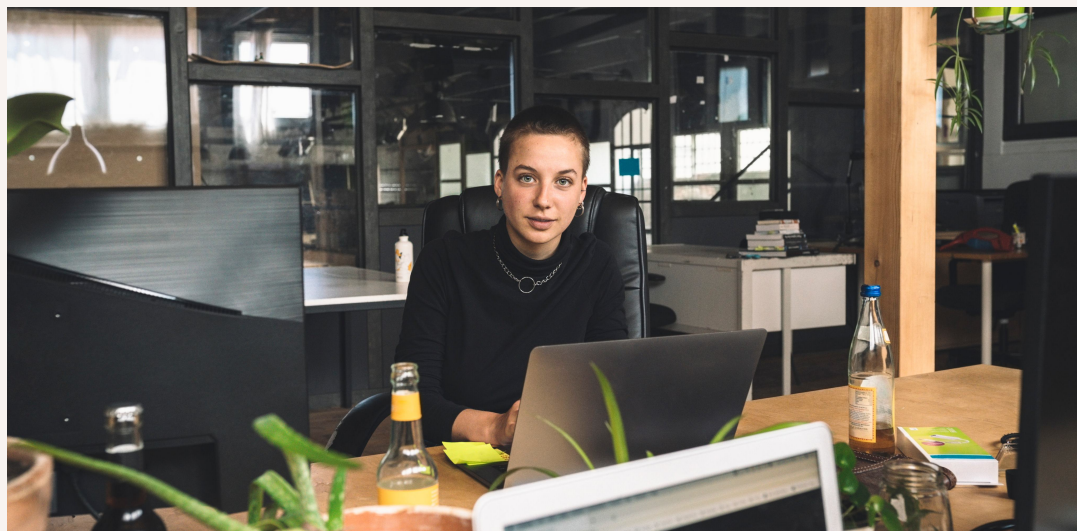




Whitepaper

Combating Phishing

A proactive approach



You can't afford to take risks when documents contain highly sensitive information. Protecting your data is Docusign's top priority.

That's why our world-class security and operations teams work 24/7 to protect the millions of Docusign users and the wider internet community from phishing attacks.



An experienced team and a sophisticated methodology

DocuSign proactively detects and deters phishing attempts by tapping the deep expertise and experience of the DocuSign security team in combination with sophisticated automated techniques, including:

- **Leveraging custom automation tooling** (developed in conjunction with the DocuSign cybersecurity team) to process potentially fraudulent URLs submitted to spam@docuSign.com by customers or reported in threat intelligence feeds
- **Using machine learning algorithms** to improve accuracy and reduce false positives when identifying phishing attempts
- **Using performance dashboards and visualizations** to track phishing trends over time and analyze phishing pages in real time
- **Enforcing a DMARC (Domain-based Message Authentication, Reporting and Conformance) reject policy** on DocuSign.net, so any spoof email purportedly sent from docuSign.net is rejected by all email providers supporting DMARC, after which, the email content is sent to DocuSign for analysis
- **Analyzing attackers' actions and proactively detecting attacks** by conducting forensic investigations and credential seeding
- **Partnering with leading security vendors and law enforcement organizations** to share, blacklist and take down malicious websites and prevent further phishing attacks

Don't get phished

Tips for foiling attackers

A few simple techniques can help you spot the difference between a spoof DocuSign email and the real thing:

- Hover over all embedded links: URLs to view or sign DocuSign documents contain “docusign.net” and always start with “https”
- Access your documents directly from docusign.com by entering the unique security code found at the bottom of every DocuSign email
- Don't open unknown or suspicious attachments, or click links—DocuSign will never ask you to open a PDF, office document or zip file in an email
- Look for misspellings, poor grammar, generic greetings, a false sense of urgency and/or a demand
- Enable multi-factor authentication where possible
- Use strong, unique passwords for each service— don't reuse passwords across multiple websites
- Ensure your anti-virus software is up to date and all application patches are installed
- Contact the sender offline to verify the email's authenticity, if you're still suspicious
- Report suspicious DocuSign emails to your internal IT/Security team and forward to spam@docusign.com

Sophisticated attackers

send emails that spoof real DocuSign envelopes and emails but contain false links that lead to malware, such as ransomware. When a large malware or phishing campaign is detected, a security notice containing relevant details is posted on the [DocuSign Trust Center](#).




Fake DocuSign examples

In the examples below, the URLs don't start with "https" nor do they include "docuSign.net."


Fake email

<dse_na3@docuSign.net001>

From: DocuSign via DocuSign <dse_na3@docuSign.net001>
 Date: March 9, 2020 at 9:32:45 AM MST
 Subject: Completed. Please DocuSign: Payment Info



docuSign



Your document has been completed.


[VIEW COMPLETED DOCUMENTS](#)

http://civils360.com/wp/redirect.php

Fake login page








https://sunrisenewspost.com/wed/Dc1/docu/a/

https://sunrisenewspost.com/wed/Dc1/docu/a/



DocuSign

LOG IN TO DOCUSIGN USING

-  Google
-  Microsoft Account
-  AOL
-  Yahoo!
-  GoDaddy
-  Office 365
-  Other Email

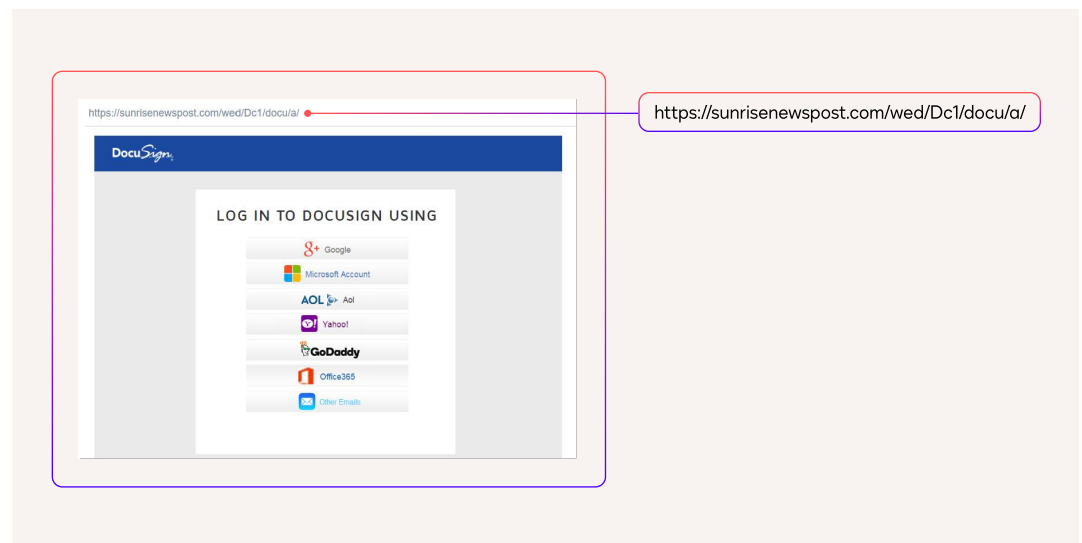
Fake DocuSign examples

In the examples below, the URLs don't start with "https" nor do they include "docusign.net."

Fake email



Fake login page



Phishing

On the rise and more sophisticated

As a well-known and trusted brand, DocuSign is a prime target for malicious, third-party phishing attacks. According to [PhishLabs](#), attacks in 2017 shifted to enterprise-focused phishing that impersonates services that organizations rely on such as Software as a Service (SaaS) platforms. DocuSign-themed phishing attacks topped the list of most used lures.¹

When savvy attackers send phishing emails to individuals, compromising the DocuSign account isn't always the aim of the attack. Often, they want to gain access to the victim's email credentials, utilizing the username and password combination used on DocuSign. The tendency of most people to reuse usernames and passwords across websites, coupled with the trend of organizations using email addresses for user IDs, makes it easier for attackers to steal valuable information and exploit it.

The ultimate goal of these attacks is to sell stolen information, gain access to proprietary information for competitive reasons, lock up systems and demand a ransom or further exploit the individuals.

What is phishing?

Phishing is a technique used by attackers to trick individuals into divulging personal information—like their login credentials—or launching malware to steal broader sets of personal data stored on their computers or connected networks.

A phishing email typically looks like a valid email from a trusted source, duping recipients into opening the email and clicking on enclosed attachments or links.

It's estimated that 4% of people will click on an attachment or link in a phishing email.²

Beyond phishing: social engineering

Social engineering is the broad term used to describe the various tactics and techniques—including phishing—used by attackers to psychologically manipulate and deceive individuals into divulging personal or confidential data. Tactics used include:

- Taking a position of authority
- Exploiting one's desire to help
- Playing on emotional needs or fears
- Offering something to win or obtain for free

¹ PhishLabs, 2018 Phishing Trends & Intelligence Report
² Verizon, 2018 Data Breach Investigations Report

Conclusion

With the number of phishing attacks growing every day, it's essential to stay ahead of these challenges. Docusign is committed to employing the latest technology and industry knowledge to keep our customers safe from attackers—but it takes awareness and commitment from everyone involved to achieve the highest level of security.

Learn how to tell the difference between spoof and legitimate emails, put into practice the tips for foiling attackers and remember to report suspicious emails to spam@docusign.com. Doing so helps in keeping you—and the wider Internet community—safe

For Docusign security and system performance information, visit the [Docusign Trust Center](#).



About DocuSign

DocuSign brings agreements to life. Over 1.5 million customers and more than a billion people in over 180 countries use DocuSign solutions to accelerate the process of doing business and simplify people's lives. With intelligent agreement management, DocuSign unleashes business-critical data that is trapped inside of documents. Until now, these were disconnected from business systems of record, costing businesses time, money, and opportunity. Using DocuSign IAM, companies can create, commit, and manage agreements with solutions created by the #1 company in e-signature and contract lifecycle management (CLM).

DocuSign, Inc.
221 Main Street, Suite 1550
San Francisco, CA 94105
[docusign.com](https://www.docusign.com)

For more information
sales@docusign.com
+1-877-720-2040