When documents contain highly sensitive information, you can’t afford to take risks. Protecting your data is DocuSign’s top priority. That’s why our world-class security and operations teams work 24x7 to protect the 100+ million DocuSign users and wider Internet community from phishing attacks.

It Takes a Village…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 and automated techniques, including:

- **Leveraging custom automation tooling** – developed in conjunction with the DocuSign Cybersecurity Centre of Excellence – to process potentially fraudulent URLs submitted to spam@docusign.com by customers and detected in threat intelligence feeds from private and public sources
- **Utilizing 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, and malicious content is reported to and analyzed by DocuSign
- **Analyzing attacker’s 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 Scammers

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

• Hover over the link – URLs to view or sign DocuSign documents contain “docusign.net/” and always start with https
• Access your documents directly from www.docusign.com by entering the unique security code, which is included at the bottom of every DocuSign email
• Do NOT 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, and a false sense of urgency
• Enable multi-factor authentication where possible
• Use strong, unique passwords for each service – don’t reuse passwords on 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 IT/security team and spam@docusign.com

Fake/Spoof DocuSign Examples

Sophisticated scammers occasionally send emails with fake DocuSign 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.

The URL doesn’t start with https nor does it include “docusign.net/”
Phishing: On the Rise and More Sophisticated

As a well-known and trusted name, the DocuSign brand is a prime target for malicious, third-party phishing attacks. According to PhishLabs, attacks more than doubled against DocuSign and other leading SaaS providers in 2016.*

When savvy fraudsters 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 account utilizing the username and password combination used on DocuSign. The common practice of reusing passwords across websites, coupled with the trend of organizations using email addresses for user IDs, makes it easier for fraudsters to steal valuable information and exploit it for financial gain.

The ultimate goal of these attacks is “wire transfer” or “business email compromise” fraud – one of the fastest-growing schemes over the past several years, according to the FBI. In this scenario, scammers steal money from small businesses in a complicated man-in-the-middle attack on financial transactions.

What Is Phishing?
Phishing is a technique used by hackers 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 attempt typically looks like a valid email from a trusted source, duping recipients into opening the email and clicking on the enclosed attachments or links.

Beyond Phishing: Social Engineering
Social engineering is the broad term used to describe the various tactics and techniques—including phishing—used by criminals 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

* PhishLabs, 2017 Phishing Trends & Intelligence Report
Conclusion

With the proliferation of phishing attacks growing every day, it’s essential to stay ahead of these challenges and mitigate any risk. DocuSign is committed to employing the latest technology and industry knowledge to keep our customers safe from fraudsters – but it takes an 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 fraudsters, and remember to report suspicious emails to spam@docusign.com. Doing so helps keep you – and the wider Internet community – safe.

For DocuSign security and system performance information, visit the DocuSign Trust Center at https://trust.docusign.com/.