DocuSign®

Whitepaper

Protecting Your Organization Against DocuSign Brand Impersonation

With the number of phishing attacks growing every day, it's essential to understand the potential threats, like brand impersonation, and how to thwart them.

Threat actors intentionally choose the most well-known and trusted brands as social engineering lures for phishing attempts and other cyberattacks. Unfortunately, these threat actors try to impersonate DocuSign in an attempt to trick you into revealing your credentials and more.

This paper explains what brand impersonation is, how DocuSign is combating it and the steps you can take to protect yourself and your organization from these threats.

Brand impersonation: what it is and what it isn't

Brand impersonation is a social engineering technique that imitates a familiar brand for malicious purposes. In the case of DocuSign, attackers take advantage of user familiarity with the DocuSign eSignature service to increase the likelihood that would-be victims will fall for the attack.

What's important to note, however, is that brand impersonation doesn't mean there's been any compromise of the DocuSign platform—which is a common misconception.

In fact, it's easy for threat actors to craft DocuSign-themed phishing attacks by simply copying publicly available resources, such as DocuSign's website, despite the fact that the DocuSign eSignature platform is highly secure. DocuSign meets some of the most stringent US, EU and global security standards and uses the strongest data encryption technologies available.

For more on phishing attacks, what they are, how to spot them and tips for foiling attackers, read Combating Phishing: A Proactive Approach.

Common brand impersonation threats using the DocuSign brand

Phishing

Credential phishing is one of the most prevalent attacks that abuse the DocuSign brand. These attempts typically come via malicious emails, but they may also occur through URL redirection and social media or a combination of these tactics. Often, outdated logos and branding elements are used, but savvy criminals pay attention to updates and may eventually move to our current brand.

To address this, DocuSign uses an automated phishing classification system called Pescatore to identify and takedown DocuSign-themed phishing sites. With this system, DocuSign sends thousands of takedown requests per year.

To the right is an example of a DocuSign-themed phishing site. Before entering your DocuSign credentials, double check that you're on the correct website: https://www.docusign.com or https://www.docusign.net (if an embedded link in a DocuSign email).

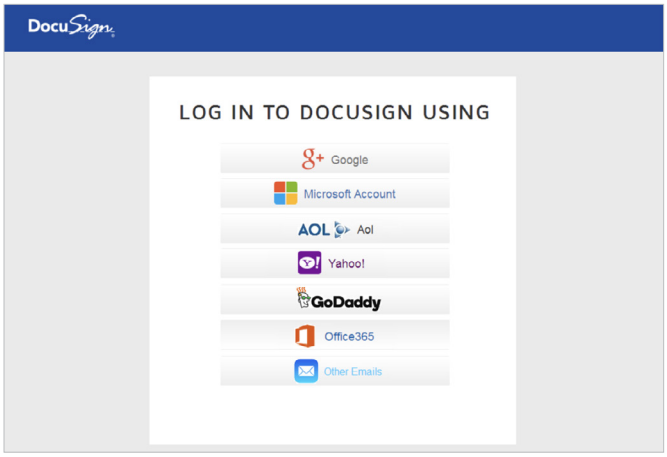

Figure 1: DocuSign-themed phishing site

Malicious email campaigns

Based on DocuSign's internal monitoring, we see numerous DocuSign-themed malicious email campaigns every month. The lure is presented in the form of email content, which may or may not include attachments.

Email campaigns are dangerous, because they can lead to various attacks, such as phishing, fraud, backdoors, banking trojans, ransomware or a combination of these threats.

Whenever we observe a noteworthy campaign, we publish an alert on the DocuSign Trust Center. This helps you remain vigilant while also allowing us to share relevant threat indicators to network defenders. Malware families that have abused the DocuSign brand for malicious email campaigns have included Hancitor, Trickbot, Qbot, Ficker Stealer, IcedID, Ursnif and others.

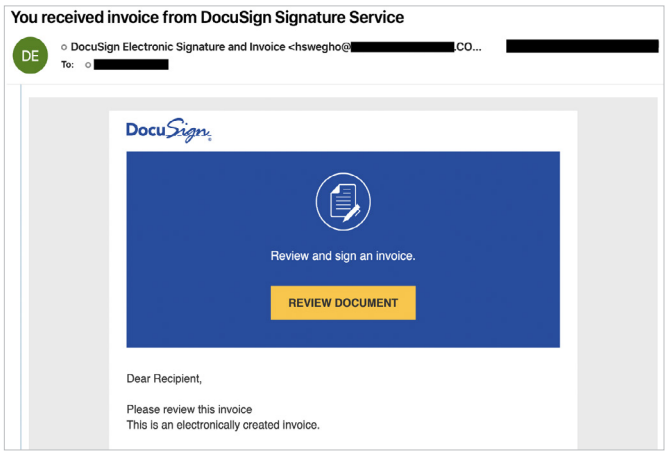

Figure 2: DocuSign-themed malicious email

DocuSign-themed attacks: how to protect your organization

Educate users

Educate users about brand impersonation attacks and how to recognize them. Our whitepaper, Combating Phishing, and our blog, "How to Avoid Phishing Scams," offer easy-to-follow tips on how to protect yourself from phishing and malicious emails.

Block threat indicators

Implement a system that regularly pulls and blocks fresh threat indicators in your organization's environment. DocuSign provides threat indicators as part of our alert notifications on our Trust Site.

Invest in email security

A good email protection system can protect your organization from many email-borne threats, including brand impersonation emails. Additionally, an email security gateway allows you to implement additional security controls that can further protect your organization.

Implement multi-factor authentication (MFA)

In the case of a successful credential compromise stemming from a brand impersonation attack, MFA provides an additional layer of security by blocking account logins that don't originate from the original user.

Report incidents

Help us protect you. If you encounter a DocuSign-themed threat, please report the incident to us so we can take appropriate action.

DocuSign is committed to employing the latest technology and industry knowledge to keep our customers safe from attackers, and we're equally dedicated to increasing awareness and making it easy for you to get the information you need to achieve the highest level of security.

For DocuSign security and system performance information, as well as a well of educational content, visit the DocuSign Trust Center.

DocuSign, Inc.
221 Main Street, Suite 1550
San Francisco, CA 94105

docusign.com

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