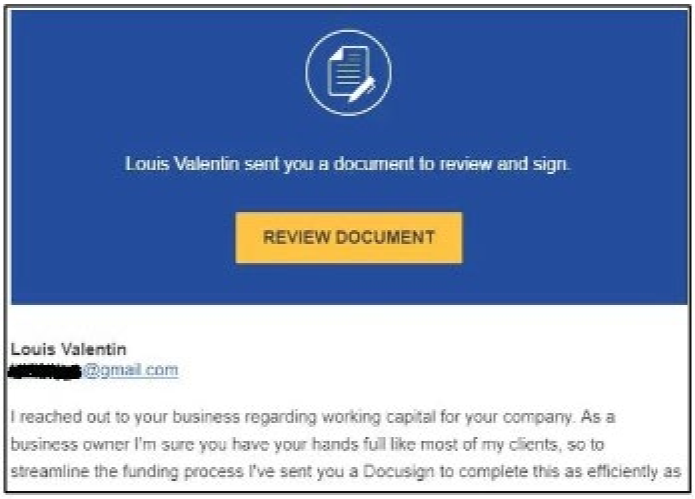
DocuSign / Adobe Acrobat Sign Online Services

We have received several inquiries the last few weeks about online services such as DocuSign, Adobe Acrobat Sign, etc. These are online services that are becoming more and more common in our digital world. They allow for easy access to signatures and quick approval to move forward on a variety of projects. They are great tools, but unfortunately, some bad actors have discovered the power of these tools as well.

From the DocuSign website:

There is a phishing scam that is not so new, but it could be making its way into your inbox soon. It will even pass the usual spam and malware filters and email protection devices. This is because this scam uses the DocuSign infrastructure with the standard DocuSign email notification. Since DocuSign is a well-known and trusted name, the vendor is a prime target for malicious phishing attacks that attempt to perpetrate fraud. If a person clicks on the standard yellow "Review Document" button in the DocuSign notification scam, he or she may receive a standard form requesting sensitive information that could be used to steal the person's identify or perpetrate other forms of fraud. If someone falls for this attack, the damage could be extensive, including financial loss and potential legal repercussions. Therefore, it is imperative for individuals to remain vigilant to this and other types of social engineering threats.



Louis Valentin sent you a document to review and sign.

Louis Valentin
[redacted]@gmail.com

I reached out to your business regarding working capital for your company. As a business owner I'm sure you have your hands full like most of my clients, so to streamline the funding process I've sent you a Docusign to complete this as efficiently as

What Can You Do?

The following tips may help you avoid becoming a victim to a DocuSign phishing scam:

- Were you expecting the document, and do you recognize the sender? Contact the sender offline to verify the email's authenticity.
- 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, an office document, or a zip file in an email message.
- Look for misspellings, poor grammar, generic greetings, and a false sense of urgency.
- Enable multi-factor authentication (MFA) where possible.
- Use strong, unique passwords and don't reuse passwords on multiple websites.
- Ensure your anti-virus software is up to date and all application patches are installed.
- Report suspicious DocuSign emails to IT immediately using your PAB or by calling the IT Service Desk.

For more information, visit https://www.docusign.com/trust/security/incident-reporting.