This Month's Tip: DocuSign Users at Risk!

Be on the lookout for cyber-attacks that include fake DocuSign email messages.

Attackers send fraudulent emails with a link to an authentic looking (but fake) DocuSign login page designed to steal your login credentials and access your accounts. These emails appear to come from a reputable organization or person and contain links or attachments for common documents or notifications (e.g., invoices or account alerts).

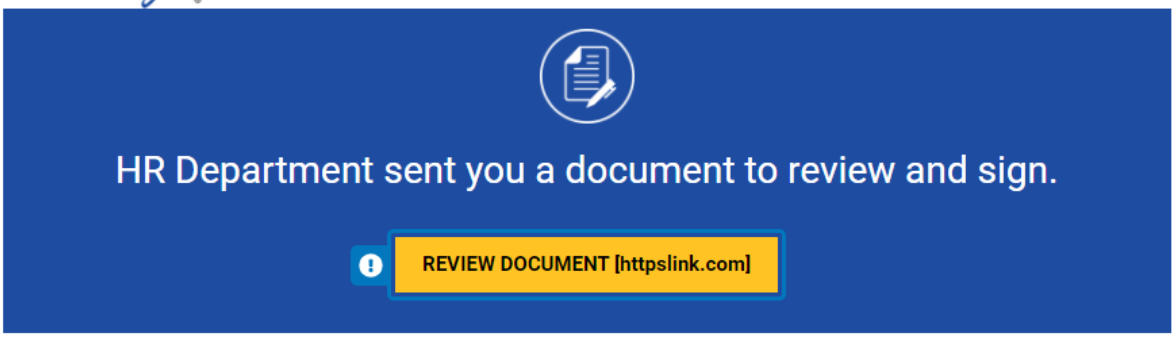
Once attackers have your credentials, they might try to reuse your password to access other accounts, collect sensitive information about you, or use your accounts to trick others.

Multiple variations of this fraudulent email exist, but let's look at one example:

An Example Attack Email

To: Doug
From: HR Department <HR@refated.com>
Subject: [EXTERNAL] HR Sent you a Document

DocuSign



Hi, Doug, please sign your benefits enrollment document.

Thanks,

HR Department

Do Not Share This Email
This email contains a secure link to DocuSign. Please do not share this email, link, or access code with others.

Alternate Signing Method
Visit DocuSign.com, click 'Access Documents', and enter the security code: DEFBAB84A2E04CCEBC71B2DCE501B87B3

About DocuSign
Sign documents electronically in just minutes. It's safe, secure, and legally binding. Whether you're in an office, at home, on-the-go -- or even across the globe -- DocuSign provides a professional trusted solution for Digital Transaction Management™.

Questions About the Document?
If you need to modify the document or have questions about the details in the document, please reach out to the sender by emailing them directly.

If you are having trouble signing the document, please visit the Help with Signing page on our Support Center.

Download the DocuSign App

This message was sent to you by HR Department 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.

Examine Sender
Why would the HR department use a different email domain (@refated[.]com) and why would it come from an external sender? Look for small details that seem off!

Look at Links
When you hover over a link, is the URL what you expect? This link takes you to httpslinks[.]com. Is that a page our HR team would use?

Consider Content with Context
Are you currently enrolling in benefits or was this information requested? Always use caution if the request seems odd.

Be Careful of Signatures
Doesn't this signature look like a real DocuSign email? Scammers often include official looking text to trick you into thinking the email is legitimate.

If you have any questions regarding this tip, please contact Information Security via Mark.Nagiel@SupremeLending.com. Thanks for participating in the Information Security effort!