AttackSpotlight

DocuSign Phishing Campaign

DocuSign Users at Risk

Attackers are sending fraudulent DocuSign emails with links to an authentic-looking (but fake) DocuSign login page designed to steal your credentials. Once attackers have your username and password, they can do real harm to you or your organization.

They might try to:

Reuse your password to access other accounts

Collect sensitive data about you

Use your accounts to trick others into giving up sensitive information

What do I look for?

This is one example of the fake emails. There's a wide variety of these malicious emails because DocuSign is used for so many purposes (legal, financial, employment, etc.).

From: LAZRB HR Department<LAZRB_HR@refated.com
Subject: Please DocuSign Your Benefits Enrollment
To: Doug Xue Hoo<dhoo@laz-rb.com>

DocuSign

LAZRB HR Department sent you a document to review and sign.

REVIEW DOCUMENT

http//:www.blackberndental.ca.

LAZRB HR Team
LAZRB HR@refated.com

Hi, Doug please sign your benefits enrollment document.
Thanks,
The LAZRB 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 LAZRB 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 the Sender

Why would your company's HR department use a different email domain (@refated.com)?

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 blackberndental.ca.

Is that really a page your HR team would use?

Consider Content with Context

Are you currently enrolling in benefits? Does your company typically use DocuSign?

If the request seems odd, use caution.

Be careful of closings

Doesn't this closing look like a real DocuSign email?

Scammers often include official-looking text to trick you into thinking the email is legitimate.

How do I protect myself?

If you get an email asking you to log into DocuSign:

Don't click any links.

Carefully examine the email.

Looks legitimate: Call, message, or send a new email to the sender to verify the email. Never reply to the initial email.

Looks suspicious: Report it to the appropriate people in your company or to your email provider.

proofpoint

Security Awareness Training