Scam of the Week: Tricky Tags in Google Drive Phishing Attack

Phishing emails are often designed to trick you into clicking a malicious link. Most email clients, such as Microsoft Outlook and Gmail, have filters that add warning messages to emails with suspicious-looking links. Unfortunately, the bad guys are always finding new ways to bypass these security filters.

The latest way that scammers sneak past your email security is by taking advantage of the collaboration tools available for the Google Drive platform. The platform allows you to tag any user in a file by using their Gmail address. Once tagged, the user will receive a notification directly from Google. This means that if a bad guy tags you in a Google document, you will receive a legitimate notification from Google that includes a link to the bad guy's file. If you view the file, you'll likely find that it directs you to click another link. This second link is actually a malicious attempt to steal your sensitive information.

Don't fall for this trick! Remember:

- Always be suspicious of emails or notifications from someone you do not know.
- Never click on a link within an email that you weren't expecting—even if it came from a legitimate website.
- If you receive a suspicious email or notification, contact your IT department or follow the specific procedure for your organization.

Stop, Look, and Think. *Don't be fooled.*
The KnowBe4 Security Team
KnowBe4.com