

Scam of the Week: Cybercriminals are Getting Creative with Canva

Cybercriminals often use legitimate websites in their phishing attacks as a way to get around the security systems that your organization has in place. A recent example of this is the use of Canva, a popular graphic design platform. Canva provides users with a variety of ways to create and share visual content. Cybercriminals are using Canva to create an official-looking document that contains a clickable, malicious link. Creating and storing this document on Canva allows the attackers to get through security measures because Canva is a legitimate website.

Once the scammers have created and stored their file on Canva, they will send you an email that includes a link to this malicious file. The email claims the link leads to an important document that needs your attention. However, if you click this link, you are taken to the Canva file and prompted to click *another* link in order to view the document mentioned in the email. Clicking this second link will redirect you to a phony login page for your email provider. Any information entered on this page will be sent directly to the scammers. Don't be fooled!

Remember these tips:

- Never click a link in an email that you were not expecting.
- Call the sender to be sure the email and link are legitimate. Do not call the phone number provided within the email as it may be a fake number.
- When you're asked to log in to an account or online service, navigate to the official website and log in. That way, you can ensure you're logging in to the real site and not a phony look-a-like.

Stop, Look, and Think. *Don't be fooled.*

The KnowBe4 Security Team

KnowBe4.com