Scam of the Week: Exploiting the Coronavirus: Re-opening your organization? The bad guys have a plan!

Recently, some countries have chosen to lift restrictions that were originally put in place to control the spread of COVID-19. Beware! The bad guys are already taking advantage of this news. They have crafted a well-written phishing email that appears to come from the VP of Operations in your organization. The message claims that your organization has a plan for reopening, and it instructs you to click on a link to see this plan. Clicking the link opens what appears to be a login page for Office365, but don't be fooled! If you enter your username and password on this page, you would actually send your sensitive credentials directly to the bad guys.

Here's how to protect yourself from this clever attack:

- Never click on a link or an attachment that you weren't expecting. Even if it appears to be from someone in your own organization, the sender's email address could be spoofed. When in doubt, reach out to the sender by phone to confirm the legitimacy of the email before clicking.
- When an email asks you to log in to an account, do not click the link in the email. Instead, go directly to the website through your browser. This ensures you are accessing the real page and keeping your credentials safe.
- This attack tries to exploit the restlessness and uncertainty of life in quarantine. Don't let the bad guys toy with your emotions. Think before you click!

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