Scam of the Week: Watch Out for “Free Gift” Scams

Watch out! Cybercriminals are posing as a mail carrier company that claims to have a “free gift” waiting for you.

They start by sending a shipment notification email. The email includes a tracking code and other details about your package. If you click on the link in the email and enter your tracking code into this webpage, you’re told that the package has arrived in your country but you must pay a very small delivery fee before you can claim it. If you fall for this offer and enter your payment details, your financial information is stolen and your “free gift” is never mentioned again.

Here are a few reminders to help protect yourself from scams like this:

- *Beware of free gifts.* If it sounds too good to be true, it probably is. Delete suspicious emails or follow the reporting procedures put in place by your organization.
- *Be cautious of courier emails.* Delivery notification emails are often used in phishing attacks. Even if the email appears to be from a familiar organization, reach out to the sender directly (by phone) to get a trustworthy tracking number.
- *“HTTPS” does not equal “secure”.* These days, many cybercriminals are using “HTTPS” websites for their scams because most people look for a padlock in the address bar. However, the padlock does not guarantee that you’re on a legitimate website, it only means that you’re on a website that has obtained an HTTPS certificate.
- *Don’t click.* Never click on links or download attachments from emails you weren’t expecting–even if it appears to be from a legitimate organization.

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