Scam of the Week: Smishing for Access to Your Bank Account

Emails are a quick and easy way for cybercriminals to phish for your information—but it's not their only tool. Smishing, or SMS Phishing, is another way the bad guys try to trick you. Many of us are used to receiving legitimate promotions, reminders, and security notifications via text message. These messages—both real and fake—are brief and often include links, so it can be difficult to spot a smishing attempt.

One recent example involves scammers posing as your local postal service while sending malicious text messages as part of their smishing attack. The message claims that you have a package waiting for pick up, but to see more information you must click the link in the text. If you click the link, you're taken to a phony verification page. Here, you're asked to enter your banking information in order to verify your identity. If you provide any information on this page, your data is sent directly to the cybercriminals—giving them full access to your bank account. Don't be fooled!

Here's how to stay safe from this smishing attack:

- Think before you click. Are you expecting a package? Is this how the postal service usually handles things? Consider anything out of the ordinary a red flag.
- Never trust a link in an email or text message that you were not expecting. Instead of clicking the link, open your browser and type the official URL of the website you wish to visit.
- Go old school. Pick up the phone and call your local post office. Be sure to call their official phone number—not the one that sent you the suspicious text message.

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