KnowBe4



Security Hints & Tips

Watch Out For Smishing!

What it is...

Many companies, products, and services have started offering text message alerts to keep you up to date. Scammers are aware of these alerts and they're taking advantage of unsuspecting individuals. They send a text with dangerous links, or prompt you to respond with personal information by posing as your bank, an online account, or other service–to name a few examples. This Short Message Service (SMS) or text-based phishing scam is called Smishing, and the bad guys have taken a liking to it.

How it works...

The following are only a couple of examples. The bad guys are constantly coming up with new ways to “smish” you:

Use this Link: Scammers pose as a familiar company or service and send shocking alerts such as–“Your account has been locked due to multiple failed logins.”–accompanied by a link to supposedly resolve the issue. Smishing links can contain malware that instantly installs if you made the mistaking of clicking. This malware can contain keystroke-logging software or permit access to your applications and files–making it easy to steal your identity or hold your files for ransom.

Call this Phone Number: Smishing attacks often try to persuade you into calling a number by telling you there’s been an issue with your account or that suspicious activity has been detected. A scammer will be ready to take your call and persuade you into providing personal information or making a payment.

Think before you tap!

- Remember that government agencies, banks, or any other legitimate business will never request sensitive information over a text message.
- Take your time. Much like email phishing, texting scammers will often use the social engineering tactic of creating a false sense of urgency in their message.
- Never click on any links or call any phone numbers in unexpected texts. Contact the company directly if you’d like to verify the text message.

The KnowBe4 Security Team