CYBERSECURITY AWARENESS MONTH

Whose Text Message Is That Anyway?

Is that text from Mom or. . .?

We all know about phishing scams, right?

When a scammer uses a text instead of an email, it's just another kind of phishing attack called a "smish," short for SMS phish. "SMS" stands for "short message service" and is the technical term for the text messages you receive on your phone.

Hackers never miss an opportunity or overlook an option when trying to trick you into doing what they want. Some smishing scams even impersonate companies you do business with - your bank, cell phone provider, cable company, and so on. In early 2020, scammers impersonated Verizon in wide-ranging smishing attack that instructed people to go to a fake Verizon web site that looked like the real thing, if you didn't notice the URL.

But you don't need to be caught unprepared. Just like an email phishing scam, a smish will have some telltale signs. Here's what to watch out for:

- **The text is from a 5000 number**
  That's a number commonly used by scammers, so be cautious if you get a text from a 5000 number.
- **You don't recognize the number**
  If you don't recognize the number, don't respond. If it's important, the person or company will use another way to reach you.
- **Something about the text just doesn't feel quite right**
  If your *spidey* sense is tingling that's a good sign. Don't ignore it. Give the sender a call instead of replying to their text.
- **The text says you need to respond immediately because its an emergency or urgent**
  Scammers try to scare you into responding immediately. If you get a text that is alarming, even from a company you recognize or may do business with, don't respond right away. Take a deep breath, look closely at the text, and then respond by calling the company who sent the message. Don't use the phone number in the text, but the contact info on the company's web site.
- **Attachments**
  Even an attachment from a friend or someone or organization you trust might be carrying malware or a virus. Don't click or open them.
- **Asking for personal info, or to verify a service you didn't sign up for**
  Trustworthy companies never ask for personal information via text. Don't respond.