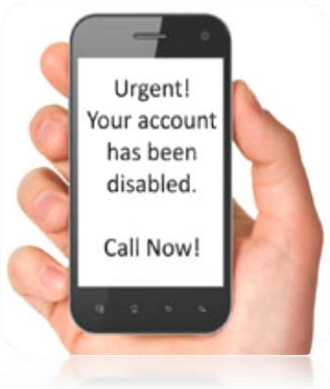
Smishing: 4 Things You Should Know



You may never have heard the term "smishing," but if you're like most people, you've experienced it. Here are some essential facts about this fast-growing security problem:

1. **Where the name originates.** We all know about phishing, traditionally considered an email phenomenon. Well, smishing is the same thing—but the attack messages come via text messages on your phone. Technically, these messages are known as SMS text, so "SM" plus "phishing" equals "smishing."

2. **Why it's a growing problem.** Keep in mind that your phone has more computing power than the PCs of just a few years ago. Also, consider the incredible amount of sensitive data that lives on that phone: your contacts, work-related emails, account numbers, credit-card data, and more. This info is what the bad guys are after, often to drain your funds or commit identity fraud.

3. **How phones are riskier than PCs.** Experts say that by now, most experienced computer users have at least some savvy when it comes to spotting phishing messages. However, most users have a different relationship with their phone. It's more personal, more connected to their life. So study after study finds that people are more likely to fall for smishing than for email phishing.

4. **What you should do.** First, be as skeptical about text messages as you are about emails. Anytime you think you've sniffed out a smishing attack, you should simply delete the text and add the number to your phone's "blocked" list. Experts stress that you should never respond to a smishing attack by typing *No* or *Stop*, even if the message explicitly says you may do so; the response will simply cause your phone to be flooded with fresh attacks.