Text Message "Smishing"

In the world of text there is a SCAM called Smishing, which is a form of phishing. Smishing is when someone tries to trick you into giving them your private information via a text or SMS message.

Smishing is particularly scary because sometimes people tend to be more inclined to trust a text message than an email. Most people are aware of the security risks involved with clicking on links in emails. This is less true when it comes to text messages.

Smishing uses elements of social engineering to get you to share your personal information. The information a smisher is looking for can be anything from an online password to your Social Security Number to your credit card information. Once the smisher has that they can often start applying for new credit in your name or use your identity for other fraudulent purposes.

Another option used by smisher is to say that if you don't click a link and enter your personal information that you're going to be charged per day for use of a service. If you haven't signed up for the service, ignore the message. If you see any unauthorized charges on your credit card or debit card statement, take it up with your bank.

In general, you don't want to reply to text messages from people you don't know. That's the best way to remain safe. This is especially true when the SMS comes from a phone number that doesn't look like a phone number, such as "5000" phone number. This is a sign that the text message is actually just an email sent to a phone.

You should also exercise basic precautions when using your phone such as:

- ✓ Don't click on links you get on your phone unless you know the person they're coming from. Even if you get a text message with a link from a friend, consider verifying they meant to send the link before clicking on it.
- ✓ Never install apps from text messages. Any apps you install on your device should come straight from the official app store. Err on the side of caution. If you have any doubt about the safety of a text message, don't even open it.

Almost all of the text messages you get are going to be totally fine. But it only takes one bad one to compromise your security. With just a little bit of common sense and caution, you can make sure that you don't become a victim of identity theft.

If you have any questions or concerns please do not hesitate to call the Department at 413-628-4441 ext. 1 or 413-625-8200.

Chief Beth Bezio