To all KYECTF members:

Please advise your clients, colleagues, families and friends of the scamming trend called SMiSing or SMS phising which has increased in popularity over the past two months.

SMiShing is basically phishing scams that are sent over Short Message Service (SMS) text messages.

As you may know, most phishing scams play on your fear of things such as:

- Fear of someone stealing your money
- Fear of being accused of a crime that you did not commit
- Fear of someone doing harm to you or your family
- Fear of something embarrassing being revealed about you (whether it is true or not)

A lot of phishing attacks which end up being successful likely go unreported because the victims don't want people to think they were gullible enough to get conned.
Phishers refine their scams over time learning which ones work, and which don't. Given the short nature of SMS messages, phishers have a very limited canvas on which to work so they have to be extra creative in a SMiShing attack.

Here are a few tips to help you tell spot SMiShing scam texts:

- **Review your bank's and credit card company's policy on sending text messages**

  Many banks don't send text messages because they don't want people to fall for smishing attacks. If they do send texts find out what number they use to generate them so you will know if they are legitimate. The scammers may use spoofed alias numbers that look like they are from your bank, so you should still be skeptical and not reply directly. Contact your bank at their regular customer service number to see if the text was legit or not.

- **Beware of messages that have a number that says it is from "5000"**

  Email-to-Text services often list 5000 or some other number that is not a cell number as where they originated from. Scammers are likely to mask their identity by using Email-to-Text services so that their actual phone number is not revealed.

- **Ask yourself if the suspicious text preys on the fears mentioned above**

  If the message content fits into one of the fear categories above, be extra skeptical. If it is threatening in any way to you or your family members, report it to the local authorities and also to the Internet Crime Complaint Center (IC3) .

- **Never reply to a suspicious text without doing research and verifying the source.**

  If it is really your bank texting you, then they should know exactly what you are talking about when you call them using the phone number on your latest statement. If they say there are no issues with your account, then the text was obviously bogus.

  Can anything be done to prevent smishing texts from reaching you? Here are some steps you can take to keep the SMiShers at bay:

- **Use Your Cell Providers Text Alias Feature**

  Almost all major cell providers allow you to setup an Text Alias that you can use to receive texts. The texts still come to your phone and you can send texts, but anyone you text sees your alias instead of your actual number. You can then block incoming texts from your real number and give all your friends and family the alias you are using. Since scammers most likely won't guess your alias and can't look it up in a phone book, using an alias should cut down on the number of spam and smishing texts you receive.

- **Enable the "block texts from the internet" feature if available from your cell provider**

  Most spammers and SMiShers send texts via an internet text relay service which helps hide their identity and also doesn't count against their text allowance (scammers are notoriously frugal). Many cell providers will let you turn on a feature that will block texts that come in from the internet. This is another easy way to cut down on spam and smishing e-mail

The Better Business Bureau has issued warnings about this kind of scam. Here's some advice from the BBB:

- **Don't fall for it.** Know that retailers or others generally don't just give away very valuable gift cards or products for free. If it seems too good to be true, it probably is.
- **Don't reply.** Delete the message, without replying. If the text includes a phone number, don't call it. You'll just be calling attention to yourself as a potential victim to target. Don't click any links, as they could leave dangerous files on your phone or other device.
- **Don't give up your personal information.** You may be told that your information is needed in order to release a prize to you. Don't believe it. Don't give your bank account number or wire money to anyone, either. (Some scammers say you need to send in money for shipping or taxes, for example, before they can send you a big gift.)
- **Report it.** Call your cell-phone service provider and have the number the text came from blocked. You might have them block all premium text messages, as well.
- **If the scammers succeed:** If you think you've been a victim of smishing, contact the BBB. They can help you determine if you've been victimized and file a complaint against the perpetrator. You can also file a complaint with the Federal Trade Commission (FTC) at www.ftc.gov or via 1-877-HELP (4357). You should also call your affected credit card companies or banks, to alert them and perhaps cancel accounts and get new ones.

- **Be vigilant:** Finally, remember to check your credit report regularly, for signs of foul play. You may, after all, have been victimized without even realizing it. You can get a free copy of your credit report from each of the reporting agencies once per year, at www.annualcreditreport.com to look for fraudulent activity, and report the incident to BBB.

References:
-Bradley, T (2012, May 3). 'Smishing' Attacks are on the Rise. Retrieved June 4, 2012, from http://www.pcworld.com/businesscenter/article/254979/smishing_attacks_are_on_the_rise.html
-Maranjian, S. (2012, May 30) Smishing Scams: Sorry, You Did Not Win a $1,000 Target Gift Card. Retrieved June 4, 2012 from http://www.dailyfinance.com/2012/05/30/smishing-scams-sorry-you-did-not-win-a-1-000-target-gift-card/
-O'Donnell A. (2012, May 18) Protect Yourself From SMiShing (SMS Phishing) Attacks. Retrieved June 4, 2012 from http://netsecurity.about.com/od/secureyouremail/a/Protect-Yourself-From-Smishing-Attacks.htm

Thanks,

Rick Nord
Special Agent
United States Secret Service
Louisville Field Office