New Scam Targeting Users of Cell Phones - An ACCESS Fraud Alert

November 14, 2011 - There is a new scam making the rounds that targets users of cell phones. Known as a "smishing" scam - similar but not to be confused with phishing scams - potential victims are sent text messages. If they click on the links in the message, or if they reply to it, they could have real problems with fraud or even identity theft.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

The scam is very simple. Crooks send out millions of text messages that contain links to malicious software. Once a victim clicks on the link, that malicious software is downloaded to their phone, where it collects user names, passwords, account numbers and other personally identifiable information. That information is then secretly transmitted back to the people who designed the software.

Victims can quickly find that their bank accounts are drained, their credit cards are maxed out and in a worst case scenario, that their identities have been stolen. To make matter even worse, a study by Trustee shows that cell phone users are three times more likely to click on links on their cell phone than they are when using e-mail.

So here are some rules to follow if you respond to text messages on your phone.

1. If you have a smart phone, install antivirus and anti malware applications on it. Just this one step can save you a lot of heartburn later on. And there are numerous applications available; often for free.

2. Never click on links from unknown parties - in text messages or email, on your phone or on your computer.

3. If you receive text messages from your bank or credit card company that appear to be real, don't click on links in these messages. You can't be sure that it was actually your bank or credit card company that sent them to you. Instead, pick up the phone and call these companies to confirm the information you receive. And don't use the phone numbers that may be supplied in the text message you receive. That may be fake too. Take the time to look the number up yourself.

4. Don't respond to text message from unknown sources. All you are doing is confirming that your phone is active. That could come back to haunt you later on.

5. And finally, all of the rules for safe browsing that you practice on your computer should also be practiced on your phone. If anything, your cell phone is more vulnerable to attack than your computer, and the results of an attack can be devastating.

byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter: