New Scam Targets Cell Phone Users in US and Abroad

October 18, 2013 - Scam artists are now targeting mobile phone uses whose phones use a SIM card. While not all phones use the cards, most AT&T and T-Mobile devices require them. Other American cellular providers have certain phone models with have the cards; usually required in phones that will work internationally. Those who fall for the scam can find that they have racked up thousands of dollars in international phone calls and, in some cases, have their bank accounts drained or getting hit with other charges.

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 simple and effective; allowing hackers to reassign the SIM card in the victims' phone to another device. Once that is done, a cloned SIM card is used by the crooks to make phone calls and engage in other activities. Here is the way it has been working in the United States.

Most victims receive a phone call; supposedly from a representative of their mobile phone carrier. The caller is likely to know the victim's address already and may offer discounts or other perks in return for them participating in a customer survey or enrolling in a new service. All the victim has to do is provide the last four digits of their social security number to verify their identity.

Those four digits are frequently used as the SIM card password in mobile phones. Once the caller has that information, he can reassign the card to another phone. Within hours of that happening, the victims phone will no longer work but the phone that the crooks assign its SIM card too is likely to be accumulating thousands of dollars in international call charges.

Crooks are also using the scam to help them commit various forms of identity theft. For instance, if an ID thief has managed to get access to someone's ATM card, many banks now send out text messages to verify that ATM transactions are authorized. But if the scammer can reassign the SIM card in a victim's phone, he can intercept any text messages sent to the victim.

Internationally, some phones are actually tied to bank accounts and can be used to make purchases in retail establishments. As a result, mobile phone customers who live in countries other than the United States may be even more attractive targets of these scam artists than Americans. But that isn't stopping the scam here.

All of the victims that we are currently aware of have been contacted by phone. Since the ultimate goal of the caller is to

gain access to the victim's cell phone account password, anyone receiving a call asking for the last four digits of their SSN or other private information should get off the phone quickly. Don't be fooled if your caller ID says that it is your phone company calling. These crooks are spoofing the caller ID information that shows up on victim's phones.
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:

Follow ACCESS