New ID Theft Scam Coming to Your Home Computer

August 21, 2012 â€“ A new scam to steal your identity, drain your bank accounts and use your credit card information is making the rounds, and this one is a little different from any weâ€™ve seen before. Home computer users in Connecticut have been receiving calls telling them that their home computer networks have been spreading a computer virus. They are then asked to provide sensitive information about their home network to the caller. Anyone falling for the scam is essentially telling the caller everything they need to know to break into their network, and maybe even their computer.

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 calls have been coming from a phone number that is spoofed. So far, the people receiving the calls have said that the phone appears to belong to McGraw Hill, but they could be spoofed to look like they come from anyone including law enforcement agencies.

When victims answer their phone, they are told that their home network is spreading a dangerous computer virus to other computers and they are asked to provide all of the information necessary for the caller to log into their network wirelessly.

Anyone who has access to this information can intercept any communications going across the network. This includes passwords, bank account information, social security numbersâ€¦ pretty well any data that is transmitted. In many cases, they will also be able to see other computers that use the network and gain direct access to the hard drives on each of them. This could allow they to implant malware and directly download any information that is stored on those devices.

There are absolutely no barriers to entry for this scam. It is inexpensive for anyone to start this type of scam and very difficult for law enforcement to track down the people behind it. The victims never see the face of the person behind the

scam, and there is a real possibility that the people placing the calls have actually altered their voices electronically. In other words, itâ€™s a scam with almost no risk to the scam artists. Because of that, it will almost certainly spread across the country very rapidly.

You should never give out information about how to access your computer network â€“ home or work â€“ unless you actually know who you are furnishing that information to. Law enforcement agencies and companies involved in computer protection do not call consumers asking for network log-on information.

If you receive a call similar to the one described here, get as much information as you possibly can from the caller without giving out any information that could compromise you or your computer network. If you have caller ID, make a note of the phone number calling you. Then make your own phone callâ€¦ to the police.

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