Telemarketing for Fraud and Identity Theft

November 22, 2011 - It has been a long time since ID thieves have needed to physically lay their hands on your wallet to steal your identity. The more sophisticated thieves arenâ€™t even rummaging through your trash anymore (although you still need to make sure that you are shredding personally identifiable information before you throw it out). Instead, they are rummaging around the internet, looking for electronic copies of the information they need to assume your identity. The information that makes you a person, in the eyes of creditors and the federal government. But what happens when the thieves can only get some of your information? Well, they hire a telemarketing call center to target you for the rest of it, of course!

The internet security company Trusteer is reporting that its researchers found an advertisement for a telemarketing center. The advertisement offered to call individuals, banks and businesses to assemble a complete identification record when only partial information is available. The cost? Ten dollars per call.

Calls can be made in English and several other languages. The service appears to be operating out of Russia but is open during both European and US business hours. It is especially dangerous because even if you are trying to protect your identity, if the fraudsters behind the service have enough information on you, they can target businesses that you do business with to gain additional information.

Although they may not be able to gain access to enough of your information to assume your identity for all purposes, they may be able to gain access to enough of your information to commit fraud. Things like making purchases using already existing lines of credit you may have, or the ability to drain your bank accounts.

There are some safety precautions that you can take to help protect yourself though. Here are a few of them.

- Always choose passwords and PIN numbers that will be hard for someone else to guess. Never use your birthday for a password or PIN.

- Never carry your SSN or passwords in your wallet or purse.

- Regularly change passwords and PIN numbers.

- Shred your personally identifiable information before throwing it out. This includes address labels that show your name.

- Do not place personal information on social networking websites. In fact, one of the most reliable sources of information on you is for ID thieves and fraudsters to befriend people on your friends list!

- Make sure that if you use a social networking site for purposes other than business that your profile is only visible to your friends.

- Be suspicious of any telemarketing calls you receive that ask you for personally identifiable information. Any such request should be refused if you did not originate the call. This is especially important if your phone number is on the no-call list and you receive a call claiming to be from a business that you don't know or have not done business with in the past 18 months.

This is not the first case of a call center being setup for this purpose, but it is one of the most brazen. It is highly likely that this type of activity will increase so it is important for everyone to be on guard.

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: