Safeguarding Your Credit Card Numbers Not As Easy As It Used To Be â€“ Especially When Traveling

September 6, 2011 â€“ Up until ju8st a few years ago, you could be pretty sure that if your credit card was in your wallet, it was reasonably safe. Of course, anyone you presented the card to could have stolen your information and used it themselves, but that kind of crime has always gone on. With the advent of computer technology though, there are many more threats to contend with today than there used to be. It us up to each of us to know what those threats are, and how to protect ourselves.

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);
})();

Ironically, one the greatest threats to having your credit cards stolen may now be the simple act of carrying your credit cards in your wallet. Thatâ€™s because more and more credit card companies are placing radio frequency identification (RFID) chips in their cards. These chips actually broadcast your credit card information over short distances.

RFID is cropping up in more and more places that threaten individual privacy. The idea behind it was originally to make life a little easier for merchants and consumer alike. No longer would merchants need to swipe your credit card. They could simply wave it over an RFID reader and get all of your information. It is faster, simpler, gets rid of the problem of bad magnetic strips on the back of the card that can no longer be read. Unfortunately, it didnâ€™t take hackers long to realize that if a merchant could read your card information without ever touching your card, so could a criminal.

What hackers have found out is that by using an RFID reader, they simply need to waive it by the purse or wallet of someone with an RFID enabled credit card. That can get them everything they need to be able to make a purchase in your name. By using what is called a hi-gain antennae, they may actually be able to accomplish the same thing but from several feet away. We know that this tactic will work with RFID enabled passports so there is no reason to believe that it wonâ€™t work on credit cards too.

Another vulnerability that consumers now face is the prevalence of unprotected Wi-Fi networks. These networks are now common place in restaurants, airports and hotels. There are also a number of cities that provide them free of charge to anyone living in, or visiting them. While this may seem convenient, it is also a big problem.

Data that is transmitted over an open network is not encrypted. That means that if you are logged onto a network that anyone else can also get into, and you make a purchase using your credit card, your credit card data will be available to anyone who knows how to find it. And heaven help you if you submit a tax form or access your bank account from such a

network. Anyone doing this might as well be wearing a large bulls-eye on their back.

One more potential vulnerability is the now the widespread use of portable devices that we use to connect to the internet. These would include smart phones, tablets and laptop computers. Many of us donâ€™t use any other type of device when getting online. And why not? These devices can go with you wherever your travels bring you. They are small, lightweight, reliable and fairly inexpensive. But all of those traits make them attractive to thieves and make them easy to lose.

There are some steps that everyone can take to reduce the chances of becoming a victim. Here are just a few points to keep in mind.

First, if you are using a laptop or other portable device, make sure that you are not storing your user names, passwords and credit card information on it. If you use a password manager to manage sensitive data on this type of device, make sure that your password manage has a unique password of its own, that it doesnâ€™t automatically insert the password for you, and that any stored data is encrypted. That way, if your portable device is lost or stolen, the data you store on it should be somewhat secure.

If you use Wi-Fi networks when you travel or when you visit the local coffee shop, donâ€™t do any online shopping or upload any sensitive documents from them. You are just inviting trouble if you do.

And finally, look at your credit cards and your passport. If they have RFID technology built in, there is likely to be a symbol o on them or you may actually be able to see the actual RFID chip in them. If you donâ€™t know what to look for, call your credit card companies and ask them if any radio frequency technology is included in your credit cards.

If you find that you have RFID in your credit cards, you have two or three choices. Wrapping your cards in aluminum foil provides reasonably good protection. You can also purchase an RFID protected wallet, credit card sleeves or passport covers. These will also provide a reasonable amount of protection. Of course, if you take the card out of the foil, anyone near you may be able to read it.

You also have another choice. You can simply choose to leave any credit cards that have RFID in them at home if you donâ€™t think youâ€™ll need them. Thatâ€™s one choice that your credit card company isnâ€™t too likely to talk to you about.

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: