

The Risk Of Electronic Fraud & Identity Theft

Article by: Darren Miller

Electronic Fraud and Identity Theft

Human beings are pretty sensible when presented with an imminent threat or risk. That is, if it's staring us directly in the face. Many threats and risk are presented in subtle ways, and it is these subtleties we tend to overlook.

It's The Little Things We Tend To Overlook

Thousands of years ago, it was the subtle things that caused us to take action, to error on the side of caution and protection. A good example, the reports regarding animals seeking refuge early on during the tsunami that claimed the lives of over 300,000 people this past January. Over time, most people have lost the ability to identify the signs, determine the probability, validity, and impact of certain threats and risk.

Making Assumptions vs. Staying Vigilant

At home, my family has given me the nickname "Safety Dad". I tend to be hyper-vigilant when it comes to the safety and protection of my family, probably to a fault. I take a similar position on the security of my computer systems and my financial well-being. On the other hand, I tend to make assumptions about things when I should not. For the most part, I like to think that people are good natured. I believe the majority of people would like to think this way. The sad fact is, this is an assumption that can impact us greatly, and not in a positive manner.

The purpose of this article is to share with you my thoughts and position on some of the basic things you can do to protect yourself from several types of threats. Particularly those that involve electronic fraud and Internet fraud. Although some of these items are not directly related to the Internet, the moment someone has your private or financial information (identity theft), the Internet will be one of the first places they visit.

(Protect Yourself Against Electronic Fraud)

Automated Teller Machines (ATM) & Skimmers

Have you ever heard of a "Skimmer"? If you haven't, you need to be aware the risk this presents you. Skimmer's are devices that appear to be a legitimate part of an automated teller machine but are in fact, fake card readers. They capture all the information stored on the magnetic stripe on the back of the card. Skimmer's have been around for quite some time but their use is on the rise again. The following link will show you what a skimmer may look like and how it is used.

Links

<http://www.defendingthenet.com/Newsletters/ATMSkimmerFraud.htm>

Did you know the cost to a bank or ATM vendor is minimal if their machine is compromised, but to you it may be severe? The company that owns the ATM only has to worry about the cost to replace the machine, plus the amount of money inside. You, on the other hand, stand to lose not only your bank account funds, but possibly your identity.

Phishing and Web Site Redirection

This type of electronic fraud comes in many forms, and is one of the most popular ways of collecting private information, and money from the masses. Why? Because it is simple to do and very effective.

If you receive an e-mail from your bank, credit card company, or other online merchant like, Ebay.com or Amazon.com, requesting information such as passwords and financial info, delete it and report it immediately. Many of these e-mails link you to web sites that look exactly like that of the real company but are in fact fakes. Take a look at Ebay's Online Security and Protection section to get an idea of what you need to do in order to identify scams like these.

Links

<http://pages.ebay.com/help/confidence/index.html>

If you receive an e-mail from someone promising you millions of dollars if you assist them with their finances, delete it immediately!. Some of these scams have been running for years and new ones surface frequently. I recently saw one supposedly from the wife of the late Yasser Arafat, promising millions of dollars if someone would help her establish a trust fund in the US. The reasons these types of e-mail scams are so wide spread is because they are highly effective and relatively easy to do. Thousands of people get ripped off by these scams every day. To see examples of several recent scams, take a look at the following Phishing Scams page.

Links

<http://www.defendingthenet.com/NewsLetters/RecentPhishingScams.htm>

Another good source of information on these types of scams can be found at the State of NY Banking Department.

Links

<http://www.banking.state.ny.us/index.htm>

Credit Card Fraud

Never place your credit card face up when paying for something. Many people will simply place their credit card on the table, face up, when paying for a meal, for instance. In the time it takes for the server to pick up your check, someone walking by can visually scan your card for everything they need to go on an Internet shopping spree. There are thieves that specialize in this type of fraud.

When paying for something, particularly at a restaurant, check to see if the full or partial credit card number is on the merchant receipt. In most cases, only the partial number is visible. However, when the full number is there, I cross out all but the last four digits with a pen. The merchant has already scanned the card at this point, they should not need a paper backup of the number.

If your credit card is stolen, lost, or used fraudulently, you can call your card company and speak with the fraud department. However, I recommend you contact your card company's credit line department first. This is the department that can extend your credit almost instantaneously. They can also decrease it within seconds as well. If you have a limit of \$5,000, they can reduce it to \$100 immediately, then pass you to the fraud department. Call your card company and request the direct number to this department and make a record of it.

If you notice someone swiping your card more than once when paying for an item, ask them why. Regardless of how sensible the answer is, call your card company and request a list of the last few transactions, you might be surprised what you find.

If your card company sends you checks to use for cash advancements and you don't plan on using them, don't keep them around, shred them immediately. We get these all the time in the mail. As far as shredders go, everyone should have one. You can pick up a small one for under \$30 and it is well worth the investment.

Any statements or correspondence you have regarding your credit cards should be in a secure place or shredded.

Credit Reporting & Monitoring

Thoroughly review your credit report at least every 90 days, more frequently if possible. It's better to find out sooner than later if someone else's actions are negatively impacting your credit report, trust me. There are three major credit reporting agencies, Equifax, Experian, and TransUnion. They all have reporting and monitoring solutions available. Some of these services may be free of charge.

Links

<http://www.transunion.com>

<http://www.experian.com>

<https://www.econsumer.equifax.com>

If you find something strange on your credit report, contact the credit reporting agency immediately. In addition to calling them (if possible), send them a certified letter describing what you have found. It's very important to document any and all correspondence on these matters.

Conclusion

I am sure this information may be old news to some. However, if just one person reads this article and learns something new, then my objective has been met.

One of the best ways to protect yourself from electronic fraud and identity theft is to ask questions. Primarily, ask yourself whether or not the particular situation you are faced with makes sense? Why would your bank request information from you via e-mail? Why would someone in another country be willing to give you millions of dollars to assist them with their banking woes?

There is a certain percentage of our population who has absolutely no morality when it comes to the acquisition of wealth. These people know the risk of getting caught is minimal. In many cases, even if they do get caught, they are willing to deal with the consequences given the potential monetary payoff. Stay vigilant and educate yourself on these matters. It really is the best way to protect yourself against the myriad of threats and risks we are presented with

everyday.

About The Author

Darren Miller is an Information Security Consultant with over sixteen years experience. He has written many technology & security articles, some of which have been published in nationally circulated magazines & periodicals. Darren is a staff writer for <http://www.defendingthenet.com> and several other e-zines. If you would like to contact Darren you can e-mail him at <mailto:darren.miller@paralogic.net> or <mailto:defendthenet@paralogic.net>. If you would like to know more about computer security please visit us at <http://www.defendingthenet.com>.

If someone you know has sent you this article, please take a moment to visit our site and register for the free newsletter at <http://www.defendingthenet.com/subscribe.htm>