Cybercrime Protection Tips: Protect Yourself Against Internet Fraud

The internet has made life easier in so many ways. The accumulation of human knowledge is available at our fingertips. We can connect with people on the other side of the world, as if they were only on the other side of the street.

No longer do we need to leave our homes to shop for the items we need, as a greater selection is available on our computer screens, along with countless reviews by both professionals and consumers. And a whole new world of entertainment has been opened up to us by the internet.

But the internet has a dark side as well. Not only has the internet made life more convenient for the average person, it has made it more convenient for criminals as well. A whole new breed of criminal has arisen, specializing in using the internet for nefarious purposes. This has been dubbed the moniker “cybercrime.”

The term cybercrime refers to any crime committed involving computes and networks. It is a broad term, covering a wide range of criminal activities, including such activities as:

- Stealing of business secrets
- Disruption of critical infrastructure
- Stealing of cutting-edge research from universities
- Fraud
- Identity theft
- Sexual predators

While this list is not all-inclusive, it gives us a pretty good idea of how broad an area cybercrime really is. The

criminals who are actively engaged in this area of crime cover just as wide a spectrum as well.

They range from computer geeks who are interested in nothing more than breaking in to systems for bragging rights, through individuals engaged in identity theft, to massive criminal organizations that are raking in hundreds of millions of dollars.

Just to show you how massive an “industry” this has become, the FBI has recently busted the Infraud Cybercrime Ring, which has netted some $536 million in profits from their criminal ventures. While one of the larger organized cybercrime rings out there, they are by no means the largest.

There are national governments as well which are involved in cybercrime, although I’m sure that those governments would refer to it as “cyberwarfare” instead. The difference is one mostly of semantics, but to you and I, the effects are roughly the same, as in both cases the perpetrators are targeted at disrupting our lives and stealing from us.

China is reputed at leading the world in cyberwarfare, with a separate division of their army devoted to this aim. Much of their efforts are focused on breaking in to other governments’ systems, but they are also actively involved in disrupting power supplies, as the ability to disrupt a nation’s electric grid would be an extremely useful weapon for crippling a government during times of open warfare.

Our electric grid gets “tickled” several times a day, as hackers try to gain access to the control systems, both for the grid itself and for power plants. China has reportedly hacked all the way into one of our nuclear power plants, taking control of it for some hours.

Cyberattacks like this can be very dangerous, with the low end of the danger being disrupting the power in people’s homes and businesses. At the high end, the danger includes causing a

nuclear power plant to melt down or even conceivably to blow up, with all the danger to life that such an event entails.

Like any other class of criminal, those involved in cybercrime are trying to take what honest, hard working people make and convert it to their use. Whether this comes through using identity theft to raid our bank accounts or use our credit ratings is immaterial. In either case, they are trying to steal from us.

Computer companies, internet service providers, software companies and even phone companies invest billions of dollars per year in trying to deny these criminals access to our computers and networks, but like any other area of crime, the initiative is with the criminals.

So, how does this affect you and I as individuals? First of all, the money these companies are spending on cybersecurity ultimately comes out of our pockets as higher costs for goods and services. Just about any product or service we buy ends up costing us more, because of this additional cost to the companies we do business with.

A much more direct way that this affects us is through identity theft. In 2014 (the last year for which I can find data) identity theft cost victims $15.4 billion, with the average cost per incident running $1,343. Few of us can afford that big a bite out of our budges without it causing us some serious problems.

This doesn’t include all the lost time that malware and the protection from malware costs us. While some malware merely annoys us, sending us advertising we don’t want; other forms of malware can take control of our computers, giving out private information to others or allowing those others to use our computers for their nefarious purposes.

One insidious form of malware that is becoming more prevalent is ransomware. This form of malware infects computers, taking

control of the data contained in the hard drive. It then demands payment for a decryption key, so that the data can be accessed.

Ransomware may even look legitimate, especially some of the more sophisticated versions. No notice is given to the computer's owner until the data on the hard drive is encrypted, and then the program presents itself as an anti-virus or anti-malware program, which has discovered malware on the computer.

In this type of case, it is designed to look like the solution to the problem, rather than the problem itself.

Like all malware, ransomware needs the computer owner's involvement to get onto the computer. This either happens through opening a legitimate looking link on an e-mail, or through websites that are intended to look legitimate.

One such method is attaching the malware to a program download, so that when you download one program, it asks you if you want to download another "useful" program. Many people click on these, thinking that they are part of what they are trying to get.

So, What can You Do?

There are actually a number of things you can do to protect yourself and your computer from cybercrime. In many cases, there is a "social engineering" element in any cybercrime attack, where the criminals need to get you to do something which gives them access to your computer. If you can avoid those things, you can protect yourself from 99% of cyber-attacks.

Let me demonstrate the idea this way; you're walking through your workplace and find a flash drive on the floor. Being normally curious, you take it to your desk and plug it into

your computer to see what it contains. You might be doing this for the best of reasons, so that you can return it to the rightful owner.

But if it contains malware, the simple act of opening that flash drive with Windows Explorer can be enough to trigger the malware and infect your computer.

Granted, the chances of that exact scenario happening are slight. But that doesn't mean that they don't exist. A much more likely scenario is for you to open an e-mail attachment which contains malware.

That is one of the oldest and still most effective means of spreading malware, especially since criminals have become more sophisticated in making the websites they are downloading from look like legitimate websites.

One of the greatest tools to the cyber-criminal is social media. Through it, they can find a plethora of information about most people. That information can be used to break into bank accounts, charge things to individuals or create e-mails that cause the individual to give them access to even more information.

To protect yourself and your computer, care must be taken whenever you are online. The following steps may not stop all potential attacks, but they can stop most of them.

Social Media – Avoid posting personal information on social media. This information can give criminals keys to answering your "secret questions" used for verifying your identity on online accounts.

Friends – Be sure to only friend people on social media that you know personally. Remember, whatever you post to your friends is likely to be seen by their friends (people you probably don't know) as well.

E-mail – Don’t open e-mails that come from people you don’t know. If you do, don’t click on any links, unless you are sure what those links are and where they go.

Web Addresses – If you find it necessary to click on a link contained in an e-mail, such as to verify your e-mail for opening an account, be sure that the URL listed in the link is for the company that you think it is. Do this even if an e-mail and website look legitimate, as one thing that criminals can’t hide is the URL that they are asking you to connect to.

Parental Controls – Use parental controls on your computer to keep your children from being contacted by or from contacting online predators.

Monitor – Even with parental controls in place, monitor your childrens’ online activity. Some online predators disguise themselves as other children, in order to make contact with potential victims.

Downloads – Never download anything from a website that you are unsure of. There are a number of websites online which act as watchdogs for fraudulent software. So if you are unsure of a program, do a search for it online, before downloading it. If it is suspect, you should see articles stating that it is.

Firewall – Keep the firewall on your modem turned on at all times. Firewalls help keep hackers out of your computer. Also verify that the software firewall in your computer’s operating system (Windows or iOS) is turned on.

Anit-virus Software – Install and update a good anti-virus software package on your computer. There are even good free ones available.

Keep Up on Your Updates – Many of the updates that Microsoft produces for their Windows operating system are to block access to one sort of malware or another. Always be sure to install those updates as soon as possible. Better yet, have

the automatic update feature turned on, so that your computer does it on its own.

Careful About Downloads – Downloads are one of the top ways that criminals get malware onto your computer. Always know what you are downloading and that it has been checked for all known viruses.

Turn Your Computer Off – One of the best protections for your computer is to turn it off when not in use. Unfortunately, this is not popular, because of the wait time for your computer to load, when you turn it back on.

Be Careful Shopping – Online shopping is easy and convenient. But it requires giving your credit or debit card information to companies you don't know. One protection is to use a third-party payment platform, like PayPal.

Photos – It's amazing how much information can be gleaned about you from your personal photos. Be careful about what you upload to the internet, especially to social media. Once you upload a photo, it is there forever; you can't delete it.

Checking in – Posting where you are, or "checking in" at restaurants and other locations allows the world to know where you are. Criminals can use this information to send you a "free" offer, from a restaurant you have visited. They can also use it to find that you are not at home, so it is safe to break into your home.

What You Like – Just like photos, people can learn a lot about you by what you "like" on Facebook and other social media sites. This can be used by businesses, criminals and even the government to target you.

While this list is rather comprehensive, don't take it as a definitive list of everything you should do. The area of cyber-security is so broad, that it is impossible to cover it completely in one article. Rather, take this as a starting

point in developing your own defenses.

As you learn of other defensive measures that you can take, implement them and make sure that your family does so as well. All it takes is one careless family member to cause problems for the whole family.