



## ParentPapers: You Are The Target

*Last Updated: 03 June, 2007*

<http://www.secureparents.com>

Welcome to SecureParents, a free website dedicated to you, the busy parent. We are dedicated to helping you at no cost secure you and your family in today's information age. We understand the tremendous pressures and time limits that parents have. Our resources are designed by experts to be simple yet provide the critical information you need. ParentPapers are a series of papers designed to give you this information in less than 15 minutes.

### PAPER TOPIC:

In this paper we discuss how you and your home computers are the primary target for criminals around the world. We cover who is targeting you, how and why.

*This paper is copyright "SecureParents". You are free and encouraged to distribute this paper to whomever you like. The only limitation is this paper cannot be modified nor sold for commercial purposes. This paper is distributed under the Creative Commons license, Attribution-NonCommercial-NoDerivs 3.0 Unported. In no event will SecureParents be liable for any damages, including loss of data, lost profits, cost of cover, or other special, incidental, consequential, direct or indirect damages arising from this documentation or the use thereof, however caused and on any theory of liability. This limitation will apply even if SecureParents has been advised of the possibility of such damage. You acknowledge that this is a reasonable allocation of risk.*

**Introduction**

A common misconception among parents today is that they are not a target on the Internet, that most hackers or criminals go after large corporations, banks or businesses. Unfortunately, nothing could be farther from the truth. What most parents don't realize is that they and their families represent the number one target on the Internet today. We will cover who is targeting you, why they are targeting you and how.

**The Attacker**

Today's cyber attackers are interested in one thing, money. Years ago attackers (or hackers) had a variety of motives for breaking into systems. These could include the desire to test new tools, intellectual curiosity, or attempting to make a name for themselves. Today's attackers care about only one thing, cold hard cash. Their motive is the same as most other criminals, to make as much money as possible with the least amount of effort and the least amount of risk.

For thousands of years civilizations have dealt with crime, such as extortion, identity theft or fraud. Today these same crimes are happening but in cyber space. Organized crime has found the Internet to be one of the most profitable ways to commit crime but with much lower risk and effort. The criminal of today has simply taken computer technology and adapted it to their criminal needs. Even more dangerous is just how organized the threat has become. Its not your high-school drop out hanging out in his parent's basement, these attackers are highly paid professionals operating in organized groups working to make as much money as possible. It just so happens you represent one of the primary targets for that motive.

**The Target**

The typical home user and family represent the number one target because they (including you) represent the most profitable target. There are four reasons for this.

1. Its much easier for cyber criminals to break into your computer then it is for them to break into a bank. Think about it. Large corporations and banks spend millions of dollars a year protecting their systems, how much can you afford to spend?
2. Your information and your computer are worth a lot of money. Data such as your tax records, bank account login, or credit card numbers can easily be sold or exchanged on the Internet today. In addition, your computer is a source of revenue. Criminals can use your computer as a gateway to launch attacks against other computers, to send spam to millions of victims, host pornographic pictures or fake bank websites, or used to store stolen information (such as millions of stolen credit cards). Criminals can even make money renting your hacked computer out to other criminals. Its absolutely amazing all the different ways they can make money with either your information or your computer.
3. There is very little risk in breaking into a home computer. Most family computers have no logging, no way to capture how the system was broken into or the time nor skills to trace back an attack and identify the attacker involved. In addition, law enforcement will most likely not be able to help you track down the criminals involved. They are simply overwhelmed with much larger cases and do not have the resources to help home users.

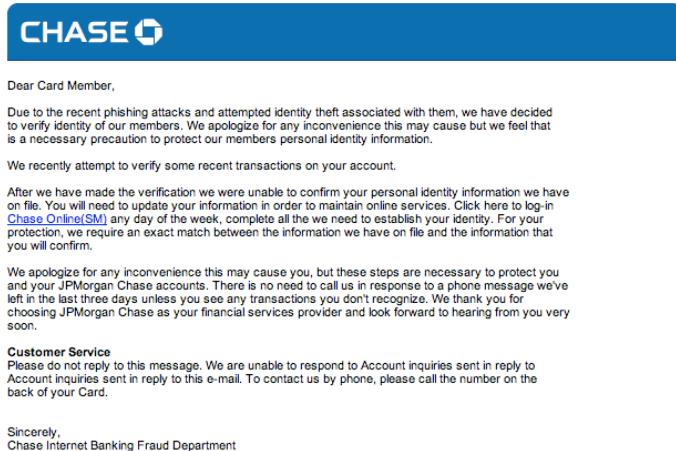
4. Finally home users represent the largest number of computers on the Internet today. There are literally millions of potential victims all over the world. These criminals may be able to make only \$100 from every computer they hack into. However, when you multiply that by the millions of potential victims connected to the Internet, you can understand just how profitable this business is.

Combined, these four things make you and your home computer a primary target. Its not you personally that is being attacked, but they are attacking you as one of the millions of home users around the world.

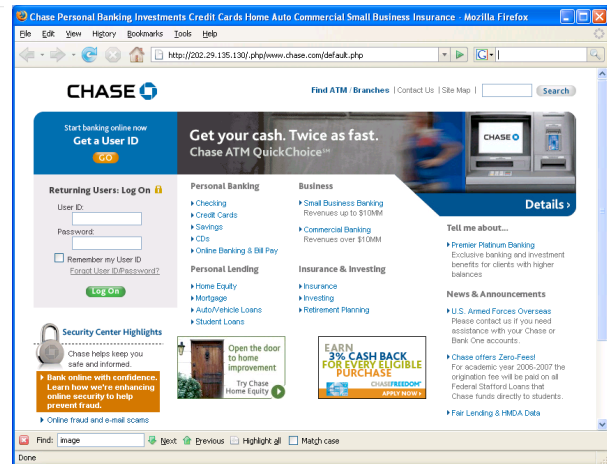
### **How They Attack**

Criminals use whatever tools and strategies that will make them the most money with the least effort. To do this on the Internet everything they do is highly automated with sophisticated tools. In the days before computers, if a criminal wanted to break into a house, he would search every house in the neighborhood to find the easiest one to break into. This takes a tremendous amount of time and risk as they could get caught by the police. The Internet has changed all of that. In today's computer age criminals can easily scan, probe and attack every computer on the Internet in less then 24 hours. Even more amazing is the fact they can do it from their own house while they are asleep with almost no chance of being caught. There is little effort on their part as automated programs installed on hacked computers around the world do the work for them.

In the past several years criminals have started changing their tactics. They are still going after home users, its how they do it that is different. In the past cyber criminals would attack computers over the network. They would probe, scan and attack vulnerable systems over the Internet using network based attacks. However, computers now a days are becoming more secure, with firewalls, automatic patch updates and secure configurations by default. These means they are harder to break into, taking more time and effort. Criminals are very creative and adapt quickly. Now, instead of trying to hack into your computer and steal your passwords or hack into your computer and install malicious programs, now a days they simply ask you to do the work for them. Its called social engineering, it means they are attempting to fool or trick you, often by pretending to be something you trust. See Figures 1 and 2 for an example of a common social engineering attack.



**Figure 2:** In this email we see what appears to be an email from Chase bank, asking us to click on the link and update our account information. In reality, this is a social engineering attack. This is not an email from Chase bank, but instead an email from criminals pretending to be something we trust.



**Figure 1:** If you click on the link, you are taken to a website that appears to be Chase bank. Actually, this is a bogus website setup by criminals. This website is designed to steal your bank login and password.

Email is becoming one of the most common means for criminals to target people like you. Email is fast, simple and can be sent to millions of people around the world. Everyone uses email meaning anyone can be a victim. In addition its extremely cheap for criminals to automate and difficult to track the criminal down. The example above is called a Phishing attack, in this case criminals are attempting to steal your banking information by fooling you into going to a bogus website. Other common examples would be having the email include a malicious attachment (called malware) that you install by clicking on it, or by directing you to a malicious website that can hack into your browser. For more information on such threats and how to protect against them, refer to the ParentPaper: [Ten Steps to Securing Your Home Computers](#).

### Risk

Unfortunately, don't expect this problem to go away. Because there is so little risk involved cyber criminals will continue their attacks. Cyber criminals and the Internet are a global problem. There are a tremendous number of technical, economic, and political issues for law enforcement to overcome before they can track down and prosecute these individuals. Until there are global laws and law-enforcement has the resources they need to identify and prosecute cyber criminals the problem will not go away. In some ways its similar to the wild, wild west of the United States in the early 1800's. The best you can do is to protect you and your family from this threat.

**Protecting Yourself**

Now that you understand who is targeting, how and why its key that you protect yourself. Fortunately for you we have documented how to do that in our ParentPaper: [Ten Steps to Securing Your Home Computers](#). In addition, our website has extensive number of resources, including links to other websites with more information on a variety of topics to help protect you.

**Summary**

You and your family represent the primary target for many of today's cyber criminals. You may not realize it, but both your information and your computer has tremendous value. Criminals use highly automated and sophisticated tools to attack their victims around the world. Often these tools depend on social engineering, tricking you into doing something for them. Keep in mind, its not you they are personally attacking, but the millions of home owners around the world like yourself. The first step to protecting you and your family against these threats is understanding that you are the target.

**Websites**

In this paper we mentioned several important websites. Here you can find them all listed.

ParentPapers:

Ten Steps to Securing Your Home Computers [www.secureparents.com/papers.shtml](http://www.secureparents.com/papers.shtml)

**About Us**

Concerned about protecting your online finances and your credit rating? Wondering who is collecting information on your children? Confused on how to best secure your computers at home? SecureParents is designed for you - the busy, working parent. It's your one stop for all the steps you need to take to secure yourself and your family in today's rapidly changing information age. The website is free, supported by and for parents. If you have any comments or suggestions about this paper, our website, or you have a story you would like to share with us we would love to hear from you! Please send all feedback or questions to [info@secureparents.com](mailto:info@secureparents.com).