

# Personal Computer Users Could Be Weakest Link In Fight Against Terrorism.

**Robert Ing**, D.Sc., D.Lit., F.A.P.Sc.

Full Article Available at [www.drroberting.com](http://www.drroberting.com)  
Copyright © 2003, 2004, 2005 Dr. Robert Ing, Toronto, Canada

A terrorist has two prime objectives; to obtain information and to disable a target at any cost. A personal computer user could unknowingly assist a terrorist in accomplishing these objectives but it doesn't have to be this way.

## Information

Approximately 70% of North American personal computer users conduct personal financial transactions on their machines. These transactions range from checking and maintaining personal bank accounts, investment portfolio maintenance and online purchases to electronic bill payments and income tax filing. Additionally, as much as 85% of users use their machines for managing their personal financial data through various accounting and database software. On most personal computers a plethora of personal notes letters, diaries and address books may also be found. To a terrorist, this information would be quite useful in stealing the identity of the computer owner in order to obtain false identification for the purpose of infiltrating targeted companies, government agencies and borders.

Another information concern is that 90% of personal home computer owners use their machines for work related activities. This could mean that sensitive or at the very least restricted data concerning a public or private entity could be found on a home computer. This information could be anything from an internal memo regarding a financial transaction or executive itinerary to the floor plans of a building or a document outlining technical specifications. All very useful for a terrorist seeking a new target of interest.

## Disable

If the terrorist already has all the information required, the next order of business is to disrupt, disable or destroy the target at any cost. In order to do this, the terrorist will seek out unknowing accomplices. The unknowing accomplice could be a home personal computer with the ability to connect to the Internet. In the case of launching a terrorist attack on a computer network; the network targeted could be anything from a financial network, major corporate or government network to a public utility computer system used to control telephone service or an access card/alarm system computer that may need to be disabled prior to a physical criminal act on a targeted premises.

## How is this Done?

Whether it is the use of a personal computer or the information on one a terrorist needs, all that is required is that the perpetrator place a small hidden piece of software on the machine to infect it. The method used to infect a personal computer can range from sending an e-mail, electronic greeting card or file to the user, to having the infection program lie in wait on a web page or hidden in an otherwise legitimate software program. Just because a personal computer is never connected to the Internet does not make it immune, as often the owners of these computers feel a false sense of security making them all the more vulnerable. In cases such as these, the infection occurs through external media such as shared diskettes, previously infected software and in some cases even through audio CDs played on the computer. Once infected, a non-Internet connected computer will become a carrier of the infected program and will infect other computers in the manner it was infected.

When the infection program finds itself on an Internet or network connected computer it will attempt to infect other computers that are online. However, more importantly it will also attempt to do one of two things; harvest information from its infected host, or permit the remote control of the infected host by the perpetrator.

## **Information Harvest**

An infection program may be specially programmed to search for specific files that contain certain keywords in their title or content, such as "personal", "banking", "credit", "password" or any other words the perpetrator may be interested in. Other infection programs may be less selective and just record any information that is typed on the keyboard, displayed on the screen or any file that is opened.

Once the information harvesting program has obtained a specific amount of data or at a predetermined time, it will attempt to secretly e-mail this information back to the perpetrator. This is done in one of two ways; the program will either wait for the unsuspecting computer user to go online and then hide the transmission of its data with other incoming/outgoing e-mails and files or if the program detects that the computer is connected to a dedicated "always on" Internet or network connection, the harvested data may be sent at anytime.

In the case where the infected computer has an "always on" Internet or network connection but is switched off when not in use, the infection program may have the capability to switch on the computer, send its harvested data and then switch the computer off.

For the majority of data harvesting programs, the harvesting seldom stops with the first harvest and tends to continue until the infection program is neutralized or the perpetrator moves on.

## **Remote Control**

Another infection program will allow the perpetrator to literally take control of a single or large numbers of personal computers. This type of program will allow the perpetrator to switch the computer on and off, send and receive e-mails and logon to websites using the victim's account, view all of the information contained on the computer, switch on any cameras or microphones attached to the computer in order to monitor the victim, change settings on the computer and launch any program on the machine.

Once a personal computer is under the control of the perpetrator it may be used in conjunction with as many as 1,000 or more infected machines to launch an attack on a major corporate, public safety or public utility computer network. In order to do this, the perpetrator will instruct all infected personal computers to begin their attack on the target network at a specific time of day. The infected personal computers will simultaneously make multiple attempts to connect to the target network, send large amounts of useless data or send multiple e-mail messages to specific internal e-mail accounts. The target network is overwhelmed by the amount of information received and therefore shuts down or locks up. As a result, the target network could be disabled for anywhere from a few hours to several days. Attacks of this type, depending on their methodology are known as DDOS, DVOS and mail bombing attacks.

Depending on the type of infection program; these are commonly known as viruses, trojans, (trojan horses), malware (malicious software) and backstops (instructive code).

## **Don't Let A Terrorist Have Access To Your Computer.**

Personal computer owners can take these steps to ensure their own privacy, security and to reduce the risk potential of their computer being used by a terrorist or other computer criminal.

1. Install Virus detection and firewall software on your computer and make sure you follow the software manufacturers' recommendations to keep it up to date. Need help? Visit [www.drroberting.com](http://www.drroberting.com) and check out the downloads section.
2. Do not use computer passwords that are easy to guess. Examples of bad passwords are default passwords, your name, telephone number, birthday, family or pet names, mother's maiden name, and passwords that are less than 8 characters in length. Do use passwords that consist of letters and numbers.
3. Never open or download an e-mail attachment, click on a link in an e-mail or go to a webpage address listed in an e-mail from someone you do not know. If the attachment is from someone you do know, but has the file extensions .pif, .exe, .com, .vbs, .vbe, .dll, .ini, .bat, .bin, .dot, .reg, .js, .scr or .xlm do not download it but contact them first to see if they really sent you this file. Some infection programs will disguise themselves by using a familiar e-mail address to get you to lower your vigilance.

4. Never give personal information out on the Internet and this includes the information you reveal on your personal webpage. Personal webpages should never provide home addresses, telephone numbers, specific employer or personal details such as exact date of birth. Be selective about the information you divulge.

**About the Author**

Dr. Robert Ing is a digital forensics and electronic counter-intelligence specialist. He may be reached at 416-563-6958, or via e-mail at [Ring549@aol.com](mailto:Ring549@aol.com), [www.drroberting.com](http://www.drroberting.com)