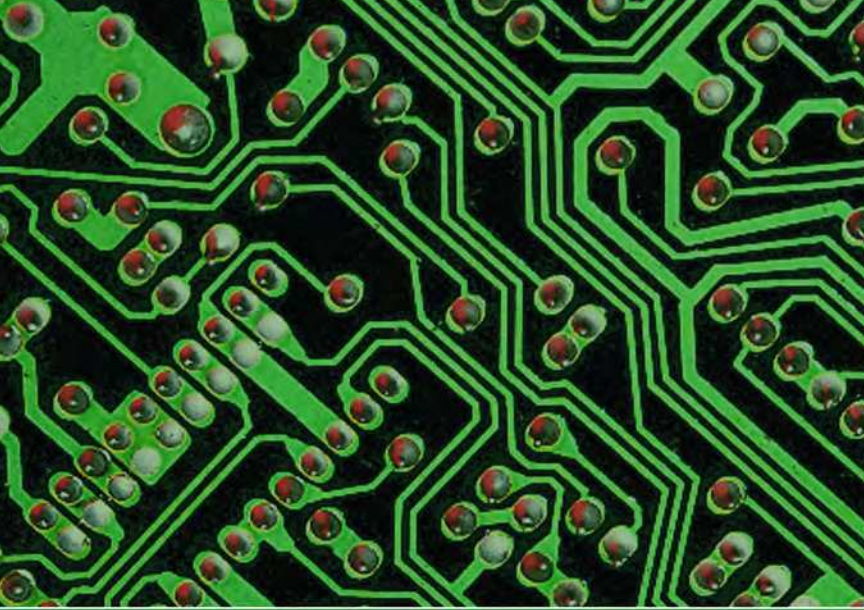


Best Practices

For Seizing Electronic Evidence

v. 3

A Pocket Guide for First Responders

U.S. Department of Homeland Security

United States Secret Service

BEST PRACTICES FOR SEIZING ELECTRONIC EVIDENCE

This third edition of the *Best Practices for Seizing Electronic Evidence* was updated as a project of the United States Secret Service and participating law enforcement agencies. A working group of various law enforcement agencies was convened to identify common issues encountered in today's electronic crime scenes. Representatives from the following agencies designed and developed this manual:

Alabama District Attorney's Association - Office of Prosecution Services
Los Angeles Police Department
Los Angeles County Sheriff's Department
Medford Police Department, Massachusetts
Presque Isle Police Department, Maine
Rockland County Sheriff's Department, New York
Ventura County District Attorney's Office, California
United States Secret Service

For additional copies, please contact the local office of the United States Secret Service.

The committee wishes to thank those departments and agencies who provided their personnel and resources in support of the publication of this guide. This guide has also been endorsed by the International Association of Chiefs of Police.

OFFICER SAFETY

The safety of the officer is paramount in the investigation of any crime. Today, virtually every crime has an electronic component in terms of computers and electronic technology being used to facilitate the crime. Computers used in crimes may contain a host of evidence related to the crime being investigated, whether it is a conventional crime or a terrorist act. In light of this, law enforcement officers and investigators should not become complacent with individuals or their environment simply because the crime may involve a computer.

During the investigation of electronic crimes or the seizure of computers and electronic items, be aware that as in any other crime, unexpected changes to a subject's involvement in a case may occur resulting in unexpected individual and environmental threats to an officer's safety.

Utilizing proper procedures and tactics will ensure your personal safety as well as the safety of others at the electronic crime scene.

GOLDEN RULES

There are general principles to follow when responding to any crime scene in which computers and electronic technology may be involved. Several of those principles are as follows:

Officer safety - secure the scene and make it safe.

If you reasonably believe that the computer is involved in the crime you are investigating, take immediate steps to preserve the evidence.

Do you have a legal basis to seize this computer (plain view, search warrant, consent, etc.)?

Do not access any computer files. If the computer is off, leave it off. If it is on, do not start searching through the computer.

If the computer is on, go to the appropriate sections in this guide on how to properly shut down the computer and prepare it for transportation as evidence.

If you reasonably believe that the computer is destroying evidence, immediately shut down the computer by pulling the power cord from the back of the computer.

If a camera is available, and the computer is on, take pictures of the computer screen. If the computer is off, take pictures of the computer, the location of the computer and any electronic media attached.

Do special legal considerations apply (doctor, attorney, clergy, psychiatrist, newspapers, publishers, etc)?

GOLDEN RULES

EVIDENCE PRESERVATION

Stand-Alone Home Personal Computer

For proper evidence preservation, follow these procedures in order.

- **If networked (attached to router and modem), see instructions on next page.**
- Do not use computer or attempt to search for evidence.
- Photograph computer front and back as well as cords and connected devices, as found. Photograph surrounding area prior to moving any evidence.
- If computer is "off", do not turn "on".
- If computer is "on" and something is displayed on the monitor, photograph the screen.
- If computer is "on" and the screen is blank, move mouse or press space bar (this will display the active image on the screen). After image appears, photograph the screen.

- Unplug power cord from back of tower.
- **If the laptop does not shutdown when the power cord is removed, locate and remove the battery pack. The battery is commonly placed on the bottom, and there is usually a button or switch that allows for the removal of the battery. Once the battery is removed, do not return it to or store it in the laptop. Removing the battery will prevent accidental start-up of the laptop.**

- Diagram and label cords to later identify connected devices.
- Disconnect all cords and devices from tower.
- Package components and transport / store components as fragile cargo.
- Seize additional storage media (see storage media section).
- Keep all media, including tower, away from magnets, radio transmitters and other potentially damaging elements.
- Collect instruction manuals, documentation and notes.
- Document all steps involved in the seizure of a computer and components.
- See section on important investigative questions.

Networked Home Personal Computer

For proper evidence preservation, follow these procedures in order.

- **Unplug power to router or modem.**
- Do not use computer or attempt to search for evidence.
- Photograph computer front and back as well as cords and connected devices, as found. Photograph surrounding area prior to moving any evidence.
- If computer is “off”, do not turn “on”.
- If computer is “on” and something is displayed on the monitor, photograph the screen.
- If computer is “on” and the screen is blank, move mouse or press space bar (this will display the active image on the screen). After image appears, photograph the screen.
- Unplug power cord from back of tower.
- Diagram and label cords to later identify connected devices.
- Disconnect all cords and devices from tower.
- Package components **(including router and modem)** and transport / store components as fragile cargo.
- Seize additional storage media (see storage media section).
- Keep all media, including tower, away from magnets, radio transmitters and other potentially damaging elements.
- Collect instruction manuals, documentation and notes.
- Document all steps involved in the seizure of a computer and components.
- See section on important investigative questions.

EVIDENCE PRESERVATION

EVIDENCE PRESERVATION

Network Server / Business Network

- Consult a computer specialist for further assistance
- Secure the scene and do not let anyone touch except personnel trained to handle network systems.

- **Pulling the plug could:**
  - **Severely damage the system**
  - **Disrupt legitimate business**
  - **Create officer and department liability**

Storage Media

Storage media is used to store data from electronic devices. These items may vary in memory quantity.

- Collect instruction manuals, documentation and notes.
- Document all steps involved in seizure of storage media.
- Keep away from magnets, radio transmitters and other potentially damaging devices.

PDA, Cell Phone & Digital Camera

Personal digital assistants, cell phones and digital cameras may store data directly to internal memory or may contain removable media. The following section details the proper seizure and preservation of these devices and associated removable media.

- If the device is “off”, do not turn “on”.
- With PDAs or cell phones, if device is on, leave on. Powering down device could enable password, thus preventing access to evidence.
- Photograph device and screen display (if available).
- Label and collect **all cables (to include power supply)** and transport with device.
- **Keep device charged.**
- **If device cannot be kept charged, analysis by a specialist must be completed prior to battery discharge or data may be lost.**
- Seize additional storage media (memory sticks, compact flash, etc).
- Document all steps involved in seizure of device and components.

PURPOSE

In today's society, people utilize various electronic media and computers in numerous aspects of their lives. Criminals also use a host of electronic media and computers in facilitation of their unlawful activities. Modern and current technology permits suspects to commit crimes internationally and remotely, obtain intelligence and conduct counter-intelligence with near anonymity. Instant communication and electronic mail provides a venue for communication between suspects as well as victims.

As such, computers and other electronic media can be used to commit crimes, store evidence of crimes and provide information on suspects and victims.

This field guide is designed to assist the patrol officer, detective and investigator in recognizing how computers and electronic devices may be used as an instrument of a crime or as a storage device for evidence in a host of federal and state crimes. It will also assist these individuals in properly securing evidence and transporting it for examination at a later time by a digital evidence forensic examiner.

We recommend that the patrol officer, detective and investigator consult and seek assistance from their agency's resources or other agencies that seize electronic media. This may include your local District Attorney, State Prosecutor or Assistant United States Attorney.

AUTHORITY FOR SEIZING EVIDENCE

This guide assumes that the patrol patrol officer, detective or investigator is legally present at a crime scene or other location and has the legal authority to seize the computer, hardware, software or electronic media.

If you have a reason to believe that you are not legally present at the location or the individual (suspect or victim) does not have the legal ability to grant consent then immediately contact the appropriate legal counsel in your jurisdiction.

PLAIN VIEW

The plain view exception to the warrant requirement only gives the legal authority to **SEIZE** a computer, hardware, software and electronic media, but does **NOT** give the legal authority to conduct a **SEARCH** of this same listed electronic media.

CONSENT

When obtaining consent, be certain that your document has language specific to both the seizure and the future forensic examination of the computer hardware, software, electronic media and data by a trained computer forensic examiner or analyst.

If your department or agency has a consent form relevant to computer or electronic media and its analysis by a computer forensic examiner, it should be used. If you do not have a form and are drafting a consent form, consult with your District Attorney, State Prosecutor or Assistant United States Attorney for advice regarding proper language and documentation.

SEARCH WARRANT

Search warrants allow for the search and seizure of electronic evidence as predefined under the warrant. This method is the most preferred and is consistently met with the least resistance both at the scene and in a court of law.

Search warrants for electronic storage devices typically focus on two primary sources of information:

Electronic Storage Device Search Warrant

- Search and seizure of hardware, software, documentation, user notes and storage media.

- Examination / search and seizure of data.

Service Provider Search Warrants
- Service records, billing records, subscriber information, etc.
- Obtain identification information for further investigative purpose.

Special Issues

Role of the computer
- The search warrant should state the computer's role in the crime and why it will contain evidence.

Nexus
- Establish why you expect to find electronic evidence at the search location.

Specify evidence sought
- Specifically describe the evidence you have probable cause to search for and any evidence of ownership of the computer.

Boiler plate language
- Adapt all search language to the specific facts of your case. Avoid using boiler plate language.

Non-Disclosure
- May be necessary to protect the integrity of the investigation, to protect informants or to prevent the disclosure of trade secrets / intellectual property.

Special Master
- Special legal considerations involving doctors, attorneys, spouses, publishers, clergy, etc.

The following is a general reference guideline for consent forms pertaining to computers and electronic media. Consult your District Attorney or Assistant U.S. Attorney regarding consent language applicable to your jurisdiction.

CONSENT TO SEARCH ELECTRONIC MEDIA

I, _____, hereby authorize _____, who has identified himself / herself as a law enforcement officer, and any other person(s), including but not limited to a computer forensic examiner, he / she may designate to assist him / her, to remove, take possession of and / or conduct a complete search of the following: computer systems, electronic data storage devices, computer data storage diskettes, CD-ROMs, or any other electronic equipment capable of storing, retrieving, processing and / or accessing data.

The aforementioned equipment will be subject to data duplication / imaging and a forensic analysis for any data pertinent to the incident / criminal investigation.

I give this consent to search freely and voluntarily without fear, threat, coercion or promises of any kind and with full knowledge of my constitutional right to refuse to give my consent for the removal and / or search of the aforementioned equipment / data, which I hereby waive. I am also aware that if I wish to exercise this right of refusal at any time during the seizure and or search of the equipment / data, it will be respected.

This consent to search is given by me this _____ day of, _____

20_____, at _____ am / pm.

Location items taken from: _____

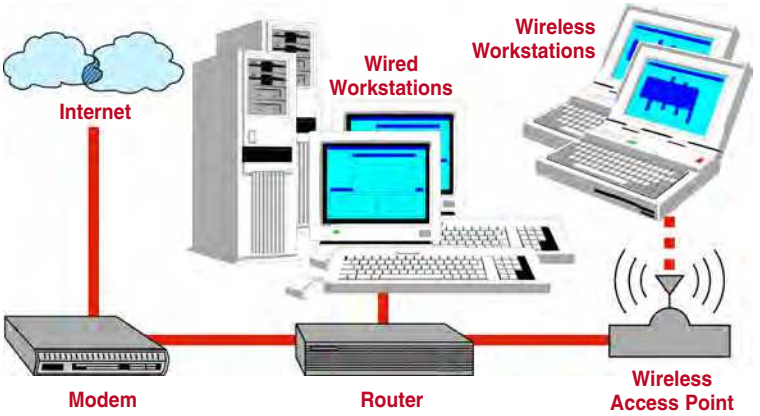
Consenter Signature: _____

Witness Signature: _____

Witness Signature: _____

HOME NETWORKING ELEMENTS

Home Networking Basic Elements



As seen in this picture, a home network is often comprised of a modem, router and desktop or laptop computers.

The typical purpose of a home network is to allow multiple computers to share a single internet connection, such as DSL, cable or dial-up. A home network also permits multiple users to share information with other computers on the network.

When confronting a home network, you should disable the network's connection to the internet as soon as practical. This is accomplished by disconnecting the power source from the modem and / or router.

In many instances home networks are connected via wireless routers or access points, which can be easily hidden.

Increasingly, many home networks also serve as small offices or businesses. When confronting these types of home networks, you should contact a computer specialist and have him or her present or readily available to provide assistance with seizing the computer and digital evidence.

The following is a list of crimes which may involve the use of a computer or other electronic media. Listed below are the crimes and potential evidence which may be recovered from various types of electronic evidence.

Computer Fraud Investigations:

- Account data from online auctions
- Accounting software and files
- Address books
- Calendar
- Chat Logs
- Customer information
- Credit card data
- Databases
- Digital camera software
- E-mail, notes and letters
- Financial and asset records

Child Abuse and Pornography Investigations:

- Chat logs
- Digital camera software
- E-mails, notes and letters
- Games
- Graphic editing and viewing software
- Images
- Internet activity logs
- Movie files
- User created directory and file names which classify images

Network Intrusion Investigations:

- Address books
- Configuration files
- E-mails, notes and letters
- Executable programs
- Internet activity logs
- Internet protocol address & usernames
- Internet relay chat logs
- Source code
- Text files and documents with usernames and passwords

Homicide Investigations:

- Address books
- E-mails, notes and letters
- Financial asset records
- Internet activity logs
- Legal documents and wills
- Medical records
- Telephone records
- Diaries
- Maps
- Photos of victim / suspect
- Trophy photos

CRIMES AND DIGITAL EVIDENCE

Domestic Violence Investigations:

- Address books
- Diaries
- E-mails, notes and letters
- Financial asset records
- Telephone records

Financial Fraud and Counterfeiting Investigations:

- Address books
- Calendar
- Currency images
- Check and money order images
- Customer information
- Databases
- E-mails, notes and letters
- False identification
- Financial asset records
- Images of signatures
- Internet activity logs
- On-line banking software
- Counterfeit currency images
- Bank logs
- Credit card numbers

E-Mail Threats, Harassment and Stalking Investigations:

- Address books
- Diaries
- E-mails, notes and letters
- Financial asset records
- Images
- Internet activity logs
- Legal documents
- Telephone records
- Victim background research
- Maps to victim locations

Narcotics Investigations:

- Address books
- Calendar
- Databases
- Drug recipes
- E-mails, notes and letters
- False ID
- Financial asset records
- Internet activity logs
- Prescription form images

Software Piracy Investigations:

- Chat logs
- E-mails, notes and letters
- Image files of software certificates
- Internet activity logs
- Software serial numbers
- Software cracking utilities
- User created directories and file names which classify copyrighted software

Telecommunication Fraud Investigations:

- Cloning software
- Customer database records
- Electronic serial numbers
- Mobile identification numbers
- E-mails, notes and letters
- Financial asset records
- Internet activity logs

Identity Theft Investigations:

- Hardware and Software Tools
  - Backdrops
  - Credit card reader / writer
  - Digital camera software
  - Scanner software
- Identification Templates
  - Birth certificates
  - Check cashing cards
  - Digital photo images
  - Driver's licenses
  - Electronic signatures
  - Counterfeit vehicle registrations
  - Counterfeit insurance documents
  - Social security cards
- Internet Activity Related to ID Theft:
  - E-mail and newsgroup postings
  - Deleted documents
  - On-line orders
  - On-line trading information
  - Internet activity logs
- Negotiable Instruments
  - Business checks
  - Cashier's checks
  - Credit card numbers
  - Counterfeit court documents
  - Counterfeit gift certificates
  - Counterfeit loan documents
  - Counterfeit sales receipts
  - Money orders
  - Personal checks

INVESTIGATIVE QUESTIONS

PURPOSE: This section is to provide assistance to the patrol officer, detective or investigator in identifying particular types of electronic crimes as well as providing general questions which should be asked during the initial phases of the investigation.

In conjunction with these investigative questions, the following information should be provided / documented to assist in the forensic examination of the electronic media:

- Case Summary - investigative reports, witness statements
- Internet Protocol (IP) Addresses - if available
- Key Word List - names, locations, identities
- Nicknames - all nicknames used by victim or suspect
- Passwords - all passwords used by victim or suspect
- Points of Contact - name of investigator making request
- Supporting Documents - consent form, search warrant
- Type of Crime - provide specific information

General Investigative Questions that may be asked regarding a crime involving computers and electronic evidence are as follows:

- When and where was the computer obtained? Was it new or used?
- Who has access to the computer hardware and software?
- Where is the computer's electronic media (compact disks, floppy disks, thumb drives, etc) stored?
- Whose fingerprints might be found on the electronic media?
- If other people have access to the computer, hardware or software can they access everything on the computer or only certain files, folders or programs?
- How many people use the computer? Who are they?
- What is the level of computer experience of each computer user?
- What times of the day do the individual users have access to the computer?
- What are the user names on the computers?
- What programs are used by each computer user?
- Does the computer require a user name and password? What are they?
- Is there any software that requires a username or password?
- How does the computer have access to the internet (DSL, Cable, Dial-Up, LAN, etc)?

- Does the victim or suspect have an e-mail account? Who is the service provider (Yahoo, AOL, Gmail, Hotmail, etc)?
- If e-mails are involved in the case, ask the victim and suspect for their e-mail addresses.
- Which e-mail client (program) does the suspect or victim use?
- Does the victim or suspect remotely access their computer (can they get into their computer when away from the office or home)?
- Do any of the users use on-line or remote storage?
- Have any programs been used to "clean" the computer?
- Does the computer contain encryption software or hard drive wiping utilities?
- Is the computer always on?

Electronic Crime Specific Questions target specific offenses and are as follows:

Identity Theft / Financial Crimes:

Victim Questions:

- Are you aware of any unusual activity on any of your accounts?
- What accounts have been compromised?
- Have you provided any personal information to any organization or individual?
- For what purpose was that information provided?
- Have you recently completed any credit applications or loan documents?
- Do you maintain any of your personal information on your computer?
- Have any bills or other financial statements not regularly arrived via mail?
- Have you checked your credit reports?

Suspect / Target Questions:

- Where is your computer software (CDs, floppy disks, etc)?
- Does the computer contain any software for making checks or other financial documents?
- Does the computer contain any software to manipulate photographs?
- Does the computer contain any scanned or manipulated identification?
- Was the computer used in doing any on-line purchases?

INVESTIGATIVE QUESTIONS

Internet Crimes Against Children (ICAC):

Victim Questions:

- Has the victim been on-line in any chat rooms?
- Does the victim use the internet, e-mail or chat from any other computers? If so, at what locations?
- Did the victim provide any information to anyone on line regarding their true name, age and location?
- What is the victim's e-mail address or on-line chat room name?
- Who is on the victim's "buddy list" in chat rooms?
- Does the victim save / archive chat room logs?
- What type of chat / e-mail client does the victim use?
- What were the specific sexual acts observed in the images or the electronic communications?
- Has the victim received any pictures or gifts from the suspect?

Suspect / Target Questions:

- Where are all of the suspect's computers?
- Does the suspect remotely store data (external hard drive, on-line storage, etc)?
- What is the suspect's on-line identity or chat room name?
- Has the suspect electronically communicated with any person?
- How does the suspect communicate with other persons? (chat, e-mails, etc.)
- Has the suspect viewed any child pornography using the computer? If so, how did the suspect obtain the child pornography?
- Did the suspect send child pornography to any other person in the suspect's state or in another state?
- Did the suspect realize that they were viewing images of children as opposed to computer generated images of children?

Intrusions / Hacking: (Network Questions)

Home Networks

- Can you physically trace all of the network cables back to their respective computers?
- Can each computer be associated to an individual user?
- Is the network connected to the internet?
- How is the network connected to the internet (DSL, Cable, Dial-up, etc)?
- Where is the DSL / cable modem located? Is it currently connected?
- Who is the internet service provider (ISP)?
- Is there more than one computer that can connect to the internet?
- Is there any wireless networking in place?

Business Networks

- Who first observed the illegal activity?
- Obtain the type of illegal activity and contact information for all witnesses.
- Identify the network administrator and obtain contact information. (The network administrator should not be contacted by the first responder.)
- Are any employees / former employees considered to be a suspect?
- Is there a printed diagram of the network available?
- Are computer logs being maintained?
- Can the computer logs be immediately secured for further investigation?
- Have any other law enforcement agencies been contacted?

Crimes Involving E-Mails

Victim Questions:

- Identify victim e-mail addresses and internet service provider (ISP) information.
- Identify all usernames and e-mail accounts used by the victim.
- Obtain any printed copies of e-mails that the victim has received. Do not turn on the computer to print e-mails.

Suspect / Target Questions:

- Identify suspect e-mail addresses and internet service provider (ISP) information.
- Identify all usernames and e-mail accounts used by the suspect.
- Obtain all passwords and associated software / usernames used by the suspect.

Instant Messaging / Internet Relay Chat (IRC) Crimes

Victim Questions:

- Ask if the victim had logging or archiving activated during chat sessions.
- Identify the victim's online screen name and e-mail addresses.
- Obtain copies of any material the victim has already printed.
- What type of software / chat client is used by the victim?

Suspect/Target Questions:

- Identify the suspect's online screen name and e-mail addresses.
- Obtain all passwords and associated software / usernames used by the suspect.

GALLERY

Computer Tower

Pager

Blackberry

Storage Media
(CDs, DVDs, Floppy Disks,
Zip Disks and Flash Cards)

Cell Phone

Desktop / Server Hard Drive

Laptop Hard Drive

Wireless Router

iPod

Thumb Drives

GALLERY

Glossary and Explanation of Terms

BACKUP: A copy of information off a computer.

BOOT: To load the first piece of software to start a computer.

BYTE: A unit of data generally consisting of 8 bits.

KILOBYTE (KB): A Kilobyte is 1024 bytes.
MEGABYTE (MB): A Megabyte is 1024 Kilobytes.
GIGABYTE (GB): A Gigabyte is 1024 Megabytes.

CD-R: Compact disk to which data can be written to but not erased.

CD-RW: Compact disk to which data can be written and erased.

CPU: Central processing unit. It is the "brain" that performs all arithmetic, logic and control functions.

DDOS: Distributed denial of service. An assault on a network that floods it with so many additional requests that regular traffic is slowed or completely interrupted.

DONGLE: A device that attaches to a computer to control access to a particular application. Dongles provide one of the most effective means of copyright protection.

DVD: Digital versatile disc or digital video disc. Similar in appearance to a compact disk, but can store larger amounts of data (typically a minimum of 4.7GB of data).

ENCRYPTION: The process of scrambling or encoding information in an effort to guarantee that only the intended recipient can read the information.

FIREWALL: A firewall allows or blocks traffic into and out of a private network or the user's computer. A firewall is a method for keeping computers secure from intruders.

HARD DISK: The hard disk is usually inside the PC. It stores information in the same way as floppy disks but can hold far more data. Popular types of hard disks are IDE, SCSI and SATA.

HARDWARE: The physical parts of a computer that can be picked up.

ISP: Internet service provider. A company that sells access to the Internet via telephone or cable line to your home or office.

MEMORY: The electronic holding place for instructions and data that a computer's microprocessor can reach quickly.

MODEM: A device that connects a computer to a data transmission line.

MONITOR: A device on which the computer displays information.

OPERATING SYSTEM: This software is usually loaded into the computer memory upon switching the machine on. It is a prerequisite for the operation of any other software.

PERSONAL ORGANIZER or PERSONAL DIGITAL ASSISTANT (PDA): These are pocket-sized machines usually containing phone and address lists, diaries and other information.

PIRATE SOFTWARE: Software that has been illegally copied.

RAM: Random access memory. The computer's short-term memory that is lost when the computer is turned off.

REMOVABLE MEDIA: Floppy disks, CDs, DVDs, cartridges and tapes that store data and can be easily removed.

REMOVABLE MEDIA CARDS: Small data storage media which are more commonly found in other digital devices such as cameras, PDAs and music players.

ROUTER: A network device that forwards packets from one network to another.

USB STORAGE DEVICES: Small storage devices accessed using a computer's USB ports. They store large volumes of data files. They are easily removed, transported and concealed. They are about the size of a car key or highlighter pen.

WARDRIVING: Driving around an area with a laptop and a wireless network adapter in order to locate unsecured wireless networks.

WIRELESS NETWORK CARD: An expansion card present in a computer that allows a cordless connection between that computer and other devices on a computer network. The card communicates by radio signals to other devices present on the network.

ZIP DRIVE / DISK: A 3.5-inch removable disk drive. The drive is bundled with software that can catalogue disks and lock files for security.

GLOSSARY

Online Identity Theft Guide

PREVENTION

- Never give out any of the following information to unknown sources:

Date / Place of Birth	**Social Security Number**
Credit Card Number	**Mother's Maiden Name**
Address	**Phone Number**

- Review credit reports at least once a year.
- Ensure secure online transactions by locating the closed lock icon at the bottom right side of your web browser before disclosing personal information.
- Unless absolutely necessary, do not store any financial information on a computer.
- Prior to discarding a computer, destroy all information contained on the hard drive. A wiping utility is necessary, as formatting will not safely destroy data.
- Use strong passwords and do not allow programs to save passwords.
- Use virus protection software and firewalls to prevent the loss of personal information from your computer or the introduction of malware.

RESPONSE

- Contact bank or credit card issuer to report fraud.
- Place a fraud alert with the following credit agencies:

Equifax - 800-525-6285
Experian - 888-397-3742
TransUnion - 800-680-7289

- File an identity theft complaint with your local police department and the Federal Trade Commission (FTC) at 877-382-4357.