# Addendum to 2012 RTBAV Student Handbook

**The following changes have been made to the 2012 Student Handbook. Please refer to the following changes when using the 2012 Student Handbook. These changes will make the handbook match up with the updated PowerPoint.**

- Physical Security (page 22) will now be before Home Security (page 9).
- Personal Alarms and Self-Defense Training will now be in the Physical Security section.
- The following will now be after Alarms in Home Security (page 18)

E. Security Cameras

Security cameras can add a layer of security to your home so you can monitor your house when you are gone or see who is at the front door without having to open it. It will also provide you with video footage of what happens in and around your property. What size or style is up to you- whether you decide on a 12-camera system that you can monitor remotely, or a single camera with one tape, they are a deterrent to potential criminals. And in the event that you are the victim of a home invasion, you will have footage to use as evidence that will help the police recover your stolen items.

If you get a more sophisticated system, you will have the ability to arm and disarm your alarms and view security camera feed remotely. You can also monitor what is going on inside your house as well as outside, if you leave your children or pets at home and would like to check in on them.

Like many safety measures, security cameras need to be maintained. If the camera is powered by batteries, you must make sure to check the batteries regularly. Also, a camera system may be vulnerable to disconnection by a tech-savvy burglar.

Getting a security camera but not activating it, or even getting a fake security camera, could also be a deterrent to criminals. They most likely won't know that it isn't real or active, and just seeing it might discourage them, making them think twice about breaking into your house!

- The following will now replace the Technological Security section:

VIII. TECHNOLOGICAL SECURITY

A. Phone Security

The telephone is an excellent source of information for everyone—including criminals. People are taken in by elaborate phone scams every day. If a person is fooled into giving out critical, personal information over the phone, they could be risking more than their money.

Criminals often use the telephone to target their victims. It is to your advantage to *never give information to strangers on the telephone*. Be especially careful when asked to participate in telephone surveys. Never give information to persons who state that they are from your bank or credit card company.

Some common phone scams to watch out for include:

- Caller says you've been "specially selected" for a certain offer, and they just need a few identifying details to make sure it's really you—full name, date of birth, and Social Security number. Just enough to steal your identity!

- Caller pressures you with an offer that you have to make up your mind about right away.

- Caller offers a free product but asks for your credit card information to pay for shipping and handling.

- Caller tells you a family member is in trouble (stuck abroad, in jail, etc.) and they need you to wire them money to help this person.

- A false name and phone number shows up on caller ID—sometimes a number you recognize or a company you've heard of—and the caller, posing as this false person or company that showed up on caller ID, requests personal information. This scam is called 'spoofing.'

- Caller, who claims to be a charity, asks for a donation and offers a generous gift. Ask them to point you to the website for more information—no charity will run a phone-only fundraiser!

- Caller says you have an outstanding ticket, fine, or warrant for your arrest. They might say they're from the DMV or courts, and tell you that you must pay a fine right now or risk jail time. Similar scams include callers saying you've incurred red-light camera fines or EZ pass missed tolls, or missed jury duty. Keep in mind debt collectors do not have the power to arrest anyone, so don't be intimidated. Ask for a name and number and call them back to make sure the call is legitimate.

- Caller says they're from the IRS. The scammer will say that you owe money or even are due a big refund, and they need bank information to process this payment. The IRS will NEVER ask for payment information over the phone and will always send taxpayers a written notification of any tax due via U.S. mail. If someone calls

claiming to be from the IRS requesting such information, hang up immediately and call the IRS at (800) 829-1040.

- Bank alerts—you get a voicemail saying your bankcard has been suspended and to please call this toll-free number to activate it. You'll have to enter all of your account details, contact information, and Social Security number to prove you are the cardholder. Don't call this number—go into the bank if you are worried your card has really been suspended or compromised.

- You receive a missed call even though you didn't hear the phone ring, or it only rang once. You call the number back and it puts you through to an international adult entertainment or chat in a non-U.S. location where you can quickly incur expensive charges. Even if it looks like a U.S. area code, it might be international (for example, 809 = Dominican Republic; 876 = Jamaica; 284 = British Virgin Islands). Look the number up online and see if there have been scams reported about it. Even if there haven't been, it's best not to call the number back—if it's really someone you know, they'll call you back!

Never give callers the answers to any questions that might give them information concerning your daily routine, bank accounts, credit cards, social security number, income level, etc. Requests for your name, address, bank account numbers and credit card numbers are especially suspect. Legitimate callers from your bank, credit card company or a credit reporting agency *should already know* this information. If you receive such calls, hang up at once, and then call your bank or credit card company using the phone number shown on your statements or bills. If a credit reporting agency or other type of company has allegedly called you, hang up the phone and return the call using the company number listed in your telephone book. You can also tell the caller that you do not give out any personal information over the phone, but will be glad to respond to a written request.

Be wary if you are asked whether you and your spouse both work—an affirmative answer will indicate to a thief that no one is home during the day.

Telemarketers

Salespersons or solicitors who call you on the phone are known as *telemarketers*. Many telemarketing calls that you receive will be frauds, or scams, that are intended to deprive you of your money without giving you anything of value in return.

Be very suspicious of any unknown caller who says that you must respond immediately to the solicitation, offers to pick up the money from your home, instructs you to send or wire money or claims to be a law enforcement officer who will help you in return for a fee.

Your best way to protect yourself from telemarketing fraud is to simply *hang up the phone*.

If you think that the call may be legitimate, but you don't want to purchase anything or make any contributions, just politely tell the caller:

- You are not interested.
- You don't want to waste their time by listening to a solicitation in which you are not interested.
- You would like the caller to remove your name from their calling list.

If the telemarketer persists in calling you, or if you suspect fraud and want to report it, contact the office of the attorney general in your state, your local consumers' protection office and your local Better Business Bureau. (You can obtain these phone numbers from your telephone book or directory assistance.)

There is a way now to stop most commercial telemarketing calls by registering all your phone numbers, home and cell, with the National Do Not Call Registry. You may register online at www.donotcall.gov. Consumers can add their telephone numbers to the registry at any time by calling (888) 382-1222 (TTY (866) 290-4236) but the call must be made from the telephone number you wish to register.

Understand that some calls are not covered. Once your number has been on the registry for 31 days, most telemarketing calls will stop. However, you still may get:

- Calls from—or on behalf of—political organizations, charities, and telephone surveyors.
- Calls from companies with whom you have an existing business relationship. A company may call you for 18 months after you make a purchase or three months after you submit an inquiry or application. However, if you request that the company place your number on its own do-not-call list, it must honor your request. You should keep a record of the date you make the request.
- Calls from companies you've given permission to call.

As of February 2008, telephone numbers placed on the National Do Not Call Registry will remain on it permanently.

Another way to reduce the amount of telemarketing calls and advertising mail you receive, is to contact the Direct Marketing Association and ask to have your name removed from their call or mail lists. Within months of your request, the volume of calls and/or mail you receive should be reduced. Your request will remain valid for five years; after that time you will have to re-register. Obtain more information from the Direct Marketing Association's website at www.the-dma.org.

Visit Know Fraud's Internet Web site at www.consumer.gov/knowfraud or write to them at Know Fraud, P.O. Box 45600, Washington, D.C. 20026. If you think that you have been the victim of fraud, you may call Know Fraud toll-free at (877) 987-3728.

Answering Machines

If you use an answering machine, do not announce your name and number as part of the message. This information could be used to locate your home.

Avoid revealing your exact whereabouts in a message. Never say that you're not at home now, or state when you expect to return. Never give callers the impression that your home is unoccupied.

A good example of a safe message on your answering machine is:

> *Hi! We're busy and can't take your call right now. Please leave your name and phone number at the beep, and we'll get back to you as soon as possible.*

Abusive Phone Calls

Abusive phone calls are a frequent occurrence. In these cases, callers use the phone for a variety of reasons. They may intend the call to be a simple prank. Or the call may be a more deliberate attempt to disturb or annoy you. More seriously, the call may be obscene, harassing and/or threatening. Calls of this nature may be illegal, punishable by criminal prosecution, and/or may subject the caller to civil liability.

Abusive calls generally fall into three categories:

- *Prank calls*: Usually made by children or teenagers. Callers' motivation is to trick, annoy or play a joke on you, not to frighten or scare you. These callers usually don't repeat the call.

- *Obscene calls*: Callers use improper language to get a reaction from you, whether it be words, tears, threats, anger or fear. Callers usually want to humiliate or intimidate you. In most cases, the calls aren't repeated. However, if the calls persist, you will need to take steps to solve the problem.

- *Harassing or threatening calls*: A clear pattern of repeated calls is usually established by the caller. Sometimes callers are motivated by anger, jealousy or revenge, and simply want to get even by harassing you. Or callers may actually be planning some type of physical harm to you. These types of calls account for more than 75 percent of abusive calls. Examples of these calls include: repeated hang-ups (with no words spoken), taunts or threats from ex-friends or ex-spouses, sexual threats, death threats and bomb threats.

The best advice on handling such calls is to *hang up immediately*. If the calls appear to warrant immediate action because of their seriousness, or continue to be used as a means of harassment, consult your telephone company and local law enforcement agency for assistance. Also, consider using an answering machine or voicemail to screen your calls.

Many optional telephone services are available to help you improve your phone security. A few of these services are described below.

Optional Phone Services

Many optional phone services that can increase your phone security are available from your telephone company. These services include: Caller ID, Anonymous Call Rejection, Call Block and Call Trace.

- *Caller ID*: Allows you to know who is calling before you answer the phone. A small display panel, located on the phone or on a separate box, will show the name and/or number of the caller.

- *Anonymous Call Rejection*: If callers dial a special code on their phones to block their names and/or numbers from being shown on your Caller ID display, they will be automatically greeted with a special announcement stating that you do not receive blocked calls.

- *Call Block*: Allows you to block phone numbers from which you do not wish to receive calls. Callers will be automatically greeted with a special announcement that you are not available.

- *Call Trace*: If you are having problems with obscene, harassing or threatening phone calls, you can activate the Call Trace feature. When activated, the last caller's phone number is recorded and stored by the telephone company. At your request, the caller's phone number will be sent by the telephone company to the appropriate law enforcement agency for investigation.

If you want additional information about these services, including use and cost, contact your local telephone company. Subscription and usage information may also be printed in the front of your telephone directory.

Using Emergency 911

When you dial 911 in an emergency situation, try to remain cool, calm and collected. Although the emergency situation places enormous stress on you, the 911 operator needs your help to obtain vital information.

It's not uncommon to forget things when you are in an emergency situation. Post your address, phone numbers and other information near the phone at home. You or a family member may need this information quickly.

If you are away from home or in your automobile, know exactly where you are before you call.

Speak clearly and concisely to the 911 operator. Don't yell, shout or speak so fast that your words are jumbled together—the operator will not be able to help you if you can't be understood.

State the nature of the emergency (a prowler, a break-in, an injury or illness, a fire, etc.). Give your name, address and phone number. Listen carefully to the operator and follow the operator's instructions carefully and completely. The operator is trained to ask certain questions—cooperate and calmly supply the requested information. If possible, have someone stay on the phone with the 911 operator until help arrives.

Don't tie up 911 with non-emergency calls. If you need to call the police, fire department or medical facility with a non-emergency question or complaint, *use their non-emergency number* listed in the phone book. Don't prevent another person from getting desperately needed help because you tied up the 911 operator with a non-emergency calls!

Cellular Phones

Cell phones have become a normal part of everyday life. If your car breaks down or you are seriously harassed by another driver, you can use it to phone for help. It is also an excellent security device in your home.

Remember the section on home security earlier in this book? It was explained that if you have wired or cordless phones in your home, these phones can be disabled by cutting the phone line or by taking an extension phone off the hook. A cell phone cannot be disabled by these tactics because it transmits and receives signals wirelessly; it does not rely upon standard phone lines.

Any charged cell phone can be used to call 911. You do not need an active cell phone service account to reach 911. Speak clearly and give the operator the address where you need assistance. Unlike a land line, your location will not automatically appear for the emergency operator.

Always keep your cell phone properly charged. You may want to keep an extra charged battery handy. Invest in a car adapter for your phone; this device will allow your phone to draw energy from your car's battery and can be used to recharge a low battery.

Know your cell phone's coverage limitations so you don't unexpectedly lose service when you go out of range. Verify the phone's range of operation. Even with the increased quantity of transmitters, some cell phone coverage is inconsistent. Ensure the phone you purchase will work in all necessary locations (i.e., home, office, frequently traveled routes and destinations).

Be aware that cellular and cordless phone conversations may not be private. Certain types of radio scanners can intercept cellular and cordless phone conversations. Although this type of equipment is no longer available on the market due to a new federal law, many units capable of interception were manufactured and sold before the law took effect. It is very easy to make illegal modifications to current scanning equipment that will enable the scanners to receive cellular or cordless calls.

Always set up the lock screen on your cell phone so you have to enter a password or draw a pattern to use the phone. If your phone is lost or stolen, this will keep people from picking up your phone and accessing personal information or racking up expensive calls.

Remember that your cell phone, like many regular and cordless phones, can be programmed to quickly call certain numbers. Be sure to program emergency numbers into your cell phone. Law enforcement agencies and emergency medical personnel now suggest putting an ICE (In Case of Emergency) phone number in your cell phone contact list. This person is someone you would want contacted in an emergency. The ICE entry should be used in addition to carrying a standard form of identification.

Many cell phones have Internet access, which, while convenient, is another way people can be vulnerable. Use the same precautions that you would if you were accessing the Internet through a computer. Always use websites that have secure connections and never connect to an open Wi-Fi network (see Section C for more information on general Internet safety).

A cell phone camera can be a valuable resource. Before a day out with your children, take a picture of them. That way, should you get separated from them, you have an updated photo to show the police and will know exactly what they are wearing for a better description. Also be careful of what pictures you keep on your cell phone. If your phone falls into the wrong hands,

you don't want that person to figure out personal information from you by looking at your pictures, or making public or threatening you with compromising pictures of yourself.

Be sure to deactivate your GPS when taking pictures with your cell phone. If you post a picture on social media while the GPS is still activated, they can get the location of where the photo was taken, your whereabouts, and whether or not your house is unoccupied. Additionally, programs called location services (either downloadable apps or services offered by cell phone carriers) let people post their current location on social media. If location services is turned on, you might be unwittingly posting your current location with each new status update or photo posted. By posting your location, people can not only see where you are, but also see that you're not at home—and that your house may be unoccupied! Turn off location services in your phone's settings to ensure you don't share your location with potential criminals.

Text Scams

Criminals are now also using text messaging to try to gain personal information, as well. This is called SMiSHing, a term derived from SMS technology used for cell phone text messages.

Here are some examples of text message scams:

- You receive a text message that states the user's bank card has been deactivated and you are directed to call a telephone number and enter your bank account and Personal Identification Number (PIN).

- You receive a text from a number you don't recognize, but looks like the texter knows you. For example, "Hey I got a new phone number, save my number!" or "Hi it's John, long time no talk!" When you text them back, it might go to a premium number that charges very high rates and leave you with a high phone bill. In addition, if you do reply, it could put you on a spam list and you could start receiving a lot of similar messages and calls from spammers.

- You receive an urgent text with a hyperlink that directs you to a website when you click on it. For example, "Urgent! There has been suspicious activity on your credit card. Click here for help!" When you visit the link, you've unwittingly given the criminals access to your device, and they can attach dangerous spyware and/or viruses that gives them control and instant access to your personal data.

B. Identity (Personal Information) Theft

Criminals use a variety of methods to obtain your personal information. They may pose as your employer or as a loan officer in order to obtain your credit report. Some may go through your trash at night in order to discover credit card numbers, bank account numbers or to retrieve

unused credit card offers that they can submit in your name using their own address. Yet others may simply take mail straight out of your mailbox.

Mail is especially vulnerable. Many people have mailboxes that allow easy access for mail distribution and removal. Of course, few people consider that anyone but themselves would remove mail from their mailboxes. Think about the types of correspondence which arrives in your mailbox: credit card statements or offers, Social Security information, bank statements, blank checks, prescription drug information, motor vehicle information, etc. All of these would be useful to someone who wants to steal your identity. Buy a cheap shredder to keep by your trash can. Instead of throwing away all of those pre-approved offers or statements, shred them. Better yet, shred all of your mail—better safe than sorry!

Some criminals may look over your shoulder (or use binoculars from a distance) while you enter your PIN into an ATM. Make sure no one is watching and shield the keypad when entering your PIN.

Some easy steps that you can take to avoid these types of thefts include:

- Never discard your ATM slips at the machine or your credit card receipts at the store. They can be retrieved by criminals and the information on them can be used to access your bank accounts or make purchases using your credit cards. Take these slips home with you and properly dispose of them.

- Never reveal your credit card numbers unless you are confident that you are dealing with a reputable business.

- Consider obtaining a debit/check card from your bank. These cards can now be used at many stores and businesses, including grocery stores, department stores and gas stations. You are not required to sign anything or show any type of personal identification or information. This type of card is used by swiping it through a sensor box at the store and using the unit's keyboard to enter your PIN. The money that you owe the store is deducted by the bank directly from your bank account. This type of card is extremely secure and very convenient to use. The receipt that you receive from the store does not have your bank account number or PIN printed on it.

- To protect yourself and prevent having your confidential mail stolen, you could use a mail service or post office box; both would limit others' access to your mail. You could also consider installing a mail slot in your front door; inserted mail would then be safely within the confines of your home. You could also consider having some items, such as blank checks, mailed to a nearby bank branch. You could then pick them up at your convenience.

- Be careful disposing credit card offers that you receive in the mail. Don't just throw them in the trash. Tear them up in small pieces, shred them or burn them.

- When setting up your PIN, computer password, or other type of security code, don't use your birthday, your anniversary date, your phone number, your house number, your name, your initials, your spouse's name, your children's names or other similar numbers and names. Criminals can easily obtain these numbers and names through a variety of methods.

- Avoid using common computer passwords such as *user, newcomer, guest, visitor, login, password,* etc., or any password containing your first or last name, spouse's or children's names, date of birth, or other common information. Criminals know that the majority of people use these types of security codes because they are so easy to remember. Select security codes that are unlikely to be deciphered by a criminal.

If your identity is stolen, here are some things you should do:

- Contact one of the three national credit-reporting bureaus. Be consistent and file a fraud alert on your credit report.

- Close any accounts you feel have been compromised.

- File a report with local law enforcement where the theft took place.

C. Cyber fraud – Electronic Theft on the Internet

Electronic theft on the Internet does exist, and many people have become victims of this new type of criminal activity known as cyber fraud. According to research conducted by *PC Computing* magazine, cyber fraud recently *increased by 600 percent* from one year to the next. This is a phenomenal increase for just one year! Don't become an Internet casualty.

Some of the following tips will help you to become a safer Internet user:

- Implement security measures for all financial accounts by placing fraud alerts with the major credit bureaus if you believe they were targeted by a scam or other forms of fraud.

- Use strong passwords for all financial accounts and change them regularly. Create a password that is difficult to guess, at least six characters long, and contains a mix of letters and numbers.

- Shut down your computer when you are not there. At the very least, password-protect your computer and lock it when you are not using it. Do this by hitting CTRL + ALT + Delete

and then select "lock this computer." It's fast, it's easy, and you could be keeping criminals out!

- Clear your browser after each use to delete history files, caches, cookies, and temporary Internet files. If a criminal accesses your computer, they can use your Internet history and saved passwords and files to apprehend your personal information. Log out of websites after you are done with them, as closing the window does not necessarily log out of your account.

- Obtain and review your annual credit report for fraudulent activity.

- Take precautions to ensure operating systems are updated and security software is current.

- Don't give your password to anyone. With your screen name and password, criminals can run up charges with your Internet Service Provider (ISP), read email sent to you and send email to others from your account.

- Chat rooms give rise to special concerns. Often, people relax their guard when in chat rooms and give out personal information. If possible, avoid them altogether. However, if you must visit chat rooms, remember that the other room visitors are strangers to you. They may share (or pretend to share) a common interest, but they are strangers nonetheless. Many criminals cruise chat rooms looking for people to victimize.

- Invest in anti-virus software and upgrade it often. Consult your ISP or computer supply store for information.

- Consult your ISP to find out if they allow you to set filters to block unwanted email. Often, you can block email from specific people, block email with attachments, permit email only from specific people, etc.

Email Safety

A common scam to appear in the cyber world is "phishing," the act of sending an email to a user falsely claiming to be an established business or enterprise. The sender attempts to scam the user into surrendering private financial information that will be used for identity theft. The email sends you to a website where you are asked to update banking, credit card, social security, and/or personal information. The website is bogus but will appear very similar to a real website. A legitimate business or enterprise already has this information. Delete these email messages!

If you receive junk email, referred to as "spam" or offensive email, inform your ISP. Most ISPs want you to report this type of email to them. They often take action, such as canceling the

sender's account, against perpetrators. The United States Attorney's Office may elect to take legal action against perpetrators.

Just like in Section A of this chapter where we went over common phone scams, criminals will try to get your information through email scams as well

If you are unsure whether or not an email you received is safe, ask yourself the following questions:

- Do you know the sender?
- If you do know the sender, does it seem like something out of character for them to be sending? If it seems unusual, their email may have been hacked.
- Are there many spelling or grammar errors?
- If the email is offering something, is it something you requested? If you don't recall signing up with the company who is sending the email or the email is unsolicited, be suspicious.
- Is the email from a different country? If it's from Nigeria or Singapore and you don't know anyone there, chances are it's a scam.
- Is the email asking for money, saying you won a prize, or giving you a too-good-to-be-true offer? Never send financial info via email to someone you don't know or pay a shipping and handling fee for a prize you "won."

Be wary of these. Do not download attachments or click on hyperlinks contained within the message. Frequently, attachments contain viruses or *Trojan Horse* programs which can damage your computer or allow access to your account. Hyperlinks may take you to websites that prompt you to enter your screen name, password and other personal information. If you think it might be a legitimate email, call the sender and verify that they indeed sent it. Otherwise, just delete the email.

Online Shopping

One of the newest and safest ways to shop online is to use a virtual credit card. This type of card prevents the risk of personal information and credit card numbers from falling into the hands of thieves. The card is normally good for one or two months, and cannot be activated after it expires.

Using a virtual credit card online increases your security level, as your personal bank account is not affected. With identity theft and email scams rising at alarming rates, this is a great way to protect you and your family.

All the major credit card companies offer prepaid virtual credit cards. Do an Internet search or ask your local bank about virtual credit cards.

Be sure that you are dealing with a legitimate company. If you are uncertain about the company, ask that a printed brochure or catalog be sent to you. Never deal with a company that has only a post office box number and fails to provide a telephone number. If the price of an item seems suspiciously low, you should exercise extra caution.

If you want to pay by credit card, be sure that the company has set up what is known as a *secure connection* between you and its server. There are several indicators of secure connections. For example, if you are using Internet Explorer of Google Chrome as your web browser, the screen icon that looks like a padlock indicates a secure connection. If you are using Netscape's Navigator web browser, you will always see a *key icon* on your screen. If the key is not broken and the color is blue, the connection is secure. If the key is broken and is on a gray background, the connection is not secure. Another way to tell is a connection is secure is to look at the address. If it starts with https it is a secure connection; http is not a secure connection. Lastly, if the https is written in green font, the connection is secure.

If you decide to place an order, be suspicious if you are asked to supply personal information such as your Social Security number or your checking account number. The merchant only needs to know your name, address, credit card number and credit card expiration date.

If you place an order, be sure to keep a record of all information about the transaction. Be sure that you have the *Universal Resource Locator* (URL) for the site. An example of a URL is www.refuse.nra.org. Write down all order or confirmation numbers.

Check your credit card statement often to make sure no fraudulent charges have been made or that your credit card number has not been compromised.

Social Networking

If you think that social networking is just for teens, think again: as of January 2014, the Pew Research Center states that 73 percent of adults who use the Internet use sites such as Facebook, Twitter, and Instagram. As a rising number of the population uses these sites, so do criminals. Take the following safety precautions when using social media:

- Adjust website privacy settings; do not use the default settings. Some networking sites have provided useful options to assist in adjusting these settings to help protect your identity.

- Be selective of your friends. Once selected, your "friends" can access any information marked as "viewable by all friends."

- You can select those who have "limited" access to your profile. This is for those whom you do not wish to give full friend status to or with whom you feel uncomfortable sharing personal information.

- Be careful what you click on. Just because someone posts a link or video to their "wall" does not mean it is safe.

- Don't post pictures or statuses in real time. If you upload a picture of yourself at the beach or park, people can tell that your house is unoccupied. Also be sure to turn off GPS while posting on social media; criminals can use this information to figure out your exact location.

- Stop and think before you post!! It is easier to type something than it is to say it. Once you post something, even if you take it down, it is not really gone—what you put on the Internet stays on the Internet!

D. Cyberstalking or Cyberbullying–Stalking via the Internet

Computer users should be aware of cyberstalkers and cyberbullies on the Internet! With more and more individuals using computers, criminals are finding easy targets online. Cyberstalkers target and gain access to their victims through many channels, such as:

- Chat rooms
- Classified ads
- Message boards
- Discussion forums
- Online clubs
- Emails

Some of the more common tactics used by cyberstalkers once they learn your personal information are:

- Calling repeatedly, including hang-ups
- Following you to learn your schedules.
- Damaging personal belongings, including property

- Burdening you with unwanted gifts or letters
- Using technology such as spyware, cameras and tracking devices
- Driving by your home or place of employment
- Monitoring your movement on the computer or phone calls
- Threatening bodily harm to you, your family or pets

Cyberbullies are very similar to cyberstalkers; however, their concentration is more on electronic information and communication devices. Students are especially vulnerable to cyberbullies. Some of the tactics cyberbullies use are:

- Email harassment
- Instant messaging harassment
- Text messaging harassment
- Creating blogs to harass you

Always remember, cyberbullies do NOT have to be stronger or larger than their victims, as is the case with traditional bullies.

Webcams are providing a new avenue for cyberstalking and extortion. Criminals can hack into your webcam remotely, using it to watch you and you will not know it. An innocent-looking message can be sent that includes malware. Once you open the message, the malware enters your computer and the criminal has remote access to it and all of its programs, including the webcam. To avoid this invasion of privacy, turn your computer off and close your laptop when not in use.

TALK TO YOUR CHILDREN AND TEENAGERS about the importance of Internet safety. Children and teens don't often realize how what they put on the Internet can be used against them. They also don't realize how many people can see what they post and how any of their posts can be copied and kept or shared with other people. Even after they delete a post, it doesn't go away!

One growing scam used against teens is called "sextortion." A criminal uses a fake online profile to get close to the teen, gains their trust, and then asks for photos of the teen. Once even one photo is sent (or sometimes they will say they have a photo even when they don't), the criminal demands more pictures or personal information, saying they will send the photo to everyone if the teen doesn't comply. The teen often feels too guilty to tell their parents. Tell your children to be very cautious and not to talk to people they have not met in person!!