Private Client Group

Guide to Personal Safety and Security

Compliments of

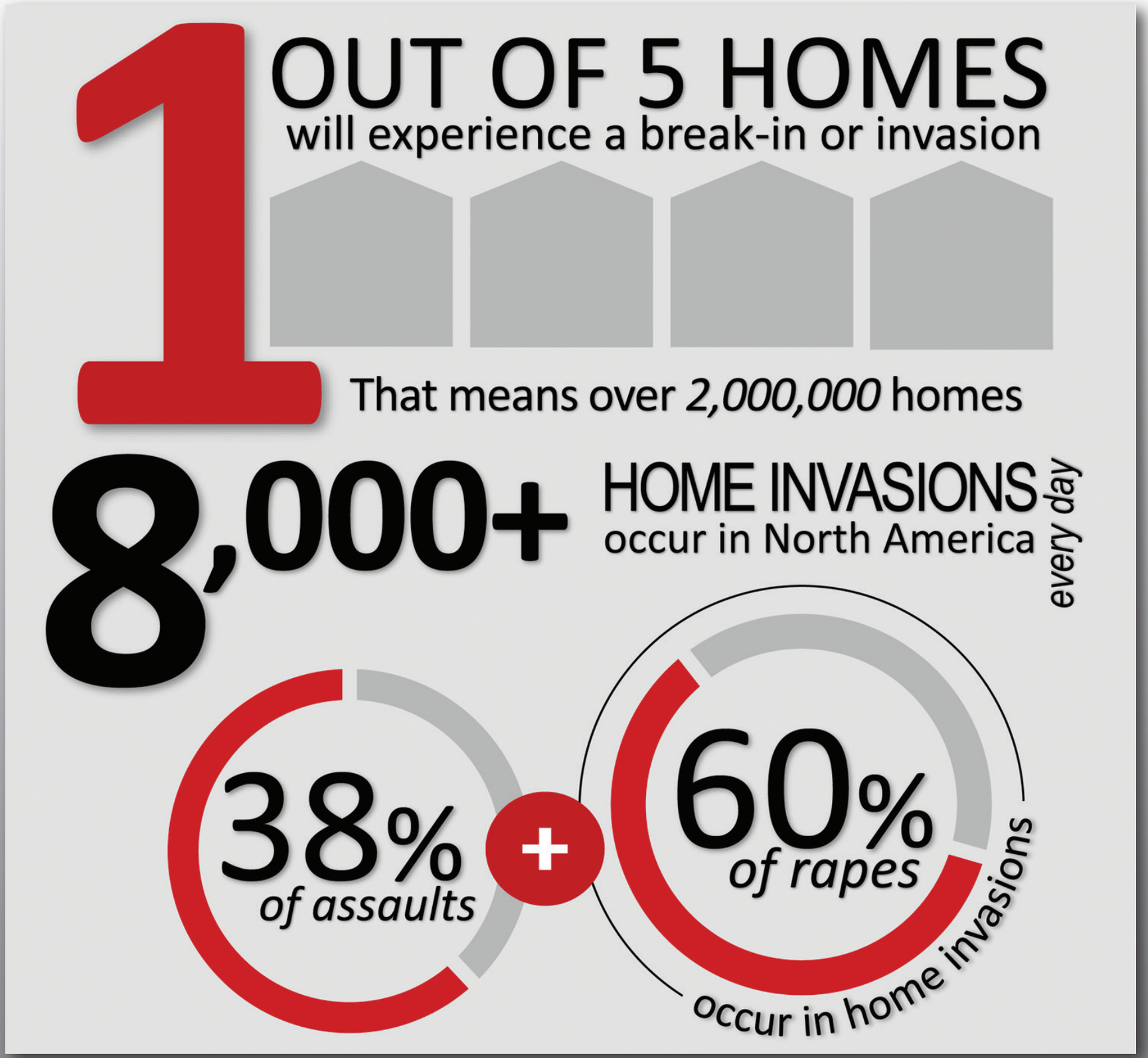
WEALTH MANAGEMENT
MIDWEST INC

For over 25 years Heartland Investigative Group has provided high-end investigative and specialty security services to an elite group of clients. Our highly certified staff of investigators, forensic specialists, and executive protection agents is relied upon by the region's leading corporations, law firms, and distinguished families. Through our Private Client Group we deliver full scale residential security audits, digital protection, due diligence, and investigative support to a select group of individuals.

A message from Paul Jaeb, CEO

"In my 25 years as an investigator and security consultant I have seen firsthand that those who do not exercise healthy skepticism and general observation are often victims. You don't have to be overly suspicious or take extreme measures – simply increase your awareness, take practical steps to protect yourself, and test your systems. Studies show that if you do these simple things you are far less likely to be a victim of a financial crime or physical assault."

WHILE AT HOME



- If you live alone, only use your last name and first initial on mailbox and phone listings. Never list “Miss” or “Mrs.”
- Never open the door to strangers. A quick visual identity check should be done through a 180-degree optical viewer. If you don’t have one, get one.
- Never rely on a chain lock - they offer very little security.
- Even the best lock cannot function if it is not used. Doors should be kept locked during the day, while in the house and when away. All the time. Every time.
- Always check the identification of repairmen and deliverymen. Never open the door automatically.
- Do not be embarrassed to place a call to an employer or business before allowing a worker inside.
- Children should never open the door for anyone - that is an adult’s job.
- Install a strong lock on the bedroom door. A cell phone next to the bed is a quick way to summon emergency help in case an intruder is heard.
- Lights should be left on at night even when you are away. Get a timer and vary the on-off pattern.
- Never give out personal information over the phone or let a caller know that no one else is home.

- Never give out your phone number. If a wrong-number caller asks your number, say “What number are you dialing?” If the caller gives the wrong number, say so. If they give the correct number, ask who they are calling and why. Be blunt until their reason for calling is established as legitimate.
- Use motion sensor lights at all entrances during the night. It’s good for you and bad for them.
- Become aware of places around the home where attackers might hide. Whenever possible, arrange for such areas to be well lit, more visible or avoidable.
- Make sure all home windows are securely locked at all times, especially at lower levels.
- Know a few neighbors who can be trusted in an emergency and keep their contact information readily available. Work to create a safety network and watch out for each other.
- When alone at night and an unexpected knock comes at the door, it is sometimes helpful for a woman to exclaim, “Harry, can you answer the door?” If the person knocking does not have legitimate intentions, this may be enough to scare the person away.
- If you are concerned about someone knocking, call someone you trust and approach the door while on the phone. Trust your instincts and call 911 if you feel threatened.
- Never report on social media that you will be gone on vacation or not at home. Make sure your children know this rule as well.

Notes

WHILE DRIVING

Popular carjacking locations are parking lots, shopping centers, gas stations, car washes, convenience stores, ATMs, hotels, valet parking, fast-food drive-thru, and outside of retail stores. Close proximity to a freeway onramp is a desirable escape factor from the carjackers perspective.

- The safest car is one that starts every time. Be sure your car is in good running order.
- Always have plenty of gas - at least one-half tank at all times. A person who runs out of gas is asking for trouble. Don't be that person.
- Inspect tires frequently. Well maintained tires are less likely to have flats and blowouts. The flat tire rule: they will always happen at the worst time in the worst neighborhood; avoid them if possible, be ready if necessary.
- Lock all doors and roll up windows before driving. Travel on busy, well-lit streets and plan routes carefully. Avoid unsafe neighborhoods even if it means taking a detour. A car in good condition is still subject to a breakdown at any time. Be aware and be ready at all times.
- Carry flares in the glove compartment. They are the clearest most visible signal of trouble.
- If a breakdown does occur, get out, open the hood, get back inside and lock all doors. Keep windows rolled up. Wait patiently for law enforcement officials to arrive, under no circumstance should you get out or unlock the doors for strangers, even if they seem to be good Samaritans.
- If possible call someone you trust on your cell phone and give them your location and stay on the phone until help arrives.
- If you must get out of the vehicle for some reason, leave a note behind with the time you left, your intended destination and description of anyone offering assistance.

- Beware of hitchhikers. Never pick them up no matter what their appearance or predicament. Never means never.

- Always lock the car when leaving and keep packages in the trunk. Packages left in the car, even if covered with newspaper or blankets, invite thieves. Ask yourself: what gets covered or hidden? Think ahead - put valuables in the trunk before you're worried they'll be stolen.

- Never stop to offer assistance to stalled cars. You can never be certain a breakdown is legitimate. If you want to help, use a cell phone to call the police or highway patrol and report the location of the stalled vehicle. You don't help anyone by putting your safety at risk.

- Don't tempt smash-and-grabbers. Keep valuables out of sight while driving.

- Keep the car in gear while stopped at traffic lights or stop signs. Give yourself plenty of room to maneuver and escape. If your safety is threatened, hold down the horn and drive away to safety. Make sure you're not followed and alert police.

- Frequently check the rear view mirror.

- Don't turn into a driveway or stop in a deserted area if you are being followed. Pull over to the curb in a busy area and let the suspect car pass. Get the license plate number and report it to the police.

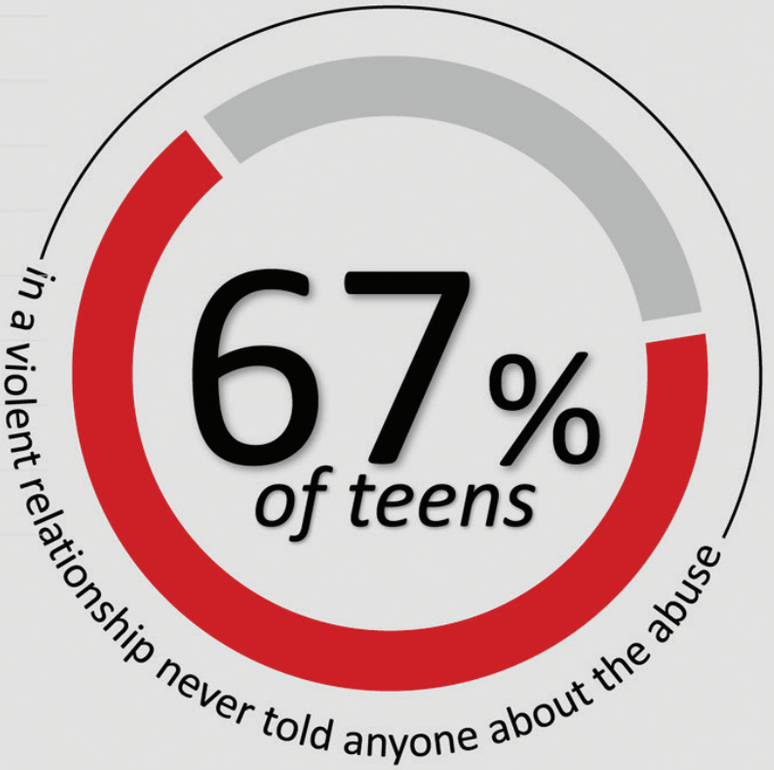
- If a car follows you to your home, stay in your car and sound the horn until the car leaves or help arrives.

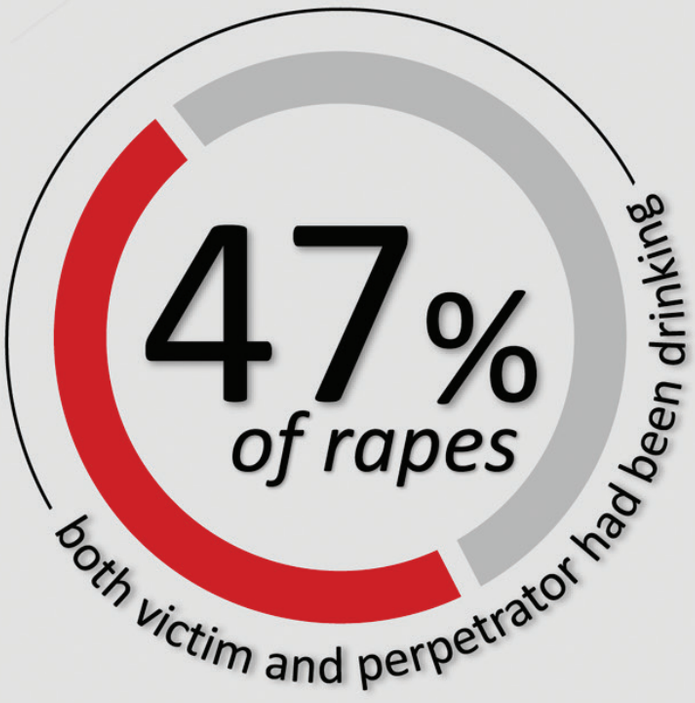
- Don't park in isolated or visually obstructed areas near walls or heavy foliage.
- Use valet parking or an attended garage if you're a woman driving alone.
- As you walk to your car be alert to suspicious persons sitting in cars.
- Ask for a security escort if you are alone at a shopping center.
- Watch out for young males loitering (handing out flyers, etc).
- Never leave the keys in the ignition, even if you are parked for a short time. Always remove the keys or fobs and take them with you.
- Have keys ready when getting in the car and always check the back seat and far rear area of SUVs to be sure no one has entered the car.
- Keep a cell phone charger in your car that is NEVER REMOVED.
- Have a Severe Weather Travel Kit in all vehicles. They are readily available at Amazon.

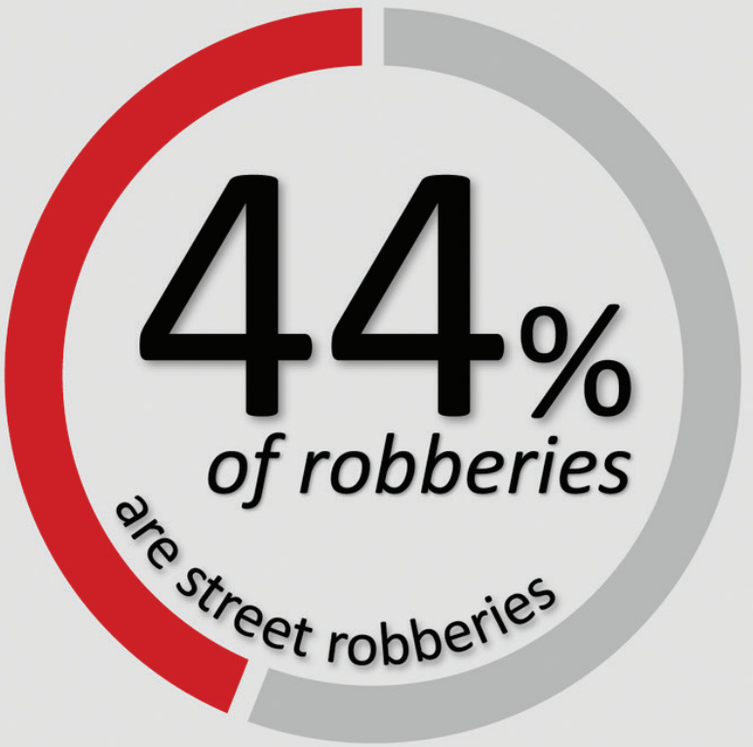
WHILE OUT AND ABOUT

Females 16-24 experience the highest rate of intimate partner violence

almost triple the national average







- Don't be too quick to enter an elevator. Many sexual assaults and robberies take place in elevators of large buildings and apartment complexes when the offender is able to attack the victim in seclusion. If there is a suspicious person on an elevator, trust your instincts and stay out. It is better to wait until the next car arrives.
- If a person enters the elevator and make you uneasy, get off immediately or at the next floor.
- When riding alone in elevators, stand next to the control panel. If you are attacked, hit the alarm button if possible, or as many floor buttons as can be reached. The idea is to make noise and keep the doors open.
- Everyone should realize that it is very risky to accept an invitation to go home with someone you have just met, even if the invitation is only for a drink or snack. This applies to men and women.
- A person planning to spend time alone with a new acquaintance should make sure a trusted friend knows the intended plans and the name and address of the new person.
- Any new acquaintance unwilling to provide truthful information concerning their employment, will not introduce friends and relatives, is unwilling to provide a land-line home phone number or home address should not be trusted. Those who keep secrets have things to hide.
- Never accept rides from strangers. Those who do are only putting themselves in jeopardy. This applies equally to men and women, and adults as well as children.
- When alone, particularly if jogging or walking at night, never wear ear buds.

For Teens:

There are many things teens and adults can do to reduce the chances of becoming a victim of teen date rape:

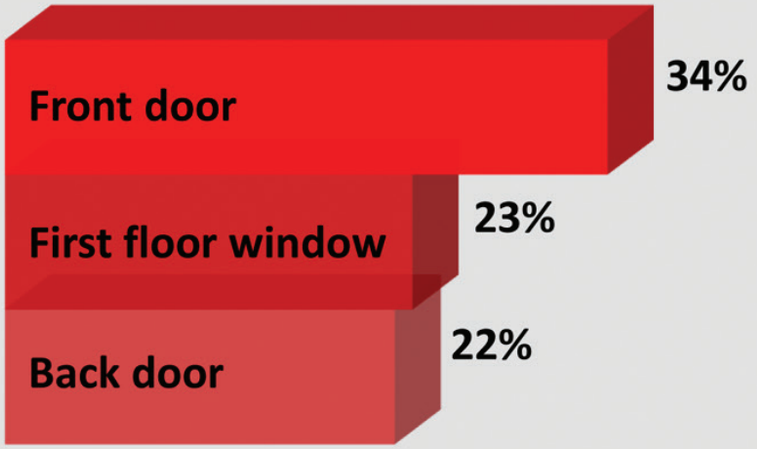
- Follow your instincts. If teens have a bad feeling about a person or situation they should get away as quickly as possible.
- Teens should know what they want from a relationship and avoid those who pressure them for more.
- All teens should carry a cell phone when they go out and have someone they can call if they need help.
- Teens should avoid getting rides with people they don't know well. A teen's car should have fuel and be in good working condition.
- If a teen is attacked or threatened, he or she should focus on making a lot of noise and trying to get away.
- Teens should learn self-defense.
- Acting confident and being aware of your surroundings makes you a less appealing target to most rapists.
- Teens who start dating young and who date people much older than themselves are at increased risk for unwanted sexual advances.

- Group dates and activities in well-lit public places are safer than being alone with someone.
- Don't drink or use drugs.
- Even for nonalcoholic drinks, don't drink out of a communal bowl - always open your own drink at parties and never let it out of your site.
- Immediately report any threats to the police.

RESIDENTIAL AND VACATION HOME SECURITY

*with burglars spending **no more than 60 seconds** breaking into a house*

Burglary entry points:



Many citizens are not conscious of always securing their homes, which results in:

- Leave drapes or shades in a normal open position during the work day; valuables should be kept out of sight.
- A few interior lights should be left on; bathrooms and hallways are logical choices. Automatic timers should be used and the timing occasionally varied. It's a good idea to come home to a well-lit house.
- A television or radio should be left on and tuned to a talk format so the home sounds occupied when the owner is away.
- Garage doors should never be left open; it is the ultimate garage sale and everything is free.
- Residents should participate in a neighborhood watch program. Form a network and help each other.
- There are good locks and bad locks. Invest in quality.
- New locks should be installed after moving to a new residence or when house keys have been lost or stolen.
- Keys should not be connected to any form of identification. The Heartland Rule: never link address with access.
- Do not leave notes on your front door; they signal an empty house.
- Door keys should not be left under flowerpots or doormats, inside an unlocked mailbox, over the doorway or in other 'hiding' places. If you can hide it, a burglar can find it. Use a coded lock box.

- When in the yard, always keep out-of-sight doors locked.
- All doors should be locked when you are working in the attic or basement.
- Suspicious “wrong number” calls or “nobody-there” calls should be reported to police officials. These calls often represent burglars trying to find out if anyone is home.
- All family members, especially children, should be warned not to give out any information. This is especially true about who is home, who is out, and how long they are expected to be out.
- Names should not be displayed on the mailbox or plaques in the front yard. This makes it easier for the burglar to look up a resident’s phone number in the directory, or online, and call to see if they’re home.
- Repairmen and others who claim to have business inside the house should show professional identification. Any doubts regarding identification should prompt a call to the individual’s company or superiors to be verified. The Heartland Rule: if you’re not expecting it, you’re not accepting it.
- Persons asking to use the phone should not be allowed inside under any circumstance. Even a strange child requesting to use the bathroom could be an accomplice to a burglar.
- Expected salespeople or workmen who have been admitted should not be left alone at any time.

- Broken streetlights should be promptly reported. Well-lit areas discourage burglars by removing favorite hiding places.
- Ladders should not be left outside. If they cannot be stored inside, they should be securely locked.
- Outdoor articles such as lawn equipment and bicycles should not be left on sidewalks, the lawn, porch, or other areas easily accessible to the general public. That's like giving them away.
- Vary your routines. Burglars have been known to watch people's movements for weeks at a time.

While on Vacation

- Ideally, a trusted neighbor or friend should collect all deliveries. If this cannot be arranged, deliveries should be cancelled.
- Leave a second car parked in the driveway instead of putting it in the garage. Better yet, ask a trusted neighbor to move it occasionally. This creates uncertainty. Burglars like sure things; keep them guessing.
- Mail should be picked up by a neighbor or the post office should hold all mail. An over-stuffed mailbox is a clear signal to burglars and an open invitation to a break-in.
- Arrangements should be made to keep lawns mowed or raked and snow shoveled. Think about it: fresh fallen snow and no footprints for three days - what does that say?

- Business travel or vacation plans should not be shared indiscriminately, particularly via social media.

- Tell a neighbor when you plan to travel. Ask them to be watchful and report any suspicious activity.

- Drapes or blinds should be left tightly closed - however a few may be left partly opened if a neighbor can readjust them from day-to-day and vary the pattern.

- At least one light should be left burning either in the bathroom or hallway. The neighbor can also vary this. Automatic timers should be used to turn additional lights on at dusk and off at your normal bedtime.

- If you have a safe, use it for valuables - including sensitive information and identity documents.

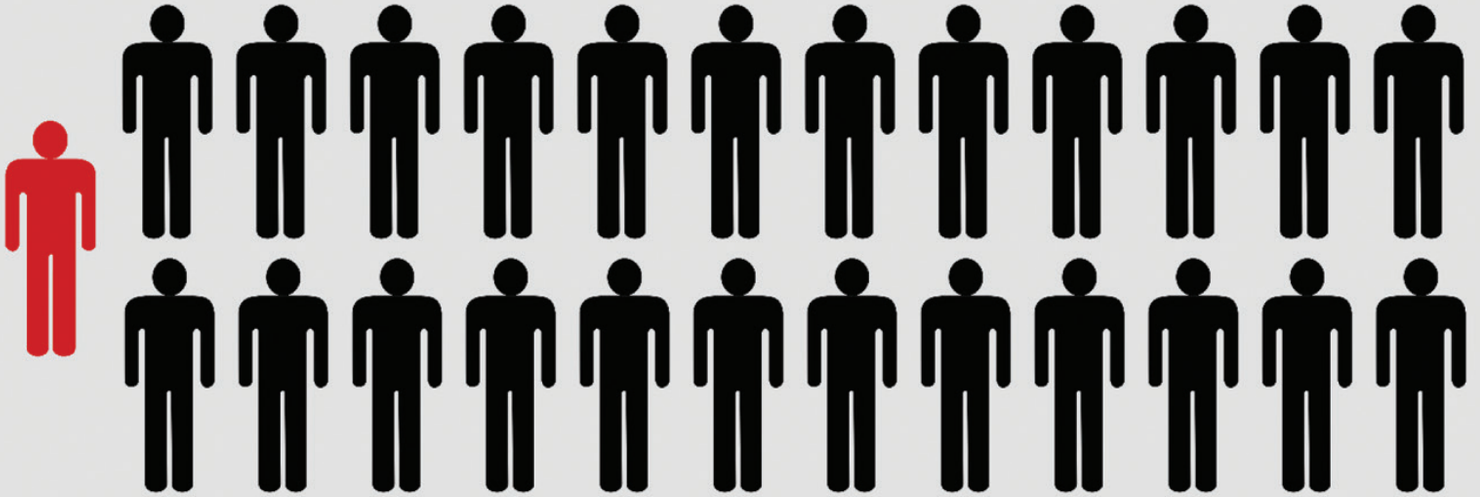
- Before leaving, you should notify the local police department. Although police cannot observe the residence at all times, they make more frequent checks.

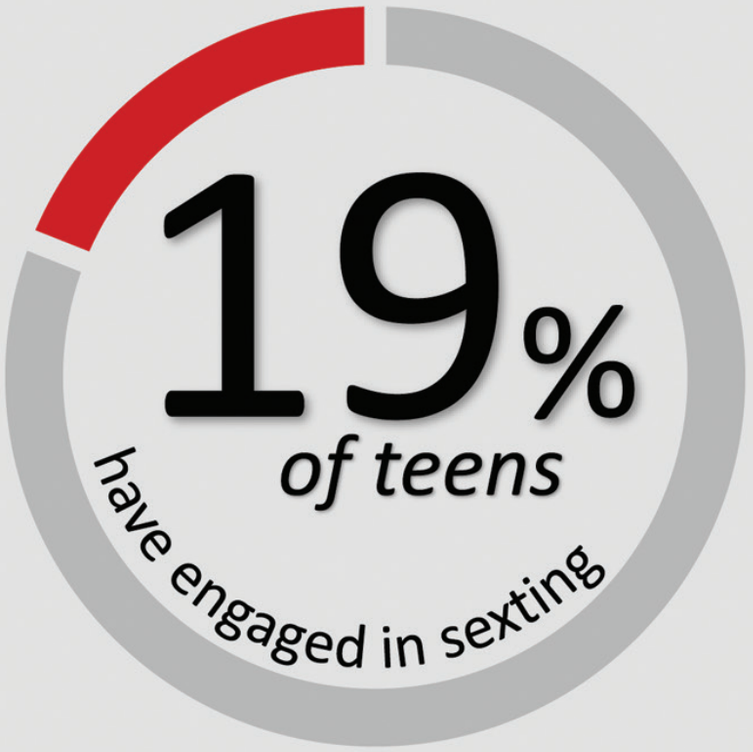
- Upon returning home, you should check for suspicious sounds, lights, and force marks before entering. If something seems wrong, you should not enter but call police at once.

Notes

PROTECTING CHILDREN

1 in 25 youth (about 4%) have received "aggressive" sexual solicitations that included attempts to contact them offline





- Parents should make sure their child receives a gradual amount of reliable and worthwhile information concerning human sexuality. Predators are out there and knowledge is power. No child should reach adolescence completely ignorant of sexual matters and they should certainly have an understanding of the danger of sexual predators.

- All internet access should be monitored. Keep computers in common areas of the home and check them frequently. The Heartland Rule: the internet allows strangers into your home; be on guard at all times.

- Obtain independent background investigations on anyone spending time with a child, including church volunteers, coaches, club leaders, and babysitters. Background checks conducted by the sponsoring organization are either non-existent or severely lacking.

- If a child reports a molester, parents need to remain calm in order to retain the trust and confidence of the child, and in order to minimize future psychological damage. As much information as possible regarding the offense and the offender should be obtained. Stay calm, gather information. Alert authorities when appropriate. Always consider the severity of any allegation. Never take matters into your own hands.

INFORMATION SECURITY

Sensitive information such as passwords are often associated with personal property (for example, bank accounts) and privacy and may present security concerns if leaked. Unauthorized access and usage of private information may result in identity theft, or theft of property. Common causes of information security breaches include:

Phishing

Phishing is a type of scam where the scammers disguise as a trustworthy source in attempt to obtain private information such as passwords, and credit card information, etc. through the internet. Phishing often occurs through emails and instant messaging and may contain links to websites that direct the user to enter their private information. These fake websites are often designed to look identical to their legitimate counterparts to avoid suspicion from the user.

Internet Scams

Internet scams are schemes that deceive the user in various ways in attempt to take advantage of them. Internet scams often aim to cheat the victim of personal property through false promises, confidence tricks and more. The elderly are particularly vulnerable to these frauds.

Malware

Malware, particularly spyware, is malicious software disguised as legitimate software designed to collect and transmit private information, such as passwords, without the user's consent or knowledge. They are often distributed through e-mail, software and files from unofficial locations. Malware is one of the most prevalent security concerns as often it is impossible to determine whether a file is infected, despite the source of the file.

PERSONAL DIGITAL SECURITY

The growth of the internet has given rise to many innovative and important tools, accessible to virtually everyone. Ten years ago our concern was strictly centered on email. However, the prevalence of social media has made communication with malicious users much more common. More and more, the misuse of email, texting, and social media is centered on vulnerable children. Common threats include:

Cyberstalking

Cyberstalking is the use of the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organization. It may include the making of false accusations or statements of fact, monitoring, making threats, identity theft, damage to data or equipment, the solicitation of minors for sex, or gathering information that may be used to harass.

Cyberbullying

Cyberbullying is often an extension of bullying outside the internet, and may take form in many different ways. For example, the malicious user might release images of the user without his or her consent. Because cyberbullying often stems from real-life bullying, this is largely a social concern, rather than internet safety. Cyberbullying occurs more

frequently than real-life bullying as the internet often provides means to carry out bullying while allowing the perpetrator to remain anonymous and hidden, avoiding backlash in the process.

Online Predation

Online predation is the act of engaging a minor into inappropriate sexual relationships through the internet. Online predators may attempt to initiate and seduce minors into relationships through the use of social media sites (Twitter, Facebook) or texting (via phone or SnapChat).

Obscene/Offensive Content

Various websites on the internet contain material that some deem offensive, distasteful or explicit. Such websites may include pornography, shock sites, hate speech or otherwise inflammatory content. Such content may manifest in many ways, such as pop-up ads and unsuspecting links. A recent trend among teens involves social pressure to view shock sites, which contain extremely graphic images and/or video. Some children experience severe emotional stress.

PREVENTION

Securing information: Keep shared information at a minimum

Cyberstalking and identity theft often begin by malicious users identifying the victim through identifying information provided by the victim himself. It is important to remember that information posted online may be seen by more people than is originally intended. Social networks make it simple to inadvertently share details about oneself (address, phone number, birthday, etc.), so as a precaution, it is best not to input this type of information onto these websites. It is also a common occurrence for users to make the mistake of sharing small bits of information occasionally, and through the use of search engines and some research it is possible to piece information together to identify the user. As such, avoid sharing personal information and personal history whenever possible. When creating usernames, websites, or email addresses, avoiding using anything that reveals any useful information such as a year of birth. Passwords and PINs should never be shared under any circumstances.

Passwords

Passwords are often created to keep personal information and property secure. If a password is compromised, it may lead to financial theft from online services such as bank accounts. One common way that

passwords may be compromised is through repeated guessing. Weak passwords make this process easier, so it is important that passwords be strong. Creating strong passwords is a way of keeping information secure. A strong password should contain the following:

- At least 10 characters
- Both upper and lower case letters
- Numbers
- Symbols (if allowed)
- Does not contain dictionary words

Avoid using simple passwords such as: “password”, “123456”, “qwerty”, “abc123”, names, birthdates, etc. Besides having a strong password, it is important to use different passwords for different accounts. This prevents access to all internet accounts, should someone get hold of a password. It is also good practice to regularly change your passwords.

PINs

PINs, like passwords, are a means of keeping information secure. A PIN may consist of at least 4 digits. Birthdays, birth-years, consecutive numbers, repeating numbers, and banking PINs should not be used as PINs for your internet accounts.

Social network websites

Profiles on social network websites may be seen by people you may not know. These websites often have privacy settings that you can alter so you can control who sees your profile and what information they are allowed to see. Do not accept friend requests from people you don't know.

Security software

Through the use of antivirus software, the user can automatically detect, prevent and remove computer viruses and various types of malware. Very often it is impossible for the user alone to identify infected files and software until it is too late, especially if the infected file or software is well disguised as a legitimate file. Because of this, it is important that the user keeps antivirus software running on the computer whenever accessing the internet so that the user can filter and block infected files.

Firewalls

A firewall is a program that controls incoming and outgoing internet traffic. Most operating systems come with firewalls. In order to keep your computer and information safe, it is important to keep the firewall on at all times when accessing the internet to prevent unauthorized access. Users are also able to control which specific programs are allowed through the firewall as well as those that are not.

Keeping up-to-date

Many computer software, such as operating systems, are not without flaws. Computer viruses often take advantage of these flaws to gain unauthorized access to a user's computer. When these security vulnerabilities are discovered they are often patched with security updates to eliminate the vulnerability. Operating systems, anti-virus software, and any other programs should be kept up-to-date with the newest security updates in order to keep viruses and harmful software from taking advantage of problems that have been fixed with updates.

Avoid scams

Be cautious of the internet. Avoid misleading ads, strangers with offers, strange emails, and questionable websites. Do research to verify the validity of these offers. If someone you know is sending you messages that don't seem like themselves, their account may have been taken over by somebody trying to get information out of you.

Parental controls

A good way to reduce the possibility of reaching offensive/obscene content is to set up parental controls. Parental controls allow users to place content filters on their computers while using the internet.

Public computer use

Public computers may be physically accessed by anyone within reach of the computer. Because of this, it is inadvisable to do any processes that involve sensitive information, such as online banking. A common way unauthorized access occurs is through users on public computers not fully logging out and clearing usage data (such as cookies), which allows access of the account to the next user of the public computer. It is also possible that the public computer could be infected with malware, unknown to the user. When using public computer terminals, remember to:

- Avoid saving private information such as usernames and passwords.
- Never leave the computer unattended while logged in.
- Clear your browsing data when you are about to leave.
- Watch out for people looking over your shoulder.

Public Wi-Fi

You should not access banking services or other financial institutions while at a public spot. Use browsers to check your email and other tasks. Browsers reduce data theft risk by providing encrypted connections. When entering a webpage in your broswer, try to enter **https** instead of **http**. This will ensure your login information is encrypted and not exposed on the wireless network.

THIRD PARTY PROGRAMS

Antivirus and anti-malware programs

Antivirus and anti-malware programs help prevent infections from occurring as well as detect and remove them from your computer. A variety of programs are available for use with purchase including Norton AntiVirus, McAfee VirusScan, and BitDefender Antivirus.

Ad and pop-up blockers

Misleading ads and pop ups can contribute to the accidental downloading of malicious software onto your computer. Most web browsers have internal pop-up blockers.

Password managers

These programs help organize passwords for your internet accounts so you won't have trouble remembering them. Password Managers encrypt your password data, and in some cases, automatically fill out your user and password data onto websites.

Heartland's Private Client Group
Leadership

Paul Jaeb, CEO
Chartered Fraud Investigator©

Tom Jaeb, President
Certified ID Theft Specialist©

Debra Thompson, Director of Forensic Accounting
Certified Public Account, Certified Fraud Examiner©

Kevin Eckhoff, Director of Security
Threat Assessment Professional©, Certified Protection Professional©

James Ristvedt, JD, Senior Investigator

Don Marose, Advisor
Lieutenant, Minnesota State Patrol; Drug Recognition Expert©

Paul Jaeb has been a licensed private investigator in Minnesota for 25 years. His clients include several public companies, over 1500 private companies, over 1000 lawyers, hundreds of banks, and dozens of distinguished individuals and families. He has held the highest leadership positions in his industry, is a sought after national speaker, online columnist for The Business Journal, and host of The American Private Investigator podcast. He leads a team of 100 professionals at their downtown Minneapolis headquarters.

Private Client Group

Heartland Companies©

Headquarters

1717 University Avenue West

St. Paul, MN. 55104

651-523-6827

pjaeb@heartlandinfo.com

www.heartlandinfo.com

PCG-5x5-WMM-20180831