Virginia Division of Capitol Police

2023

Virginia General Assembly Offsite Security Handbook

(804)786-HELP (4357)
dcp.virginia.gov
@VaCapitolPolice

Table of Contents

This information is provided by the Division of Capitol Police to provide some suggested ways you may address security concerns when you are away from the Virginia Capitol. Individual member security needs may differ, and different environments or security threats may suggest alternate courses of action. Moreover, security measures necessarily must be balanced against cost, and some security measures require trade-offs in matters of personal convenience, thus this document is not intended to be a prescription for security measures you should take. We encourage you and your family to read this document and to take these suggestions into account in making your own personal decisions about security precautions that may be appropriate for your individual circumstance. As always, the Division stands ready to assist you with your security concerns. However, if you find yourself in a situation requiring immediate police assistance away from the Capitol, the best course of action is to call 911 to obtain a prompt response from your local law enforcement agency or the Virginia State Police.

Division of Capitol Police

Administration

Colonel John T. McKee, Chief of Police
Office 804-786-5035 ChiefsOffice@dcp.virginia.gov

Communications Contact Numbers
EMERGENCY- 804-786-HELP (4357), Non-Emergency- 804-786-2568

Virginia State Police

Division One Headquarters: Richmond
Telephone: 804-553-3444; 1-800-552-9965

Division Two Headquarters: Culpeper
Telephone: 540-829-7401; 1-800-572-2260

Division Three Headquarters: Appomattox
Telephone: 434-352-7128; 1-800-552-0962

Division Four Headquarters: Wytheville
Telephone: 276-228-3131; 1-800-542-8716

Division Five Headquarters: Chesapeake
Telephone: 757-727-7288 (Chesapeake); 1-800-582-8350

Division Six Headquarters: Salem
Telephone: 540-375-9500; 1-800-542-5959

Division Seven Headquarters: **Fairfax**
Emergency number: 1-800-572-4510
Telephone: 703-803-2660 Non-emergency: After hours call: 703-803-0026

Virginia Poison Center

Local: (804)828-9123; Toll-free (800)222-1222

Virginia Fusion Center

For Emergency Threats/Incidents Involving Suspected Acts of Terrorism *Dial 911*

Use the NEW mobile app

SEE SOMETHING

SEND SOMETHING

SUSPICIOUS ACTIVITY? Call - 877-4VA-TIPS (877-482-8477)

What to do if you encounter an aggressive/reckless driver:

- Stay calm. Don't take it personally.
- Safely get out of their way and keep your distance from that driver.
- Avoid eye contact.
- Ignore rude gestures and refuse to return them.
- **Dial #77** on a cell phone or 911 for the nearest law enforcement office.
- If you are followed, go to a safe, public place and contact police.

For Virginia Traffic Information

Dial 511

VDOT 511

Download the free 511 mobile app for real-time traffic info.

Download on the App Store

ANDROID APP ON Google play

VDOT Safety Service Patrol 1-800-367-7623

Motorist assist services include:

- Tire change assistance
- Fuel to get to nearest gas station
- Jump starts
- Water for overheating radiators
- Contact local tow/recovery services
- Directions

Virginia State Capitol Alert Network

Sign-up for a VSCAN Account!

What is VSCAN?

VSCAN is an emergency notification system utilized by the Capitol Police to notify you of emergency events **in the** Capitol District**. When an incident or emergency occurs, Capitol Police can notify you using VSCAN. This is your personal connection to updates, instructions on where to go, what to do, or what not to do, who to contact and other important information.**

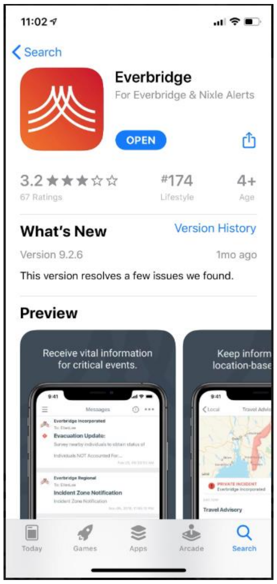
How does VSCAN work?

You can be notified via multiple contact methods such as email accounts (home, work, etc), cell phone, pager, or hand held device (smart phone). The following examples are just some of the types of alerts that you may receive via VSCAN that are impacting the Capitol District:

- **Severe Weather**
- **Critical Incidents**
- **Fire (Structure)**
- **Hazmat Situations**
- **Traffic Alerts Impacting Capitol District**
- **Earthquake and Tornado Drills**
- **Evacuation or Shelter in Place**
- **Other Important Information**

There is an App available on the iPhone and Android platforms called Everbridge. We encourage you to download this application as it offers many options such as sending photos, messages, and geographical details. In addition, it allows communication under adverse network conditions.

Questions can be addressed to: VSCAN@dcp.virginia.gov.



Everbridge
For Everbridge & Nixle Alerts

3.2 ★★★☆☆ 67 Ratings · #174 Lifestyle · 4+ Age

What's New · Version History

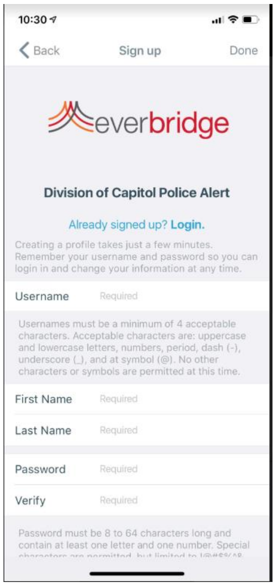
Version 9.2.6 · 1mo ago

This version resolves a few issues we found.

Preview

Receive vital information for critical events.

Keep inform location-base



Division of Capitol Police Alert

Already signed up? Login.

Creating a profile takes just a few minutes. Remember your username and password so you can login in and change your information at any time.

Username: Required

Usernames must be a minimum of 4 acceptable characters. Acceptable characters are: uppercase and lowercase letters, numbers, period, dash (-), underscore (_), and at symbol (@). No other characters or symbols are permitted at this time.

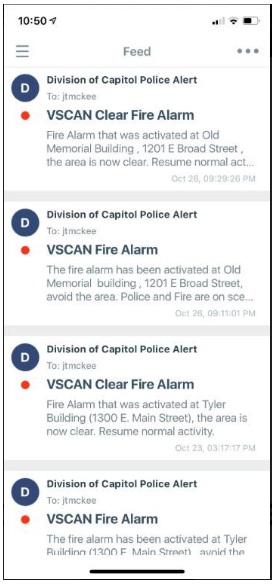
First Name: Required

Last Name: Required

Password: Required

Verify: Required

Password must be 8 to 64 characters long and contain at least one letter and one number. Special characters are permitted, but limited to !@#$%^&



Division of Capitol Police Alert
To: jtmckee
VSCAN Clear Fire Alarm
Fire Alarm that was activated at Old Memorial Building , 1201 E Broad Street , the area is now clear. Resume normal act...
Oct 26, 09:29:26 PM

Division of Capitol Police Alert
To: jtmckee
VSCAN Fire Alarm
The fire alarm has been activated at Old Memorial building , 1201 E Broad Street, avoid the area. Police and Fire are on sce...
Oct 26, 09:11:01 PM

Division of Capitol Police Alert
To: jtmckee
VSCAN Clear Fire Alarm
Fire Alarm that was activated at Tyler Building (1300 E. Main Street), the area is now clear. Resume normal activity.
Oct 23, 03:17:17 PM

Division of Capitol Police Alert
To: jtmckee
VSCAN Fire Alarm
The fire alarm has been activated at Tyler Building (1300 E. Main Street), avoid the

Mission Statement

The Mission of the Division of Capitol Police is to provide progressive law enforcement and security services to Virginia's government officials, employees, citizens of the Commonwealth and its visitors.

FOREWORD

Past events and a changed threat environment in the Commonwealth of Virginia have resulted in increased concerns about personal safety. In the Division of Capitol Police, we take pride and honor in the commitment to the personal security and protection of members of the Virginia General Assembly.

The Division of Capitol Police proudly continues to provide a high level of protection to the members of the General Assembly at their workplace. It is our goal to enhance your personal security while away from the workplace through increased safety awareness of personal protective measures. Good security begins at home and requires reporting any suspicious or unusual events to the local law enforcement agency. Upon request, the Division of Capitol Police will work with your local or state law enforcement agencies to address your offsite security needs.

This guide provides you with specific personal security information addressing concerns away from the workplace. We respectfully request you share it with members of your family. Applying these recommended considerations and measures to your daily personal activities will enhance your personal security.

John T. McKee

John T. McKee
Chief of Police
Division of Capitol Police

1 Personal Security

Criminal and terrorist acts against individuals usually occur outside of the home and after the individual's habits have been established. The purpose of this booklet is to inform you of a broad range of personal security considerations so that you can avoid unnecessary risk and deal knowledgeably with the dangerous situation if that should become necessary.

Personal Safety Basics

STAY ALERT to your surroundings.

- Know who is around you.
- Do not be preoccupied. PLAN where you are going before you go.
- Avoid low light areas and alleyways.
- Stay in well-populated areas.

Use your INSTINCTS and INTUITION.

- Intuition is reading the signals we give ourselves.
- Intuition is always right in two ways:
    - It is always in response to something.
    - It always has your best interest at heart.
- If you feel uneasy about a situation – avoid it!

PROJECT a confident image.

- Walk with confidence (firm and steady pace).
- Look people in the eye when you pass them.

Street Sense Tips

- Keep zippers and snaps closed on purses or bags.
- Hold your purse/briefcase tight and keep it close to your body – not towards your back.
- Carry your purse/briefcase towards the building side of the sidewalk and not the street side.
- The more packages you carry, the more vulnerable you are.
- If a driver stops to ask directions, avoid getting near their vehicle.
- Avoid strangers that contact you first.
- When someone tries to stop you – keep walking. Do not give them money or talk to them. If they are persistent, then loudly tell them to leave you alone and walk away.

Vehicular Travel

- Vary the times and routes when driving to and from the work place.
- Do not use vanity plates.
- Drive with doors locked. Keep windows completely closed whenever possible. All occupants should wear their seatbelts.
- Always lock your vehicle when it is parked.
- Park the car yourself whenever possible.
- Leave only the ignition key with the parking attendant, and only if absolutely necessary (never home or work keys).
- When in the vehicle, have a car charger cord for your cellular telephone and a spare battery with you.
- Be alert to the possibility of being followed. If you feel you are being followed, DO NOT CONFRONT THE PERSON(S). CALL 911
- Do not drive home or stop in an unprotected area.
- DRIVE IMMEDIATELY TO A SAFE LOCATION, such as a police or fire station.
  - If you drive to a police sub-station, make sure it is open before you exit your car. Police sub-stations are not always staffed.
- Have a secondary or even third, safe place to go, in case you cannot get to the police station.
- Ensure that trusted persons know the locations of your safe places.
- Keep your car in good working order. Make sure you have gas and fill up during the day.
- Always have your keys out and be ready to get in your car.
- Look in, around & under your car while walking to it. If something looks suspicious walk past.
- Lock your doors immediately after entering and keep your doors locked at all times.

Personal Safety in Large Crowds

- Make sure you know where the exits are, if possible park your vehicle near the facility exit for quick departure.
- If hosting an event, become familiar with the facility prior to the event.
- Identify alternate entrances and exits if the primary locations are inaccessible.
- Do not wear loose clothing or accessories that could become tangled or pulled.
- Wear closed-toe shoes and keep the laces tied to prevent tripping.
- Walk around crowds rather than pushing through them.
- If you're caught in a moving crowd, walk sideways or diagonally across it to work your way out.
- Establish a plan to rendezvous with your group if you become separated.

If you are planning to attend or host an event, keep security in mind and coordinate security needs with Capitol Police or local law enforcement.

Residential Security

The following are recommendations for keeping safe at home and preventing home invasions.

DOORS AND WINDOWS

Many home invasions occur because a door or window was left unlocked.

- Make sure that you have a solid core door with a dead bolt lock, in addition to any other lock, and a peephole. No glass should be on the door that can be broken to gain entry
- Install double cylinder dead bolt locks in the doors.
- Install three-inch screws through the strike plates for all entry doors.
- Lock all doors and windows during the day and at night, especially when you are home alone.
- Secure sliding glass doors with pins to prevent both horizontal and vertical movement, especially when you are away from home for extended periods of time.
- Be certain to draw all curtains, blinds and shutters on all windows during evening hours.
- Fix broken locks or windows and install dead bolt locks on doors leading outside.
- Change / replace locks if keys are lost or stolen or if you move into a previously occupied residence.

VEHICLE/GARAGE

- Park your vehicle inside of your garage.
- Enter your vehicle from the inside of your garage.
- Ensure that there is a backup system for the automatic garage doors.
- Ensure that all family members know how to operate the garage doors manually.
- Keep garage doors closed and locked when not in use.
- Ensure that the door from the garage into the main house itself is a solid core door with a dead bolt lock.
- Have a remote starter installed on your vehicle, especially if it is parked outside.
- If your vehicle is parked outside, ensure that the area is well lit.
- Do not leave garage door opener accessible.
- Do not leave GPS units in vehicle when not in use.
- Do not mark “home” in your GPS unit in the event that the vehicle or GPS unit is stolen.

PERIMETER/EXTERIOR

Perimeter lighting of your home is extremely important. Have lighting on an automatic timer with sensors to alert you and your family of any unauthorized access.

- Install motion detector lights for interior and exterior protection. Outside motion detector lights can be installed to automatically turn on inside lights, giving the impression that someone has entered the room, at the same time that the outside lights turn on.
- Ensure that the entire yard is illuminated at night.
- Trim all trees and shrubs to prevent an intruder's concealment.
- Incorporate any outbuildings, such as detached garages, pool house, or storage buildings, into the main security system.
- Install residential quality locks on all buildings.

GENERAL

- Install smoke detectors throughout the home. They should be hard wired into the home's electrical system with a battery back up.
- Maintain and keep proper fire extinguishers throughout the home, especially in the kitchen.
- Install an alarm system, with a battery backup. Test your alarm system monthly.
- Have the police emergency telephone number, **911**, and the police non-emergency telephone number available next to your phone for immediate use; program it into your telephone system if possible.
- Key control is absolutely essential. Keep keys in your possession. Do not place them under mats, over doors, in mail slots or in any other obvious place.
- Display decals or signs prominently on doors, windows, and in the yard to announce the presence of a security alarm system at your residence.
- Install timers on televisions, stereos, and lights.
- Do not answer the telephone with your name or official title.
- Have Caller ID for incoming telephone calls to your residence. Use Caller ID blocking to prevent your telephone number from being displayed on outgoing calls.
- Become familiar with the streets and roads surrounding your home.
- Have a planned escape route from your residence in case of fire or attack. Plan and practice driving to area emergency services, such as hospitals, police stations, and safe places.

Condominium and Apartment Security

The reduction of crimes committed against condominium and apartment dwellers must be a cooperative effort. The residents, management, maintenance staff and police working together are the only sensible answer. The following suggestions are offered to safeguard the security of members and their families who reside in condominiums and apartments:

- Have the police emergency telephone number, **911**, and the police non-emergency telephone number available next to your phone for immediate use.

DOORS AND WINDOWS

- Change / replace locks if keys are lost or stolen or if you move into a previously occupied condominium.
- Always double check doors and access windows before leaving your apartment. Make certain they are locked.

NEIGHBORS

- Avoid using the Laundromat in your complex by yourself. Team up with a neighbor.
- Develop a buddy system or an apartment alert system with your neighbors in the apartment complex to help protect each other's property. A well-organized and active tenant association would be most helpful.
- Getting to know the other tenants in your apartment or condominium complex is important. After you have met them, make a personal list for future use.
- Utilize a timer for lamps or the radio to give your apartment an occupied sound or look.

ENTERING THE BUILDING

- Do not buzz strangers into the building or allow strangers to enter the building when you are either entering or leaving.
- If someone enters the building by following you in and this person(s) is unknown to you, do not ride the elevator with them. If needed, exit the building and then re-enter at a later time.
- Report suspicious strangers, sounds or actions to police immediately, then notify the building manager and your neighbors.

Security Precautions When You Are Away From Home

- Leave the house with a lived-in look.
- Stop deliveries, such as mail and newspapers, or direct them to a neighbor’s home.
- Use a timer to turn lights on and off at varying times and locations.
- Leave a radio on (best with a timer).
- Have neighbors check the house for flyers, newspapers, or other items on the porch or in the yard.
- Secure your valuables and important papers in a home combination safe.
- If you own a home, the yard should be mowed or snow shoveled regularly.
- Leave contact phone numbers with your neighbor and the police in case of an emergency.
- Notify the police or a trusted neighbor of your absence.
- Be careful when using common facilities after dark.
- If you are living alone, do not place your full name on the identification slot or in the telephone directory. Use first and middle initials. (Example: “M.” Smith rather than “Mary” Smith.)
- Key control is absolutely essential. Keep keys in your possession. Do not place them under mats, over doors, in mail slots or in any other obvious place. Do not leave notes for the paper carrier or building manager advising of your absence. Stop deliveries while on vacation.
- Do not answer the telephone with your name or official title.
- Do not include your name or official title on your answering machine or announce you are gone.
- Have your telephone number blocked for outgoing calls.
- Have caller ID for incoming telephone calls to your residence.
- Avoid ordering products or services by telephone. If you do so, inform the merchant that you do not want your name and information given to others. (Even pizza delivery services can capture your name and personal information in their computer where it is then available to all employees.)
- Do not advise the doorman of your upcoming travel plans.
- Do not pay the paper carrier, grocery delivery person, etc., in advance; this would alert them to your absence. Have a trusted person mail your payments to them, as per your usual pay schedule.
- Notify the building manager if you leave for an extended vacation. Periodic checks can be made to protect your condominium / apartment.

2 Threats and Inappropriate Communications

Inappropriate Communications are any communications delivered:

- in writing
- by telephone
- verbally
- through an informant
- or by some suspicious activity

...that threatens, harasses, or makes ominous or unsettling overtures of an improper nature. This includes inappropriate pictures or drawings. They can contain explicit threats or ominous, unsettling, or questionable language or references. All threats are considered inappropriate communications, but not all inappropriate communications are necessarily threats. Occasionally, sensitive and high threat trials may evoke inappropriate communications from sources sensitive to the issues, parties, proceedings, or disposition of the case.

WHAT TO DO IF YOU RECEIVE A THREAT:

If you receive a direct or indirect threat and/or inappropriate communications while in Richmond, you should contact the Division of Capitol Police. If outside Richmond, contact your local law enforcement agency or the Virginia State Police and then notify the Division of Capitol Police.

3 Assault Situations

Initially, in most assaults the victim is at a serious disadvantage. The assailant usually has a plan, often a weapon and sometimes accomplices. The victim, on the other hand, is likely to be thinking about anything but an impending attack. The bottom line: the assailant has all the advantages. Your safety almost always depends on ESCAPE, not confrontation.

If you are on foot:

- Run from the assailant. Attract attention. Try not to run to a secluded area.
- While running, make noise (Scream, yell, blow a whistle, etc).
- Have **911** programmed into your cell phone.
- If you flee, drop packages or bags.
- If the assailant shoots at you, Run! If you can't run, Hide! If you can't Run or Hide, Fight!
  https://www.dhs.gov/active-shooter-preparedness#
- When police arrive, do not leave your cover until order has been restored and even then, only when told by the authorities.

If you are in the car:

- Attract attention – blow your horn, flash your headlights.
- Do not drive recklessly.
- Drive towards a safe location – a well-lit public location.
- CALL **911** AND KEEP THE LINE OPEN.

If you are in your home or office:

- If escape is not possible, go to the most secure area available – a room with a lock or a room with more than one exit.
- Call 911. Activate the alarm system.
- If you cannot escape, make it as difficult for your assailant as possible. Turn off the lights, pull down the window shades and hide.

IF YOU ARE TAKEN HOSTAGE:

In reality, the chance of being taken hostage is relatively small. It is still very important for you to take a few minutes to consider the actions you might take should the circumstances exist. Remember, the assailant has the initial advantage.

- Do not assume that all the assailants have identified themselves from the beginning.
- Follow hostage taker’s instructions exactly (do not attempt to interpret instructions).
- Remain calm. Be prepared to wait.
- Avoid personal injury.
- Do not make sudden moves or noises.
- Do not draw attention to yourself.
- Create a non-threatening image.
- Do what you are told. Be polite. Do not speak unless you are spoken to. Do not make any suggestions. A suggestion which fails might be construed as an attempt to subvert.
- Project human qualities and develop rapport.

After escape, release, or rescue:

- Cooperate with the authorities.
- Do not talk with the news media without first consulting the law enforcement officials (especially if others are still being held).

4 Air Travel

Whether you are going to the store or to Europe, the fact that you have left your home or office changes your security situation SIGNIFICANTLY. The following steps should be adhered to:

- Do not use your official title when making reservations.
- Keep your travel plans confidential, preferably within the family. Do not mention your travel plans on social media.
- When arriving at the airport, check your luggage as soon as possible and remain within security area as much as possible.
- Luggage tags should not reflect your official title.
- As a general rule, the best seats in the event of a hijacking are window seats, in the rear near an emergency exit.

> "…the fact that you have left your home or office changes your security situation significantly…"

WHEN AWAY FROM HOME FOR AN EXTENDED PERIOD:

- Your house should appear as if you were at home.
- Put several interior lamps on timers and set them at different times throughout the evening.
- Do not let newspapers or mail pile up.
- Let your adjoining neighbors know you will be away and ask them to keep an eye on your house.
- Keep your travel plans confidential, preferably within the family. Do not mention your travel plans on social media.
- Do not receive unofficial mail or packages.

Members traveling overseas can obtain general security information and travel advisories by accessing the U.S. Department of State's website at **www.travel.state.gov.**

5 Identity Theft

Identity theft occurs when a person knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit or to aid or abet any unlawful activity that constitutes a violation of federal law or that constitutes a felony under any applicable state or local law. Most identity theft involves the U.S. Mail. To reduce or minimize the risk of becoming a victim of identity theft or fraud, there are some basic steps you can take.

For starters, just remember the word "SCAM." Be:

Stingy about giving out your personal information to others unless you have a reason to trust them. Adopt a "need to know" approach to your personal data.

Check your financial information regularly and look for what should be there and what should not.

Ask periodically for a copy of your credit report. Your credit report should list all bank and financial accounts under your name and will provide other indications of whether someone has wrongfully opened or used any accounts in your name.

Maintain careful records of your banking and financial accounts.

WHAT TO DO IF YOU BECOME A VICTIM OF IDENTITY THEFT:

- Act immediately.
- If the crime involved the U.S. Mail, report it to your nearest U.S. Postal Inspection Service office.
- If the crime involved counterfeit credit cards or computer hacking, report it to the U.S. Secret Service.
- Check whether the major credit reporting agencies have accounts in your name that were opened without your consent. Ask them to place a "fraud alert" on your file.
- You may be advised to close some or all of your accounts. At the least, change your PIN codes and passwords immediately.
- Keep a record of the names and phone numbers of the people with whom you discussed your case, and of all reports and supporting documents.
- Report ID theft online with the Federal Trade Commission at **www.consumer.gov/idtheft** or call the Identity Theft Hotline at 1-877-IDTHEFT (1-877-438-4338).
- Virginia Attorney General website:
  http://www.oag.state.va.us/programs-initiatives/identity-theft
  1-800-370-0459

In addition, add these tips to your "must do" list to protect your identity:

- Do not leave mail in your mailbox overnight or on weekends.
- Deposit mail in U.S. Postal Service collection boxes.
- Shred unwanted documents that contain personal information.

The following is a list of the major credit reporting agencies:

- Equifax: **1-888-766-0008**, www.equifax.com
- Experian (formerly TRW): **1-888-397-3742**, www.experian.com
- TransUnion: **1-800-680-7289**, www.transunion.com

6 Internet Security

If a virus or a hacker attacks your computer, you could lose important personal information or software that is stored on your hard drive, as well as valuable time trying to make repairs. The Federal Trade Commission (FTC) offers the following tips:

- **Use anti-virus software.** A virus is a software that is planted in your computer to damage files and disrupt your system. You can avoid these risks by installing and using software that scans your computer and your incoming email for viruses, and then deletes them. You can download anti-virus software from the websites of software companies or purchase it in retail stores.

- **Regularly update anti-virus software.** To be effective, anti-virus software must be updated routinely with antidotes to the latest “bugs” circulating through the Internet.

- **Do not fall for a “phishing” email.** Most viruses will not damage your computer unless you open the email attachment that includes the virus. Hackers – people who use the Internet to access computers without permission – often lie to get you to open the attachments. Do not open an email attachment – even if it looks like it is from a friend or coworker – unless you are expecting it or know what it contains.

- **Use strong passwords.** Hackers may try to steal your passwords to gain access to the personal information stored on your computer. To make it tougher for them, use passwords that have at least eight characters and include numbers or symbols. Change passwords on a regular basis, especially when systems have been compromised.

- **Take advantage of your software’s security features.** Chances are that your web browser and operating system software give you some options for increasing your online security. Check the “Tools” or “Options” menus for built-in features. Similarly, your email software may give you the ability to filter certain types of messages, such as some unsolicited bulk email or spam. It is up to you to activate the filter.

The **FTC** works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit or call toll free, **1-877-FTC-HELP (382-4357)**.

- **Back up important files.** No system is completely secure. If you have important files stored on your computer, copy them onto a removable disk, and store them in a safe place.

- **If your computer is infected, take action immediately.** If your computer has been hacked into or infected by a virus, disconnect from the Internet right away. Then scan your entire computer with updated antivirus software.

- **Report serious incidents.** If you think you have been hacked into or infected by a virus, email a report of the incident to your Internet provider and the hacker's provider (if you can tell what it is).

If you have particularly sensitive information stored on your computer or you are planning to upgrade to high-speed Internet access, do not forget to:

- **Install a firewall.** A firewall is a software or hardware designed to block hackers from accessing your computer. Anti-virus software scans your incoming communications and files for troublesome files; a firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources.

- **Turn off software features that you do not use.** You may want to turn "off" some software features – instant messaging, printer-sharing or file sharing – that typically are "on" when the computer is shipped. Because these programs facilitate the passing of information between computers, they are an excellent entry point for hackers.

- **USB Flash Drive.** A USB Flash Drive is a removable data storage device. Only use a USB drive that have been issued by your agency or that has been provided by trusted sources. USB drives can introduce viruses and/or malware to secure systems without the user's knowledge.

8 Safety Skills for Children

Would your child know what to do if…

1. He or she got lost in a shopping mall?

2. A nice-looking, friendly stranger offered him or her a ride home after school?

3. A babysitter wanted to play a secret game that no one would know about?

4. He or she was at home alone and the doorbell rang?

5. A friend dared him or her to hitch hike?

While most children go through their childhood without ever experiencing physical harm, there could be times when your child is in danger or, at least, find themselves in a very scary situation. If your child has a plan of action, he or she will be able to work through the problem and bring it to a more satisfactory ending.

As a parent, one of your responsibilities is to teach your children how to protect themselves. You should always take time to listen carefully to your children's fears and feelings about people or places that scare them and make them feel uncomfortable. The **Children's Safety Checklist** on the next page provides a few basic actions to be taken which will go a long way toward your child's safety.

Children’s Safety Checklist:

1. Help your child memorize their full name, address, and telephone numbers (be sure to include the area code), and how to make emergency telephone calls from home, public telephones, and from cellular telephones.
2. Walk around the neighborhood with your children. Show them safe places to go in an emergency, like a neighbor’s house, or an open store.
3. Instruct your child never to accept gifts or rides from someone they do not know well.
4. Check your neighborhoods for areas that threaten a child’s safety, such as brush in wooded areas, abandoned buildings, areas with poor lighting, vacant lots littered with debris, and no sidewalks or bike paths next to busy streets.
5. Teach your children to go to store clerks to ask for help if you become separated in a store or shopping mall. Tell them never to go into a parking lot alone.
6. Accompany your child to public restrooms.
7. Teach children that no one, not even someone they know, has the right to touch them in a way that it makes them feel uncomfortable. Tell them they have the right to say “NO” to an adult in this situation.
8. Ensure that children are taking the safest route to school and to friends’ houses. Make sure that they avoid alleys, wooded areas and new construction. Test walk it together.
9. Never hang a house key around your child’s neck. That is a sure sign that you will not be at home when they return from school. Put it inside a pocket or sock.
10. Teach children to walk confidently and to stay alert to what is going on around them.
11. Encourage children to look out for other children’s safety and to report anything that does not seem right.
12. Tell your children to stay away from strangers who hang around playgrounds, public restrooms, and empty buildings. Teach them to report these things if they observe them.
13. Teach your children to write down and report to you the license numbers of people who offer to give rides, or hang around playgrounds or public restrooms.
14. Make sure that your children can reach you by telephone. Post your telephone numbers, along with numbers for a neighbor, police and fire departments and poison control center near all of your telephones.

Social Networking Safety

Tips for Parents

They love it! And oftentimes it seems that they can’t live without it. The rise of social networking sites has teens throughout the United States fanatical about these addictive websites. Social networking is a platform of online sites that focus on building relationships among people who may share the same interest or activities. It provides a way for users to interact over the Internet. Users are often identified by their profiles, which can consist of photos and basic information, such as location, likes and dislikes, as well as friends and family. Well-known sites such as Facebook, Twitter, Friendster, WhatsApp, Snapchat, Instagram, Tumblr, have taken social networking to a new level. In addition to the convenience of being able to access these websites from a computer, there are also applications on mobile devices that make it easy to access social applications anywhere and anytime. As a parent, you want to make sure your child is safe when he or she is engaged in social networking. You may find it challenging to keep up with the ever-changing technology. You may also feel like your child is much more Internet savvy than you are, and in fact, that may be true. However, as well informed as your teen may be, he or she may not be aware of the dangers of online networking and what precautions he or she should take to stay safe. It is time to talk to your teen about social networking safety.

Familiarizing yourself with the basic terminology that is used on most social networking sites will help you communicate effectively with your teen about the topic.

- Post -A message that can be updated to notify your selected followers of what you are doing or thinking.
- Tagging-To label friends in a photo and link to their profile pages. If tagged, you're notified so that you can de-tag or stay linked to the comment, video, or photo.
- Wall-Area on your profile where friends can post their current locations, comments, pictures, or links.
- Places- This feature allows a user to post his or her current location. This information is then shared with all of the user’s followers.
- Friend Request-A person interested in being a friend will send a request, which can either be accepted or denied.
- Blocking- Prevents another user from searching and viewing your profile; you can ban access temporarily or permanently.
- Hacker- Someone who breaks into computers or computer networks and accesses a profile user’s information to get money or to break into other personal accounts. Some may also create false profiles or pose as another user.

The four major dangers of using social networking websites are:

- Over sharing information. When creating a profile page, most websites will ask for personal information such as home addresses, birthdays, and phone numbers. Giving this information can be very dangerous and will be made public to anyone who visits a user’s profile page, especially if privacy settings are not set correctly. Even if account settings are set to private, users are still at risk of their accounts being hacked. If someone hacks into an account, he or she will be able to view and use the information. Sharing simple things like your favorite color can tip off a hacker to try to see if you used that as a password on your account. The biggest threat of over sharing information is identity theft. Identity theft is not uncommon in the world of online social networking. Online computer criminals look to steal identities in obvious and not so obvious ways. An obvious way would be someone asking for your social security number. A not so obvious way is luring a user to click on a link that will allow the criminal to download all of the user’s personal information. The anonymity provided online makes it easier for computer criminals to go undetected.
- He is not who you think he is. Social networking sites make it very easy to pretend to be someone else. Even if an individual may be friends with someone on the site, anyone can take control of a user’s account if he or she can obtain the user’s password. As a result, someone who is a “Friend” can ask for money or gain personal information that can be used to hack into other accounts. For example, you may get a message from a relative asking you for your banking information because he or she would like to wire you some money for your birthday. You may think you are talking to your relative, but in fact, someone who has hacked into your relative’s account is requesting the information.
- Location-based services. Location-based services can be one of the most dangerous features provided by social networking sites. It exposes the profile user’s location and whereabouts. The service also has a feature that allows users to tag who they are with at any given time. While it can be fun to share your location with friends and family, it can also increase your vulnerability, potentially opening you up to being robbed, sexually assaulted, or worse. Predators can use this tool to track your movements and determine when you are alone or when you are not at home.
- Posting photos. One of the features of online social networking that many teens enjoy is the photo-sharing feature. This feature allows you to post photos 24 hours a day. Whether it is from your computer or mobile device, posting photos can be done in seconds. The Internet makes it easy to obtain photos and use the images in any way a person may choose. Posting inappropriate photos that may be deemed as fun, cute, or sexy, can end up where one least expects it. Photo tampering is a big threat when it comes to posting photos online. The use of photo editing tools allows people to manipulate online images in any way they choose, whether it’s used for good or bad purposes. While posting pictures and sharing them with friends can be fun, it can also be risky.

Teaching Your Teen Three Simple Steps To Increase Safety

1. Do not give optional information-When creating a profile, you do not need to enter all of the information that is requested. The set-up page usually requires you to fill out basic information, such as your name and email. Everything else is optional. Do not feel obligated to put your address and telephone number.
2. Third level of privacy- There are three levels of privacy settings to choose from for your profile. There is “open to everyone,” “open to friends of friends” and “friends only.” The best setting to use is the “friends only” setting on all of your privacy choices. “Friends only” is the strictest level of security; it only allows people that you have accepted as a friend to view information about you.
3. Accept only people you know- Accepting only people you know and trust is a great way to ensure safety when using social networking sites. Doing this can protect you from spammers, pedophiles, and other people who use social networking sites to commit crimes.

When discussing social networking safety with your child, encourage him or her to always use discretion when posting any type of photo, location status, and message. Tell your teen to ask him or herself these four questions before posting to the world:

"Think Before They Post”

1. Should I share this? Will the information you share put yourself or someone else in danger?
2. Do people really need to know where I am and who I am with? - Is it a good idea to let everyone know my exact location?
3. Am I selecting friends online that I can trust? –Always keep in mind that it's not just about what you post, but how others may use that content.
4. Is the information I am sharing transparent? - Before sharing information to the public, does your post give out too much personal information?

Having a discussion with your teen about social networking sites can ease some anxiety about your child’s safety. Social networking sites help us stay connected to family and friends. However, it is important to make sure your child knows how to be safe while online. Encourage them to enjoy the sites but to be safe at all times.

For more information on social networking safety visit www.ncpc.org