



THE USAA
EDUCATIONAL
FOUNDATION®

Good Information for Good Decisions.®

SAFETY

INTERNET SAFETY FOR TEENS



OUR MISSION

The mission of The USAA Educational Foundation is to help consumers make informed decisions by providing information on financial management, safety concerns and significant life events.

This publication is not medical, safety, legal, tax or investment advice. It is only a general overview of the subject presented. The USAA Educational Foundation, a nonprofit organization, does not provide professional services for financial, accounting or legal matters. Consult your tax and legal advisers regarding your specific situation. Information in this publication could be time sensitive and may be outdated. The Foundation does not endorse or promote any commercial supplier, product or service.



TABLE OF CONTENTS

March 2011

The Internet And You An introduction	2
Words From The Wired World Understanding Internet terminology	4
Passwords Creating and protecting your passwords	5
Social Networking Communicating safely	6
Cyberbullying Taking action against online bullies	8
Mobile Communications Using your mobile device safely	10

2 THE INTERNET AND YOU

The Internet is one of the greatest conveniences of our time, because it brings the world to you. However, just as when interacting in person, there are dangers associated with the Internet.

Who Is Out There?

Because of the Internet's anonymity, some individuals are not who they pretend to be.

Chat rooms and other Web-based social networking sites are not “chaperoned,” and can be among the most dangerous areas of the Internet.

Why? Because you enter a chat room, strike up a conversation and soon you may be sharing personal information. Unfortunately, your typewritten conversation can be seen by everyone in the chat room and that includes adult- or older-teen predators looking for their next victims.

If a stranger approached you and asked for your name, home address, phone number or financial information, you would not give it out. So, it is important to remember not to release that information online either.

The Internet, Your Parents And You

Your parents want the best for you and it is their job to keep you safe. Make sure they are OK with your Internet activities — what sites you can visit and how long you can stay online, for example. You should also share your password with your parents. If something happens to you, their ability to access your Internet records may save your life. Talk to them. Tell them you respect their privacy and trust them to respect yours.

FOR MORE INFORMATION ON INTERNET SAFETY

- www.onguardonline.gov
- www.getnetwise.org
- www.i-safe.org
- www.netsmartz.org
- www.mcgruff.org
- www.staysafeonline.org
- www.wiredsafety.org
- www.stopcyberbullying.org

What else can you do to stay safe? Stay anonymous. Do not post information that will identify you, including:

- Your full name.
- Your home address or phone number.
- Your Social Security number (SSN).
- Passwords.
- Credit card or bank account numbers.
- Names of family members or friends.
- Your school, workplace or favorite hangout.
- Names of clubs or organizations to which you belong.
- Information that would help someone guess where you live.
- Do not use a nickname that can be used to identify you in any way — “CharlestonTeen,” “LeeHighRunner” or “KyWildcatFan,” for example.
- Never share your account password with anyone except your parents.

Protect Your Computer System

- Consider using encryption to protect your personal information.
- Shut down your computer when it is not in use — especially in public places, such as Internet cafes, coffeehouses or airports.
- Keep your antivirus and antispyware programs, other software and operating systems updated to protect against new attacks.
- Consider using a firewall on your system to protect against hackers accessing your system remotely.

4 WORDS FROM THE WIRED WORLD

COMMON INTERNET TERMS

Internet Service Provider (ISP)	A company that provides Internet access to consumers.
Password	A secret word used to confirm your identity when you log on to a Web site.
Search Engine	A program that searches for information based on key words. The search produces a list of related Web sites.
Hyperlink	An online section of text or an image that, when clicked, automatically connects an Internet user to related information or Web pages.
Blog Or Web Log	A chronological, online diary of thoughts, ideas or events taking place in the owner — or blogger’s — life.
Chat Rooms	Online gathering places where individuals with common interests “meet” for discussions that appear almost immediately on the monitors of other chat participants.
Bulletin Boards	Electronic messages that are posted for others to see.
Profile	A short, succinct Internet “resumé” that lets other Web users know a little about you and your interests.
Filters	Programs that screen Web pages to determine whether they should be displayed to users. For example, parents can install filters that prohibit their children from accessing pornographic or other objectionable content.
Encryption	A way to secure information by scrambling it into a code that can be read only by authorized individuals.
Virus	A malicious program that can make your computer “crash,” behave erratically or destroy files. Viruses are often spread by e-mail or file-sharing programs.
Hacker	An individual who remotely accesses and tampers with information on other individuals’ computers.

Creating Passwords

Passwords are used to access personal information stored on a Web site or on your computer.

Although your password should be easy for you to remember, you will need to change it often. Why? Because passwords obtained by criminals or predators may be used to gain access to your financial accounts or private information or to impersonate you when applying for credit, opening bank accounts or making purchases.

Protecting Your Passwords

- Create passwords with a combination of at least eight letters and numbers and use both uppercase and lowercase letters. Longer passwords are more difficult to decipher.
- Think of a phrase or sentence meaningful to you and that is easy to remember. Then, take the first character from each word, alternate uppercase and lowercase and use some common letter-number substitutions.
- Do not use personal information as part of your password including your name, your pet's name, the name of your school or mascot, your Social Security number (SSN) or your current or former address.
- Stay away from letter or number patterns and sequences (for example, "abcdefg" or "121212").
- Change your password every 60 to 90 days.
- Vary your password — do not use the same one for every account or retail site.
- Use a password that differs from your screen name.
- Do not store your password online.

6 SOCIAL NETWORKING

Staying Safe Online

It is important to remember that the rules of behavior that apply in person apply online, too.

- Think about how your e-mail message will be read by others. Do not say anything online that is cruel or may damage someone's reputation. Doing so puts you at risk of being accused of slander or defamation or may cause a dangerous escalation of hostilities.
- Do not give out personal information about another individual.
- Do not forward another individual's e-mail without their permission.
- Never post anything that you would regret later or cause you embarrassment or shame. The Internet is the most public of forums. Once you have posted a comment, a photograph or a video, it cannot be erased or taken back. You cannot control its duplication and it may be used against you.
- Once posted, the information can be seen by anyone online including family and friends, employers or potential employers, admissions officers at colleges you want to attend, police and other law enforcement authorities.

Know When to Log Off

Conversations that take place over the Internet can be safe. After all, you can log off if a discussion makes you uncomfortable.

The problem begins when you share too much personal information or an online friendship turns into an in-person meeting. The media is full of stories about teens whose meetings with Internet "friends" turned scary, violent or even deadly.

How can you avoid becoming a victim? First, trust your parents. They have your best interests at heart. If you are considering meeting someone you know only through the Internet, tell them. Never arrange an in-person meeting with someone unless:

- Your parents say it is OK.
- Your parents speak to the other individual's parents by phone.
- Both sets of parents go with you to the first meeting.
- The first meeting is in a public location.

WHEN SHOULD YOU SPEAK UP?

According to the National Center for Missing & Exploited Children, you should not respond to e-mail, chat comments, instant messages or news group messages that are inappropriate or make you feel scared, uncomfortable or confused. Show the message to your parents or a trusted adult and report it to your Internet service provider (ISP). Additionally, report the following to the CYBERTIPLINE at www.cybertipline.com.

- Anyone you do not know who asks for personal information, photographs or videos.
- Unsolicited obscene material from individuals or companies you do not know.
- Misleading Internet URLs that point you to sites containing harmful materials, instead of what you were looking for.
- Anyone who wants to send you obscene photographs or videos of minors (18 years of age and younger). The possession, manufacturing or distributing of child pornography is illegal.
- Online enticements for offline sexual activities. No one should be making sexual invitations to you online — and it is an especially serious crime for adults.
- Threats to your life or safety.
- Threats to others.

8 CYBERBULLYING

You have probably been bullied at school at least once. It is not fun. But what if the bully follows you into the safety of your home — by taunting you and saying hurtful things online?

Internet bullying, known as cyberbullying, is a common problem for teens and younger children. Sometimes the bully is someone you know from school. But sometimes it is an individual you do not know well at all — someone you angered in a chat room or on a gaming Web site. Perhaps the bullying seems random and you do not know why it even started.

Cyberbullying can be very public. The bully may spread mean comments and hurtful lies to many individuals via the Internet and others may join in. An individual may bully for the following reasons:

- Anger and revenge — by “teaching the victim a lesson.”
- Entertainment — bored with too much free time.
- Power — to boost the bully’s ego.
- Accidentally — not realizing the offensive contents of the message.

Being a victim of cyberbullying can be a painful experience. Cyberbullying is easy to commit because the bully does not have to confront the victim. A cyberbully may take the following actions:

- Pretend they are another individual while online.
- Spread rumors about the victim.
- Trick a victim into revealing personal information.
- Send or forward rude comments about the victim.
- Post photographs of the victim without their consent.

The more repeated the communications are, the greater the threats. Here are some tips if someone is bullying you online:

- Ask your parents to go online to warn the individual that if the behavior does not stop, they will inform his parents, the Internet service provider (ISP) and the appropriate law enforcement authorities.
- Save every communication from the bully and document the following threats:
 - Is the kind of threat an insult or could it cause harm?
 - What is the frequency of the threat? How many times has it occurred?
 - Is the source of the threat an acquaintance or a stranger?
 - Is the nature of the threat through an e-mail, text or chat room?
- Do not respond or make counter-threats or accusations. That will only make things worse.

If the cyberbully continues to make threats take action:

- Block all communication from the cyberbully such as e-mail or instant messaging (IM) accounts.
- Stay out of the chat room or other sites frequented by the bully.
- Report the incident to your ISP.
- Stay offline, if necessary.
- Delete your current account and open a new one.
- Give your new e-mail address to only those you trust.

Most cyberbullies do not realize how hurtful their actions are and the possible consequences they face. Contrary to what cyberbullies may believe, cyberbullying is a serious problem. It can escalate quickly and can be dangerous.

10 MOBILE COMMUNICATIONS

Mobile devices let you use the Internet wherever you go. You can keep in touch with friends and parents, search for information and even get help in an emergency. Many cell phones feature built-in Global Positioning Systems (GPS) that can locate you if you are too sick or injured to place a call.

However, your mobile device can also become a tool for online stalkers, scammers, identity thieves and other predators. For safe mobile Internet use, take the same precautions you take with your computer. In addition, follow these important steps.

Protect Your Privacy And The Privacy Of Others

- Never share your cell phone number with strangers.
- Never share a friend's cell phone number without permission.
- Be cautious of the information you send in a text message and do not respond to text messages from someone you do not know. Never text while driving.
- Do not allow others to take digital photographs of you in embarrassing or compromising situations.
- Never take or post digital photographs of others without their permission.
- Use extra caution when using social networking sites from your mobile device.

Guard Your Mobile Device

- Be as careful with your mobile device as you are with your wallet or purse.
- Tell your parents immediately if your mobile device is lost or stolen.
- Keep your mobile device out of sight in your pocket or purse when not in use.

- Never use your mobile device to store sensitive information such as bank account information or your Social Security number (SSN).
- File copies of your mobile device account information, passwords and contact lists in a secure location, apart from the device itself.

Prevent Unauthorized Use

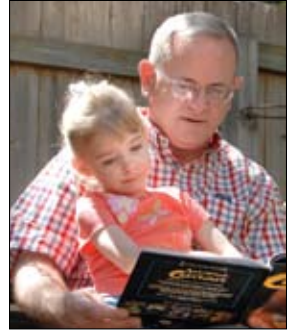
- Create a password that you must enter for use of the keypad. Choose a password easy for you to remember but difficult for others to guess.
- Turn on the autolock feature, which disables your device when not in use.
- Activate the encryption feature, if available, to protect your data and prevent others from listening in.
- Never loan your mobile device to anyone, not even to a friend.
- You can remotely track, erase or deactivate any lost or stolen device if you have equipped it with antitheft tools.

Stop Unwanted Calls

Register with the Do Not Call Registry to stop unwanted telemarketing calls. Dial (888) 382-1222 from the phone you wish to register.

12 NOTES

RESOURCES



The USAA Educational Foundation offers the following publications on a variety of topics:

PROTECTING YOUR IDENTITY AND PERSONAL INFORMATION (#520)

BICYCLE SAFETY (#542)

CYBERSECURITY (#575)

GET MONEYWISE (#504)

GET CREDITWISE (#534)

MANAGING CREDIT AND DEBT (#501)

KEEPING EVERY YOUTH SAFE (K.E.Y.S.)

- **BEHIND THE WHEEL (#565)**
- **ON THE ROAD (DVD) (#567)**
- **COST OF DRIVING (#568)**

LIVING A GREENER LIFE (#560)

SUICIDE PREVENTION (#581)

HOW TO SUCCEED IN COLLEGE (#512)

To order a free copy of any of these and other publications, visit www.usaaedfoundation.org or call (800) 531-6196.

Information in this publication was current at the time it was printed. However, the Foundation cannot guarantee that Web sites and phone numbers listed in this publication have not changed since then.

If a Web site address or phone number has changed since you received this publication, log onto a search engine and type in keywords of the subject matter or organization you are researching to locate such updated information.

THE USAA EDUCATIONAL FOUNDATION®

WWW.USAAEDFOUNDATION.ORG®



USAA is the sponsor of The USAA Educational Foundation.

The USAA Educational Foundation www.usaaedfoundation.org is a registered trademark of The USAA Educational Foundation.

© The USAA Educational Foundation 2011. All rights reserved.

No part of this publication may be copied, reprinted or reproduced without the express written consent of The USAA Educational Foundation, a nonprofit organization.

