

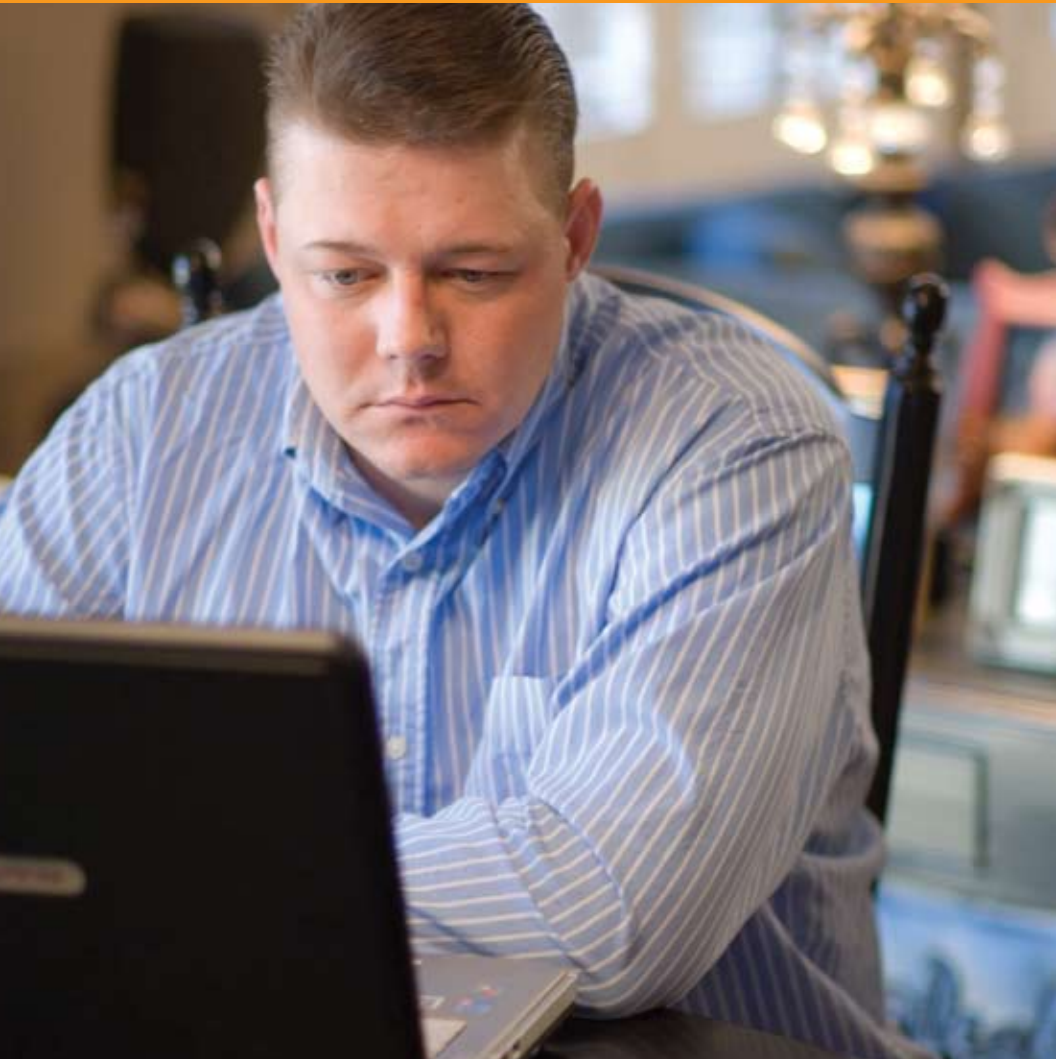


THE USAA
EDUCATIONAL
FOUNDATION®

Good Information for Good Decisions.®

SAFETY

INTERNET SAFETY FOR ADULTS



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 Information in this publication could be time sensitive and may be outdated.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	3
Passwords Creating and protecting your passwords	4
Safeguarding Your Privacy Protecting your personal information	5
Social Networking Communicating safely	6
You, Your Children And The Internet Protecting your children while they are online	8
The New Face Of The Childhood Bully Addressing cyberbullying	10
Mobile Communications Using your mobile device safely	11

2 THE INTERNET AND YOU

The Internet is everywhere today — at work, in your home, in coffeehouses, in airports. The benefits of wireless technology are boundless. With a desktop or laptop computer, or even with an Internet-enabled cell phone, you can quickly and easily go online to:

- **Reference educational resources** — Find a definition or a spelling, conduct research or take a Web-based college course without ever leaving home. You can even check your children's grades or find out if they turned in their homework.
- **Communicate with family and friends** — E-mail loved ones around the world, send video greetings and photographs, create a personal Web site, chat via instant messaging (IM) or talk live and “face-to-face” via a Web camera.
- **Search for information or entertainment** — Find out where to catch the latest film, buy tickets to a live performance, make reservations at your favorite restaurant, search for and purchase a new suit or pair of shoes, or participate in an online auction.
- **Banking and e-commerce** — Check account balances and investments, pay bills, transfer funds, buy and sell stocks and deposit checks electronically.

There is no doubt that the Internet makes our lives easier. But as beneficial as the Internet might be, it is also a place for fraud, identity theft, invasion of privacy and other cybercrimes.

Use the Internet, but use it wisely. This publication gives you tools and tips that will help you reap the benefits of electronic technology, while giving you the information you need to protect yourself and your family.

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.

4 PASSWORDS

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 cybercriminals or thieves can be used to gain access to your financial accounts or private information or to impersonate you when applying for credit, opening bank accounts or purchasing products.

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 harder to decipher.
- Think of a phrase or sentence meaningful to you and easy to remember. Then, take the first character from each word, alternate uppercase and lowercase and use some common letter-number substitutions.
- Avoid the use of personal information as part of your password. Do not use your name, your pet or child's name, 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.

You can never be sure who you are chatting with online. The friendly fellow movie fan or book lover in an online forum may actually be a clever criminal looking for his next cybercrime victim.

How can you have fun online while protecting yourself?

- 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 workplace or favorite hangout.
 - Names of clubs or organizations to which you belong.
 - Historical information that could identify your past residences.
- Do not use a nickname that can be used to identify you (for example, “CharlestonLawyer,” “CindyFromTulsa” or “KyWildcatMom”).
- Never share your account password.

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.

6 SOCIAL NETWORKING

Staying Safe Online

Fast friendships are forged over the Internet and there is no doubt that casual, online conversations sometimes are the foundation of good, lasting relationships. However, the anonymity of the Internet may compel some individuals to reveal too much about their private lives. If an online conversation makes you uncomfortable in any way, log off immediately. Remember that the rules of behavior that apply in person apply online, too.

- Consider how your e-mail message could 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 someone else.
- Do not forward another individual's e-mail without their permission.
- Never allow anyone to photograph you in an embarrassing or compromising situation.
- Never post anything that would cause you embarrassment or shame. You cannot control its duplication and it may be used against you.
- Do not send photographs of yourself or family members to Internet acquaintances. Photographs can be altered and forwarded. Elements in photographs — a landmark or a street name, for example — can be used to identify your location.
- Remember that, once posted, the information can be seen by anyone with a computer and an Internet connection: family and friends, employers or potential employers, admissions officers at schools you might like to attend — even police and other law enforcement authorities.

Be Smart, Be Safe: Meeting Someone You Met Online

Individuals misrepresent themselves online. Often the lies are small and harmless. But sometimes they are not. It is very easy for an individual with criminal intentions to mislead potential victims over the Internet.

Here are some basic safety tips:

- Speak by phone before agreeing to a meeting. Often, hearing an individual's voice and engaging in verbal conversation is very revealing.
- Learn as much as you can about the individual and verify that information.
- Meet in a public place. If your online friend is a trusted individual, he will understand and welcome your caution. If your plan for a public meeting is met with objections, immediately terminate further conversation.
- Never give out your address. Make arrangements to arrive separately.
- Take along a trusted friend or family member or make sure they know where you are going, who you are meeting and how long you will be gone. Check in with someone when you arrive and call when you are safely home.
- Watch your alcohol intake. Do not leave a drink unattended.
- Never leave with the individual. If you suspect you are being followed, drive to the nearest police station or public location for help.

Social Network Accounts After Death

There are services available to help your survivors manage your social network accounts after your death. Some allow survivors to delete, update, transfer or possibly preserve the account. As the number of abandoned accounts continues to grow, social network sites are establishing policies for the survivors of the deceased. Make sure your survivors are familiar with the social network sites in which you have an active account.

Document Storage

Consider storing your username, personal identification numbers (PINs) and passwords in a secure location away from your residence, such as a safe deposit box at a bank or a safe in your attorney's office. A key consideration is whether your executor will have convenient access to the documents in the event of your death. Since some states may restrict or limit access to a bank safe deposit box upon the death of the owner, you should consult your legal advisor or financial planning professional to determine the option which balances best security and access in order to achieve your planning purposes.

8 YOU, YOUR CHILDREN AND THE INTERNET

Protecting Your Children While They Are Online

As a parent, it is your responsibility to know what your children are doing online and guard them against the dangers that exist for unsuspecting minors. How can you do that?

- **Set parameters.** How many hours a day can they spend online? What sites can they visit? Are chat rooms OK or off-limits? What about interactive games? Set rules and enforce them.
- **Keep the family computer (or your child's computer) in a busy area.** Children, especially young children, should access the Internet where you can monitor them and monitor the sites they visit. Consider installing a software program that allows you to control their Web browsing. If your children have e-mail accounts, make sure you know their passwords and randomly check messages.
- **Educate yourself and your children.** Follow news reports and conduct research to find examples of Internet predators and other online risks. Remind your children that individuals they “meet” online are not always who or what they seem.
- **Encourage your children to talk to you.** Ask them to alert you if they encounter someone or something online that makes them uncomfortable. Remind them that you will not be angry; you love them and want to protect them from real danger.
- **Look for signs that your child might have been targeted by an online predator.** If your child is secretive, unusually quiet or spending too much time online, ask questions and be supportive.

Signs That Your Child Might Have Been Targeted By An Online Predator

- Uncharacteristic silence or withdrawal from the family.
- Turning off the monitor or reducing a Web page when you enter the room. If this is happening, log on to your child's computer and look for evidence of inappropriate sites. Ask for expert help, if necessary. "Google" your child's name to see if his personal information is on the Internet.
- Spending a lot of time online — especially at night, when most computer predators are online, too.
- Making or receiving telephone calls to or from unrecognized numbers.

Remember: Talk to your child if you suspect she is at risk and monitor access to electronic communications. It will be worth your time, because communication is the key to keeping children safe.

IF YOUR CHILD HAS BEEN TARGETED BY A PREDATOR

Immediately contact the appropriate law-enforcement authorities and the National Center for Missing & Exploited Children at www.cybertipline.com if your child has:

- Received pornography.
- Been solicited.
- Received explicit images from someone who knows he is a minor.

10 THE NEW FACE OF THE CHILDHOOD BULLY

INTERNET BULLYING, KNOWN AS CYBERBULLYING, OCCURS IN ALL COMMUNITIES AND AT ALL INCOME LEVELS.

Internet bullying, known as cyberbullying, occurs in all communities and at all income levels. Sometimes, the bully is someone your child knows from school. But the bully may be an individual your child has never met — perhaps someone she angered in a chat room or on a gaming Web site.

Cyberbullying can be more harmful and frightening than schoolyard bullying, because it is very public. The bully spreads hurtful comments or innuendo to many individuals via the Internet and others may join in.

If you suspect your child is the victim of a cyberbully:

- Use the block feature to block the sender's e-mail or instant messaging (IM) account.
- Go online yourself to warn the bully that if the behavior does not stop, you will inform his parents, the Internet service provider (ISP) and the appropriate law-enforcement authorities.
- Save every communication from the bully.
- Urge your child to stay offline, if necessary.
- Seek legal guidance, if warranted.
- If your child continues to receive harassing e-mails, delete your child's current account and open a new one.
- Only give the new e-mail address to individuals you and your child trust.

Mobile devices allow you to use the Internet wherever you are, without a computer. While on-the-go, you can network, gather 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, like your personal computer, your mobile device can 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 another individual'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.

Guard Your Mobile Device

- Be as careful with your mobile device as you are with your wallet or purse.
- Keep your mobile device out of sight in your pocket or purse when not in use.
- Do not store unnecessary data in your mobile device — only data to which you need quick and frequent access. Never store sensitive information such as bank account numbers or Social Security numbers on your mobile device.
- 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 locks your mobile device after a specified period of inactivity.
- Activate the encryption feature, if available, to protect data and prevent others from accessing your personal information.

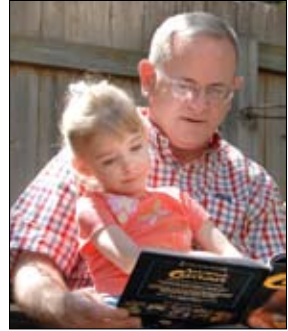
If Your Device Is Lost Or Stolen

- Contact your service provider immediately. Service agreements usually detail the steps to take in case of loss or theft.
- You can remotely track, erase or deactivate any lost or stolen device if you have equipped it with antitheft tools.
- File a police report. You will need to provide the name of your service provider and the make, model and Electronic Serial Number (ESN) of your mobile device.
- Notify the individuals on your contact list that their information may be compromised.
- Contact your credit card company if your mobile service is paid for using a credit card. You may be protected from paying for fraudulent calls.
- Place alerts on your credit report to prevent thieves from creating fraudulent accounts using information stored in your mobile device.

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.

RESOURCES



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

INTERNET SAFETY FOR TEENS
(#573)

CYBERSECURITY (#575)

MAKING YOUR HOME A SAFER PLACE (#531)

PROTECTING YOUR IDENTITY AND PERSONAL INFORMATION
(#520)

MANAGING CREDIT AND DEBT
(#501)

MANAGING YOUR PERSONAL RECORDS (#506)

RETIREMENT PLANNING IN YOUR 20s AND 30s (#516)

INSTALLING CHILD SAFETY SEATS (#544)

KEEPING YOUR CHILD SAFE
(#549)

HELPING CHILDREN DEVELOP HEALTHY HABITS (#547)

BALANCING FAMILY AND CAREER (#529)

FAMILY VALUES: BUILDING A LEGACY (#562)

PARENTING A TEEN (#515)

SUICIDE PREVENTION (#581)

FINANCING COLLEGE (#513)

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.

