Office of the Attorney General

Internet Safety

LAWRENCE WASDEN
Attorney General
700 West Jefferson Street
Boise, ID 83720-0010
www.ag.idaho.gov

State of Idaho
Office of Attorney General
Lawrence Wasden

Dear Fellow Idahoan:

The Internet is an exciting tool that puts vast amounts of information at your fingertips. With the click of a mouse, you can buy airline tickets, use research tools, chat with friends or play interactive games.

But there are also risks on the Internet, so it's important to be cyber-smart and make your experience online a safe one. It is critically important that parents supervise their children's Internet use. As we've seen all too often, trusting children are particularly vulnerable to sexual predators and other cyber-criminals.

When you go online, keep in mind your family's personal and financial safety, security and privacy. You should also take a cautious approach to online "business opportunities" and be wary of Internet scams and computer viruses.

My office has prepared this publication to help you safely enjoy the Internet. I hope you find it helpful.

LAWRENCE G. WASDEN
Attorney General

Table of Contents

CONSUMER SAFETY

SAFETY AND SECURITY

The Internet has opened a new world for many people. Information, communication and shopping at distant retail outlets are readily available. Yet there are serious risks associated with e-mail, social networking, browsing, and doing business online.

One of the greatest risks is that the Internet is an anonymous place with no face-to-face contact. Thieves and predators take advantage of this anonymity and pretend to be someone other than they really are.

These tips can help ensure your safety on the Internet.

SHOPPING ONLINE

Use a secure browser

A browser is the software you use to explore the Internet. Your browser should comply with industry security standards, such as Secure Electronic Transaction (SET). These standards encrypt or scramble the purchase information you send over the Internet, ensuring the security of your transaction. Most computers come with a secure browser already installed. It is very important that you always use the most current version of your browser and that you regularly check for software and security updates.

If you do not have a secure browser, there are many to choose from. The two most common browsers are Microsoft Internet Explorer and Mozilla Firefox. Both are available free on the Internet.

When shopping online, it is also very important that you are buying from a secure web site. See the section on "Site Security" for more information.

Shop with companies you know

Anyone can set up a business under almost any name on the Internet. If you are not familiar with a business, look for a physical address, a phone number and an e-mail address. Contact the business and ask for a brochure or catalog of merchandise and services. Request a copy of the business's refund and return policy. Contact the Better Business Bureau and the Consumer Protection Agency in the business's home state to find out what kind of track record the business has. Check with the Secretary of State to see if the business is registered. If you are purchasing an item from an Internet auction, check the seller's feedback rating.

Before you make a purchase, make sure that you know what you are paying for. Review the description, price information, and any limitations on purchases (for example, goods may not be available for delivery outside of the country; there may be minimum quantities that must be ordered; etc.) If possible, compare the description to an actual physical model of the same item.

Review the fine print and look for words such as "refurbished," "close-out," "second," "discontinued" or "off-brand."

Check whether the price is listed in U.S. dollars or another currency. Review the requirements for taxes or duty on purchases, as well as postage costs and shipping and handling charges.

Review the company's privacy policy. The policy should state what information is collected, how it will be used, and whether the information will be shared with others.

If you have questions about the item or any of the charges or policies, e-mail or phone the seller.

Be wary of "free trial" offers. By requesting the trial sample, you may be entering into a long-term commitment, including monthly shipments of additional product and automatic charges to your account. Don't provide your credit card or bank account information to receive a "free trial" sample. If it's truly a free offer, the business does not need your account information.

Internet auction sites

Shopping on an auction site does not automatically protect you from fraud. In fact, some auction sites may be wholly fraudulent. Shop only on sites that you know or can verify are legitimate.

When shopping on an auction site, you should always understand and follow the site's guidelines. Going outside the site to pay for a purchase puts you at great risk of fraud and loss of money. Some sellers or buyers will offer to deal with you directly through your e-mail, for example, claiming that your bid won a "second chance" offer. This is a tactic often used by scammers as an attempt to lure you away from the site's protection guarantees.

Be especially cautious of buyers and sellers outside of the United States. Much of the fraud reported on these sites occurs with foreign transactions. If you lose money in an Internet scam, you will have practically no chance of getting it back, especially if the seller is in a different country.

If you have a dispute with an auction site purchase, contact the seller through the auction site's system. Don't communicate "off-site" or by direct e-mail. If you are not satisfied with the seller's response, use the auction site's dispute process. Be sure to act within the site's allowed timeframe. Don't let the seller delay until the dispute deadline has passed. If you pay with a credit card, you may be able to dispute charges with your credit card company.

Keep a paper copy of your purchase

When you order something over the Internet, keep a printed copy of your purchase order, receipt, or confirmation number. A paper record will help resolve problems with your purchase.

If you pay by credit card, your transaction is protected under the Fair Credit Billing Act. This federal law gives consumers the right to dispute charges under certain circumstances and to temporarily withhold payment on the disputed charges while an investigation is done. If you pay by debit card, there are protections for unauthorized payments under the federal Electronic Fund Transfer Act. For more information on these laws, contact the Attorney General's Consumer Protection Division.

If you are purchasing an item from an Internet auction and the seller does not accept credit cards, consider using an escrow service. If the seller only accepts cashier's checks or money orders, decide whether you are willing to take the risk of sending your money before you receive the product. Be sure to take steps to protect your privacy. Do not give out personal and sensitive information such as your Social Security number, driver's license number or bank account number.

The federal Mail or Telephone Order Merchandise Rule also covers purchases made over the Internet. Unless otherwise indicated, this rule requires that the merchandise must be delivered within 30 days. The company must notify you if the merchandise cannot be delivered within that time frame.

PASSWORDS

Many websites require you to register and create a password for future access. When creating a password, the National Crime Prevention Council suggests you mix numbers with upper and lowercase letters, or use a word that is not found in the dictionary. Avoid using personally identifiable information such as your phone number, birth date, or a portion of your Social Security number.

It is also a good idea to use a different password for each Internet site you use.

Keep your passwords in a secure place. Do not have your computer "remember" your passwords unless you are the only person with access to your computer.

E-MAIL

The major difference between e-mail and the old fashioned kind of mail is privacy. Think of e-mail as a postcard rather than a sealed letter. Your e-mail can be intercepted, either intentionally or unintentionally, at many points along its path. So while e-mail is a great way to stay in touch, it might not be a great way to send confidential information.

Criminals are increasingly using e-mail as a tool for fraud. Some of the common scams include:

- advance fee scams,
- "phishing" or verification scams, and

- international lottery scams.

Advance Fee Scams

Advance fee scams include requests for your personal bank account information or asking you to pay an advance fee for taxes, attorney fees, and other transactional costs in order to receive a benefit or money. Common advance fee scams include:

- disbursement of money from wills,
- contract fraud,
- real estate transactions,
- conversion of currency,
- transfer of funds,
- sale of crude oil at below market prices and
- monetary prize awards.

One common example is the "Nigerian Money Scam." In this scam, you'll receive an urgent request to help someone get his or her money out of Nigeria (or another country). You may receive official looking documents to support the request, stating that it is from an official representing a foreign government or agency. These requests may appear to be personally addressed to you, but in fact they are sent out in mass mailings or transmissions. They'll offer you a large amount of money if they can move the money through your bank account. Of course, they'll ask for your account number. If they get it, they will empty the account. They may also ask you to pay in advance for taxes, attorney fees, and other transactional costs in order to "transfer" the money into your account.

If you receive e-mails (or faxes or letters) similar to these scams:

1. Do not respond
2. Destroy the e-mail, fax or letter.
3. If you have become a victim of this scam, that is, if you have provided your bank account number or other personally identifying information or if you have lost money, notify the closest field office of the United States Secret Service. The Idaho field office can be reached at (208) 334-1403.

Another example of advance fee scams involves overpayment for a purchase. You may become a target of this scam if you are selling an item over the Internet. The "purchaser" will "mistakenly" send you a certified or cashier's check for more than the purchase price and ask you to send back the difference. The problem is that the check the "purchaser" sends you is counterfeit. You will lose the money you sent back and the amount of the counterfeit check.

To avoid being victim to an overpayment scam, you should:

1. Confirm the buyer's name, address and telephone number.
2. Refuse to accept a check for more than your selling price. If the buyer sends a check over the amount due, return the check and ask for a check in the correct amount. Do not send the merchandise until you receive the correct amount. Do not wire money back to the buyer.
3. Consider an alternative source of payment such as an escrow service or online payment service. Be sure to verify that the escrow service or online payment

service is legitimate by reviewing its website; reviewing its policies and terms and conditions; calling its customer service line; and checking with the Better Business Bureau or the Attorney General's Consumer Protection Division to see if there are complaints against the service.

"Phishing" or Verification Scams

If you are a target of this scam, you will receive an e-mail, pop-up message or text message on your cell phone that appears to be from a trusted company. These e-mails and messages often contain color graphics and look just like the company's Internet site.

The e-mail or message will indicate that the company needs to verify information for its records and will ask you to provide (or go to a website to provide) your credit card number, automatic teller PIN number, Social Security number and/or other confidential information. This scam is also known as "phishing."

The Attorney General's Office has seen fraudulent e-mails and text messages that appear to be from well-known companies including PayPal, E-Bay, major credit card companies and community banks. These e-mails are fraudulent. They are not from these companies. The sender is trying to get information that can be used to steal your identity or your money.

The companies with whom you do business already have the information they need. Legitimate companies will not contact you by e-mail or text message to verify information you have already provided.

If you receive e-mails (or faxes, letters, text messages or phone calls) similar to this scam, you should:

1. Never provide the information requested.
2. Find the e-mail address of the real company and forward the e-mail to the company's security or fraud department. Or, you can call the company using a telephone number you know to be genuine.
3. Delete the e-mail or text message. Do not click on any link in a suspicious e-mail. Log on to your website accounts by opening a new browser window and typing the URL website address you know to be correct directly into the address bar. Do not "copy and paste" the URL link from the message into your address bar.
4. Only use secure websites to submit sensitive or personal information. Look for the lock  or key  icon at the bottom of your browser and a URL with an address that begins with "https."
5. Review credit card and bank account statements regularly to determine whether there are any unauthorized charges.
6. Maintain up-to-date anti-virus software. Some phishing e-mails contain viruses. Consider installing firewall protection.

You can report phishing to the Federal Trade Commission (FTC). Forward the e-mail to spam@uce.gov. This information is used for law enforcement purposes against people who send deceptive emails. If you believe that you have been injured (lost money, had your identity stolen, etc.) by phishing, you can file a complaint with the FTC at www.ftccomplaintassistant.gov.

International Lottery Scams

International lottery scams use e-mail, direct mail and the

telephone to entice you to purchase chances in international lotteries. When you send money to purchase a lottery ticket, many scam operators do not buy the promised tickets. Instead, they simply keep the money for themselves. Other operators will buy some tickets and keep any winnings for themselves. Operators will often make unauthorized withdrawals from your bank account or make unauthorized charges to your credit card.

If you purchase a ticket from one of these scam operators, there's a good chance they will put your name on a list of potential victims and sell it to fraudulent telemarketers and other scammers who will try to sell you other bogus offers for lottery and "investment opportunities."

If you receive a solicitation to purchase international lottery tickets:

1. Do not respond to the solicitation.
2. If the solicitation is by telephone, file a complaint with the Attorney General's Consumer Protection Division.
3. If the solicitation is by direct mail, give the letter to your local postmaster.
4. If the solicitation is by e-mail, delete the e-mail.

"Spam"

"Spam" is the e-mail version of junk mail: unwanted e-mail messages from people you do not know seeking to sell you a product or service. Spammers get your e-mail from places such as websites, chat rooms, membership directories, and newsgroup postings.

To reduce the amount of spam you receive, you should:

1. Consider having two e-mail addresses. One e-mail address can be used for personal messages and the other address can be used for newsgroups and other purposes. Or, one address can be used as your "permanent" e-mail address and the other can be considered "disposable."
2. Review privacy policies before submitting your e-mail address to a website. Some websites will allow you to "opt out" of receiving offers or e-mails from another business or having your address sold to another business.
3. Use an e-mail filter. Your e-mail account may have a tool to filter out potential spam or a method of channeling spam into a bulk e-mail folder.

The Federal "CAN-SPAM" Act of 2003 requires spammers to allow you to "opt out" from receiving future e-mails. Many people, however, report that they receive additional e-mails from other spammers after they ask to be removed from one spammer's list. You can report spammers that do not honor your "opt out" request to the Federal Trade Commission (FTC) by filling out a complaint form at www.ftccomplaintassistant.gov.

You can also forward unwanted or deceptive messages to the FTC at spam@uce.gov or complain to the spammer's Internet service provider. This information is used for law enforcement purposes against people who send deceptive emails. Be sure to include a copy of the message and header information and state that you are complaining about spam.

PRIVACY

Some Internet sites may share information about you with affiliates. They may also sell your personal information. Before you provide information to an Internet site, decide

what personal information you want to keep private and what information you are willing to have released.

If you are concerned about privacy, consider these tips.

Personal information

Never give out your Social Security or driver's license numbers over the Internet.

Do not disclose other personal information such as your address, telephone number, or e-mail address, unless you have researched a company's privacy policy and know the company has a good reputation. Even then, find out exactly what information is being collected and how the company will use it. Many companies are joined with other affiliates or partners that have full access to their customer files.

Teach your children not to give out personal or family information online.

Privacy policies

Many companies post their privacy policy on their Internet site. If you are unable to locate a company's privacy policy, send an e-mail or written request for a copy.

Read the policy carefully before you give a site your personal information. Check to see if the company will transfer the personal information you provide to affiliates or other businesses or organizations.

Site security

Before conducting any transactions online, verify that the company's website is secure. A secure website means the company has taken precautions to ensure that others cannot intercept information. You will always see a padlock  or

key  icon in the lower corner of the screen when a site is secure.

Make sure your browser has the most up-to-date encryption capabilities. Also, look for the phrase "https:" in the URL.

Cookies

"Cookies" are pieces of data an Internet site places on the hard drive of your computer. Cookies originate from the sites you visit. In effect, cookies record your digital comings and goings.

Cookies can only be read by the web server that originated the cookie. Other web servers cannot intercept cookies.

Cookies perform many functions, including serving as navigational tools or as a means for searching the Internet. Cookies also keep track of goods you intend to purchase but set aside while you finish shopping a website. Cookies can collect and transfer a great deal of information about you and your interests every time you go online — even when you don't go to the checkout or log off.

Most browsers allow you to block cookies or prompt you before a cookie is downloaded to your computer. However, by disallowing cookies, you may reduce or even eliminate your browsing options in many websites.

Visit www.cookiecentral.com for more information about cookies, including how to remove cookies from your browser completely.

Pharming

"Pharming" involves the redirection of an Internet user from a legitimate commercial website to a bogus website. "Pharmers" set up bogus sites and shuttle users from

legitimate websites by altering the domain name system or transmitting a virus.

The bogus website will look the same as the legitimate website. When you enter your login name or identification and password, "pharmers" obtain the information for their own use. This can occur even when you type the correct URL.

You can take steps to avoid being a victim of pharming.

1. Maintain up-to-date antivirus software.
2. Consider installing anti-spyware software and firewalls.
3. Be careful when entering personal or sensitive information into a website. Be sure to look for the lock  or key  icon at the bottom of your browser.
4. Review websites closely. If the website has changed since your last visit, be suspicious. If you have any doubt about the website, do not use it.

Spyware

Spyware is software that is installed on your computer without your consent. Spyware monitors or controls your computer use without your knowledge. It is also called "adware." Spyware is often used to send you pop-up advertisements, direct you to certain websites, monitor your Internet surfing, and even to record your keystrokes. Spyware can lead to identity theft.

Indications that spyware may have been installed on your computer include: numerous pop-up advertisements; a browser that takes you to sites other than those that you typed into the address bar; sudden or repeated change in your

home page; new or unexpected toolbars or icons at the bottom of your computer screen; keys that no longer work; random error messages; or slow performance when opening programs or saving files.

To prevent the installation of spyware:

1. Keep your operating system and browser software up-to-date.
2. Do not download software from sites you do not know and trust.
3. Do not install software without knowing exactly what it is. Read the end-user license agreement before you install software.
4. Set your browser security setting to a high level and keep it updated.
5. Do not click on links within pop-up windows. Close pop-up windows only by clicking the "x" icon in the title bar.
6. Do not click on links in spam or pop-up boxes that offer "anti-spyware" software. Many of these are fraudulent and actually install spyware onto your computer.
7. Consider installing a firewall.

ONLINE BUSINESS OPPORTUNITIES

The Internet also offers many business opportunities. If you find one that interests you, be sure to thoroughly investigate the company before you sign up.

The Federal Trade Commission (FTC) offers the following tips.

- Understand that seminar "consultants" are often in business to sell you a business opportunity rather than to teach you Internet basics. In some cases, they may seek to exploit your lack of experience with computers or the Internet.
- Investigate all earnings claims. Talk to others who have purchased the opportunity to see whether their experience supports the company's claims.
- Demand to see the company's claims and promises in writing.
- Ask for a disclosure document. The FTC Franchise Rule requires most business opportunities to provide a disclosure document. The disclosure document should contain detailed information to help you compare one business with another.
- Contact your local Better Business Bureau and/or the consumer protection agency in the state where the business is located. Ask if complaints have been filed against the business.

Internet Business Scams

Consumers have complained about some of the following items relating to the Internet:

- Auctions: You receive an item that is not what was represented, less valuable than promised, or you receive nothing at all. Sometimes sellers fail to deliver in a timely manner or fail to disclose all the relevant information about the product or terms of sale.
- Internet access services: You cash a check you received from a business and are then locked into a long-term contract for Internet access or another web

service, with penalties for cancellation or early termination.

- Work at home offers: You are offered the chance to earn "big bucks" by working at home or starting a new business. In fact, you will work many hours without pay and you may have to pay costs up front.
- Advance fee loans: You are offered loans for a fee, regardless of your past credit history. These offers are often a way to collect money without providing legitimate loans.
- General merchandise sales: You do not receive the merchandise, it is not the value or quality promised or you are charged extra fees.
- Travel Offers: You are offered luxury trips at bargain prices and receive lower quality accommodations and services or none at all, or you are charged extra fees.
- Pyramids, multilevel marketing and chain letters: You are offered the chance to make money through selling products and services and bringing others into the program. Neither you nor the people who brought you into the program make any money. Many of these programs are illegal.
- Weight loss claims: You are offered a "miracle" treatment, but instead are sold worthless or sometimes even dangerous products.
- Credit repair offers: You are offered the chance to erase accurate negative information from your credit records. These offers are false.
- Home Foreclosure Rescue offers: You are offered the chance to save your home from foreclosure by paying an upfront fee. Many of these companies take your fee and do not provide any loan modification or

provide any services to save your home from foreclosure.

- Adult entertainment offers: You are offered the chance to view adult images "free" if you share your credit card number to prove you are over 18 years of age. Or, you are offered "free" access to adult material by downloading a viewer or dialer computer program. You should expect to have charges placed on your credit card. You may later receive international long distance charges on your phone bill for international modem dialing.
- Web cramming: You are offered a free website for a trial period, and are later charged on your phone bill or receive invoices for the websites.
- Investment opportunities: You will be offered a "ground floor opportunity" or promised big profits in a short time. You will be charged advance fees or receive no legitimate investment at all. Be wary of investments that state that they are "IRS approved" or are tax-free and confidential.

COMPUTER VIRUSES

What is a virus?

A virus is a file or program planted in your computer without your knowledge. Its purpose is to damage files and disrupt your computer.

How does a computer get a virus?

Most viruses are spread by file attachments sent through e-mail or on a CD, DVD or removable media. When you use an infected file on your computer, the virus copies itself onto your hard drive. Some viruses strike and cause problems immediately. Others remain inactive until a specific

program is used or until a certain date occurs.

Viruses spread very rapidly. If you find that your computer has been infected, you should assume that every file and computer that you have used is also infected. Failure to scan and disinfect every disk and computer will almost guarantee that the virus will re-infect your computer or network.

How do you remove a virus?

Typically, viruses can be removed only by using anti-virus software or by re-formatting the infected hard drive. If you suspect that your computer is infected with a virus, you will need to research anti-virus software and purchase the appropriate package. Some popular brand names include Norton, McAfee and Kapersky.

Once your anti-virus software is installed, there are options to restore or repair damaged information and remove any harmful files that were saved to your computer. There is a chance, however, that you may have lost data that cannot be retrieved. You can reduce this risk by frequently making "back ups" of your personal data.

Preventive Maintenance

- Make sure that all computers have anti-virus software installed and running.
- Update your virus definition files from the anti-virus software manufacturer's website at least once a week.
- Scan e-mail attachments before you open them and scan removable media before you allow them on your computer. Do not download files sent to you by people you do not know.
- "Back up" your personal data frequently and on a regular schedule. Make backups on CD or DVD, an

external hard drive or other removable storage media, not on your main hard drive.

CHILD SAFETY

ONLINE DANGERS TO CHILDREN - INTRODUCTION

Just a few years ago "going online" meant sitting down at a desktop computer and getting on the Internet. Today, we have wireless laptops, cell phones with Internet, photo and texting capability, Blackberries and similar devices. Even gaming systems such as PlayStation, Xbox and Wii connect people in distant places with interactive text, voice and video communication. Online safety isn't limited to computers anymore!

For all of its benefits, the online world can pose significant dangers to children.

These risks generally fall into three categories:

1. Sexual victimization
2. Exposure to pornography and/or violence
3. Cyberbullying

Sexual Victimization

Because of their trusting nature, children are particularly vulnerable in Internet "chat rooms" and social networking sites. Child predators know this and often pose as children in order to gain the trust and confidence of a potential victim.

There have been many cases in Idaho in which a child has been lured to meet with an "online friend" who turns out to be an adult and a sex offender.

It is dangerous for children to put personally identifying information on the Internet, because a sexual predator can use this information to identify and locate a child to victimize. This includes photographs, name, address, age, school, extra-curricular activities, parents' names and occupations and any other information a predator could use to identify and locate a child.

The anonymous nature of the Internet adds to its danger for kids. People can pretend to be anyone online and you can almost never be certain that the person you are communicating with is really who he says he is.

Sexual predators will try to establish communication with a potential victim through e-mail, chat rooms, social networking sites, text messages and even video games. Predators hide their true identity, often pretending to be a sympathetic adult who "understands" the child's problems. Sometimes they will lead children to believe that they are communicating with another kid. They use these tactics to establish a relationship of trust with the potential victim, a process known as "grooming." Once trust is established, the predator attempts to meet the child in person. The child no longer thinks of the predator as a stranger, but rather as a friend who understands and cares about the child's problems, someone the child is willing to meet in person.

Exposure to Pornography

Sometimes you can run across online pornography accidentally. It can be attached to an e-mail or a pop-up or even sent to your cell phone. Some pornographers deliberately use web site names similar to sites kids are likely to visit while doing homework. Although it was shut down years ago, there was once a pornographic website

called "whitehouse.com[1]." The real White House website is "whitehouse.gov."

Exposure to pornography is not just limited to computers. Pornography can be downloaded and watched on any online device, such as cell phones and iPods. It's important for parents to know what content their kids have on mobile devices.

Cyberbullying

According to the National Crime Prevention Council, almost half of all American teens have been the victim of cyberbullying. Cyberbullying happens when teens use the Internet, cell phones, or other digital devices to send or post messages or images that are intended to hurt, humiliate or embarrass another person.

There are laws in Idaho that protect victims of harassment, intimidation, and bullying. If you feel that your child is the target of cyberbullying, talk to your school counselor or resource officer immediately. Cyberbullying can have very serious effects on your child, leading to withdrawal, depression and even suicide.

Red Flags for Parents

Here are some warning signs that your child is headed for trouble online. If you notice any of these behaviors, you should talk to your child about them.

- Your child changes or minimizes the computer screen when you walk into the room.
- Your child starts spending a lot more time online.

[1] The current Internet address whitehouse.com is not connected with the former pornographic website.

- Your child starts getting phone calls from people you don't know.
- Your child has new clothes, CDs or other items from unknown sources.
- Your child gets overly upset if Internet access is restricted or unavailable for even a short time.
- Your child is unusually withdrawn or non-communicative.

The Idaho Internet Crimes Against Children Task Force

The Idaho Internet Crimes Against Children (ICAC) Task Force is a statewide coalition of local, state and federal law enforcement and prosecution agencies, focused on apprehending and prosecuting individuals who use the Internet to criminally exploit children.

Internet crimes against children are, primarily, crimes of sexual exploitation of children. These crimes include distribution of child pornography and using the Internet to target children for sexual abuse.

The Idaho ICAC Task Force is committed to protecting Idaho's children through community education and by identifying, arresting and prosecuting those who commit Internet crimes against children. For more information, visit www.icacidaho.org.

Report Internet Crimes Against Children

You can help in the fight against child exploitation by reporting information that you think will be useful. You can contact us through the National CyberTipline at www.cybertipline.com or by calling, toll-free (800) 843-5678.

The information you provide will be forwarded to the appropriate ICAC law enforcement agencies in Idaho or elsewhere in the United States.

General Computer Safety Guidelines

- Be actively involved in your kids' Internet use. Teach them to tell you if they encounter anything that makes them feel uncomfortable, confuses them or is pornographic.
- Communicate. Talk to your child about the potential hazards of the Internet. Regularly have them show you the websites they visit. Get to know their online friends just as you would their regular friends.
- Report inappropriate online activity. Notify your local police or sheriff immediately if an online contact tries to set up a meeting with your child. You should also report this through the National CyberTipline at www.cybertipline.com or by calling, toll-free (800) 843-5678.
- Set limits. The Family Contract for Internet Safety is a good starting point. You can print it from the ProtecTeens DVD or the Attorney General's website. Review it with your kids, sign it together and post it near the computer, where your kids will be reminded of the rules you've agreed to every time they go online.
- Monitor kids' Internet use. Get to know the web sites your kids visit. Check the web browser history files and cache and decide if the sites are suitable for your children.
- Maintain access to your children's accounts and randomly check e-mail and any social networking sites your child visits. If they chat or instant

message, make sure you know to whom they're chatting. Check their buddy lists and chat logs.

- Locate online computers in a common area of the home, where you can frequently observe the monitor to see what is being viewed. Children should not have online computers in their bedroom.
- Learn about and use parental control software. You can use it to block inappropriate web sites, limit the amount of time spent on the Internet, and monitor online activity. You will find more information about parental control software on the ProtecTeens DVD and on the Attorney General's web site.
- Discuss the anonymous nature of the Internet with your children. Make sure they understand that anyone can pretend to be anyone online and the people they meet online may not be who they say they are. Teach them to only talk online to people they really know offline.
- Teach kids to protect their true identity online. For example, kids should not draw attention to the fact that they are kids. It's a bad idea to use a screen name that suggests your age, such as "Jessica14." Personal information can be used for identity theft. Identity thieves often target kids because the crime may not be discovered until years later, when the child identity theft victim grows up and tries to buy a car or get a credit card. Social Security number, bank account numbers, credit or debit card numbers or date of birth or physical address should never be given to anyone you meet online. Do not respond to e-mails or other messages that ask for this kind of information. Just delete them.
- Teach kids that the Internet is the most public place in the world. If you post a picture, anyone can see it

and you can never take it back. Even if you post on a secure site, it can be copied and e-mailed or posted on another site. Predators may look for pictures of kids they find attractive and then try to locate those kids. Even pictures on news sites, family sites, school sites and club sites can be misused to harm kids.

- Talk to your teens about "sexting," the practice of sending suggestive or naked pictures to friends by cell phone. Make sure they understand that once they send the picture, they've lost control of it and can never get it back. The person they sent it to can send it to other people. These pictures can end up on the Internet and cause major problems years later, when it's time to get a job or get into college. These pictures can also cause problems today. Other kids could use these pictures to gossip about or bully your child. A child who sends or possesses these pictures can be prosecuted for child pornography and be required to register as a sex offender for life.

- Secure your wireless networks. People outside of your home can access the Internet through unprotected wireless networks. They can download pornography, target a child or commit other Internet crimes. If the criminal is apprehended, it will appear that your computer was used for these crimes. If you install a wireless network, be sure to password protect access to the network using wireless encryption methods such as WEP, WPA or WPA2. When available, check the "encrypt" box for additional protection. For more information on how to secure a wireless network, visit www.icacidaho.org or contact your Internet service provider.

CHAT PROGRAMS/ INSTANT MESSAGING/CELL PHONES

Chat Rooms

Chat rooms are Internet sites people use for conversation. Chat rooms can be a dangerous place for kids. The conversations are "live" or "real-time," meaning the communication is instantaneous. The danger in a chat room is that the person with whom you are chatting may or may not be truthful about his or her identity. The conversations can be sexually offensive and violent. Do not allow your children to use chat rooms. Even seemingly safe "kids" chat rooms can be dangerous.

Instant Messaging

Instant messaging, also known as IMing, is a common form of person-to-person instant communication. It is one method predators can use to communicate with children. MS Messenger is a popular instant messaging program. Yahoo, Google and other browsers also have messaging programs, as do most social networking websites, such as Facebook and MySpace.

Many instant messaging programs have "online buddy locators," which means you can be alerted to the fact that one of your buddies has come online. Predators can have many online buddy locators. All they have to do is sit and wait for a certain child to come online.

Many instant messaging programs can also transfer files, including photographs, sound and video files. Video chat and voice chat can also be done through instant messaging programs. Predators usually use text chat in order to hide their age and appear to be another kid.

Instant messaging programs also allow you to carry on multiple conversations simultaneously. Predators often do this to weed out unreceptive kids and find a child that can be groomed for a sexual relationship.

Cell Phones and Text Messaging

Kids love to use cell phones to send and receive text messages. Cell phones can also send and receive pictures, video and other files.

Once a predator establishes contact with a child, he can use text messages to communicate. The child can be in school, with friends or anywhere away from their parents. The predator can also call and talk to the child. Teach children to never give their cell phone number to anyone that they do not know in the real world.

Online communication has its own shorthand language. This is used in e-mail and text messages to save time and keystrokes. It also keeps "outsiders" from understanding what the messages say.

Sexting

"Sexting" is the practice of sending nude or partially nude photos of yourself by cell phone. It is very popular among the kids. It happens every day in Idaho, every day in our schools. Typically, it's girls taking pictures of themselves with their cell phone and sending the pictures to somebody else, often a boyfriend.

In 2008, a survey for The National Campaign to Prevent Teen and Unwanted Pregnancy, found that 22% of teen girls and 18% of teen boys had sent or posted nude or partially nude photos of themselves. 11% of young teen girls (13 – 16 years old) admitted having done this.

Part of the problem is that once you send the picture on the cell phone, you've lost control of it. The person you sent it to can send it to other people. These pictures often end up on the Internet, causing problems years later when it is time to get a job or get into college. Some kids have lost scholarships when a college has done a background check and found these pictures online.

In some cases, sexting can be a felony crime. Sending naked pictures or keeping naked pictures of anyone under the age of 18 can be prosecuted as child pornography. A child who does so could go to jail. Some kids have been prosecuted for sending or possessing pictures they thought were a joke.

Tips for Teens

- Think about the consequences of taking, sending, or forwarding a sexual picture of someone underage, even if it's of you. You could get kicked off of sports teams, face humiliation, lose educational opportunities, and even get in trouble with the law.
- Never take pictures of yourself that you wouldn't want to see on the school bulletin board or your family's refrigerator.
- Before hitting send, remember that you can't control where this picture may travel. What you send to a boyfriend or girlfriend could easily end up with their friends.
- If' you forward a sexual picture of someone underage, you are as responsible for this image as the original sender. You could face child pornography charges, go to jail, and have to register as a sex offender.

- Report any nude pictures you receive on your cell phone or computer to an adult you trust. Do not delete the message. Instead, turn off your phone and get your parents, teachers, and school counselors or law enforcement involved immediately.

Tips for Parents

- Talk to your children. Establish rules for phone use.
- If your children do not need texting, shut off the texting service.
- Limit your children's time with the phone. If they do not need a phone, don't give them one.
- There have been many instances in which children are up all night texting on their phone. This is a good time to secure the phone on a charger.

SOCIAL NETWORKING SITES

Overview

On social networking websites, individuals create personal web pages called "profiles" to communicate with others online. Facebook, MySpace, MocoSpace and YouTube are among the most popular with teens.

Anyone with access to the Internet can create a profile on a social networking site. Once a person creates a profile, that person (or "member") can post personal information, photos and "blogs" on the profile for others to read. Members link their profiles through networks of "friends," view each other's profiles, share photos and post comments. Unfortunately, sexual predators use social networking websites to meet and groom victims online.

ONLINE GAMING AND VIRTUAL WORLDS

Online Gaming Systems

Most of the newest video gaming systems (e.g., Wii, PS3, Xbox, etc.) have the ability to connect to the Internet for interactive game play. These new video game systems allow players anywhere in the world to connect and compete against each using many popular games. Once connected, they can communicate with one another by using gaming chat rooms. Several systems also have the ability to add webcams and headsets, allowing players to talk to and see other players. It is all part of the "live, interactive" gaming experience. Unfortunately, this technology gives predators an opportunity to see and talk to your child. A predator could try to get the child to undress, or pick out a child he finds attractive for later abduction.

Online gaming systems have many parental controls that allow parents to set options for their children's online play. You can learn more by reading the operator manual that comes with the gaming system, checking the gaming system menus or visiting the gaming system manufacturer's website.

Gaming Websites

Some gaming websites offer "monitored chat" gaming. This can provide a false sense of security. Don't trust it. Do you know who the monitors are? Are you willing to let them look out for the safety of your child? Monitored chat can quickly lead to unmonitored chat, e.g. an exchange of e-mail addresses.

Safe Online Gaming Tips

- View game ratings and prescreen games online before purchasing.

- Check to see if the console comes with parental control features.
- Set parental controls before children start playing.
- Set up game consoles in a common area of the home where adults can monitor activity.
- Decide if you want to use the console's Internet capabilities.
- Set gaming rules with your children, such as how long and with whom they can play.
- Help your children select gender-neutral, age-appropriate screen names.
- Decide if you want to allow voice chat. If you do, use voice masking features.
- Teach your children not to reveal personal information through voice chat.
- Encourage them not to respond to cyber bullies and to block unwanted contact.

Virtual Worlds

Virtual worlds are growing in popularity on the Internet. Second Life is one of the most popular.

In a virtual world, you create your own person, a representation of yourself called an avatar. Your avatar can be whoever you want it to be or do whatever you want it to do. You can even create an avatar that flies.

Second Life has its own money, called the Linden dollar. To have a fulfilling second life, you need money to buy property, build a house, purchase things and participate in activities.

You can do things on Second Life to get money or you can buy Second Life money in the real world, for example you can actually purchase Linden Dollars on EBay. That money has a direct correlation to the U.S. dollar.

In Second Life, you can buy something called "Capture Scent." If your avatar comes across another avatar's Capture Scent, it will render your avatar unconscious for ten minutes and the other avatar can do whatever it wants to your avatar.

There are also sexual scenes, with avatars engaging in sexual activity.

People can embed videos or pictures anywhere throughout Second Life. So if a child is visiting somebody's house in Second Life, he could be watching pornography.

Virtual Worlds like Second Life are no place for kids.

CYBERBULLYING

Cyberbullying happens when kids use the Internet, cell phones, or other digital devices to send or post messages or images that are intended to hurt, humiliate or embarrass another person. Many teens are harassed when someone steals their password or other personal information and sends damaging messages from their email, personal website or social networking page. The ability of the Internet to reach large audiences within seconds makes it the perfect place for friends, foes and the faceless to harass other teens.

No child should put up with bullying or harassment. Teach your children to tell you right away if other kids are saying bad things about them or making threats.

Forms of Cyberbullying

There are many different types of cyberbullying. Here are

just a few examples:

- sending or forwarding mean, threatening, discriminator, humiliating, embarrassing or vindictive text messages, e-mails, or chats;
- teasing or frightening someone online;
- using lewd or insulting language and remarks;
- using someone else's password to gain access to their account;
- impersonating someone online;
- spreading rumors or lies about someone through messages, comments, bulletins, or wall posts;
- pretending to be someone you are not to gather information from others;
- posting pictures or information about someone without their consent;
- insulting someone while playing an interactive online game;
- voting on an online bashing poll or guestbook.

Stopping Cyberbullying

Talk to your children about cyberbullying and how it could affect them, both as a victim or as a participant. Make sure your teens understand that they should treat others with respect when they are texting or are online, and that there are stiff legal consequences for cyberbullying in Idaho.

Most cyberbullying starts small, seemingly private between friends, and then mushrooms into a public forum until it is out of the instigator's control. Everyone is a potential target. Half of students admit to being bullied online, while an estimated 79% of teens say it is a problem.

The single most important thing you can do is let your teens know that they can come to you if they feel they have been the victim of a cyberbully.

You can help your teens stay safe by having them follow these steps.

- Never forward or respond to mean, embarrassing or hurtful messages or images (kids call these messages "flames"). Bullies often harass others to spark a reaction that then fuels further harassment.
- Block any and all communications from a cyberbully. Spyware programs have been created to send harassing messages anticipating the target's response.
- Delete "buddies" or "friends" if they post comments or images that are meant to embarrass, threaten or harass.
- Never share passwords or other account information with anyone.
- Never give personal information out to anyone.
- On social networking sites, select the setting that allows you to preview all comments and posts of another user before they are made public.
- Document and report any harassment. Tell a trusted adult and report it to your Internet service provider or website (e.g., Facebook, MySpace, etc.). Call the police if threatened. Report cyberbullying online at www.cybertipline.com and to your school resource officer.

There are laws in Idaho that protect victims of harassment, intimidation and bullying. If you feel that your child is the target of cyberbullying, talk to your school counselor or

resource officer immediately. Cyberbullying can have very serious effects on your child.

APPENDIX A

Online Resources

You'll find more information about Internet safety at these Internet sites.

www.ic3.gov

The Internet Crime Complaint Center (IC3) collects complaints involving Internet crimes and refers them to law enforcement and regulatory agencies at the federal, state, local and international level.

www.fraud.org

The National Consumers League provides advice about the Internet and Internet fraud. You can report suspected scams with an online form.

www.netsmartz.org

The National Center for Missing & Exploited Children provides child safety information for parents and children.

www.consumer.gov

This federal agency website provides consumer information and publications.

www.pueblo.gsa.gov

The Consumer's Resource Handbook, available on this federal government website, lists local, state and federal agencies, major trade associations, and consumer groups.

www.bbbonline.org

The Better Business Bureau reliability program for participating online merchants links to a central BBB site for reports about businesses and information on how to contact individual BBB's across the United States.

www.ftc.gov

The Federal Trade Commission offers online pamphlets relating to Internet shopping, Internet and e-mail scams, online business opportunities, and additional consumer topics. The FTC also offers an online complaint form for consumers who encounter problems within the marketplace.

APPENDIX B

Glossary

The Internet has its own terminology. Here are a few key terms.

Adware – Adware is software that is installed on your computer without your consent. Adware monitors or controls your computer use without your knowledge. It is also called "spyware."

Attachment – A file that is sent with an e-mail message.

Browser – A browser is the program that requests Internet documents from a server and displays these documents on your screen. More than likely the program you are using at home is a web browser. Popular browsers include Netscape Navigator, Lynx, and Microsoft Internet Explorer.

Cookie – Small files placed on the hard drive of your computer by some websites that you visit.

Download – Copying files from the Internet to your computer.

E-mail or electronic mail – Messages, similar to letters, sent or received through the Internet. E-mail can be addressed to one person or a group of people.

Encryption – An algorithm, used to scramble data, which makes the data unreadable to everyone except the recipient. E-commerce sites often use encryption to secure credit card data. Secure websites use encryption.

Hyperlink – An electronic connection that automatically takes you from one website to another. For example, the

Attorney General's website provides a hyperlink to the Consumer Protection page on its site.

Internet commerce (e-commerce) – Buying and selling goods and services over the Internet. Transactions take place between businesses and consumers through a computer network.

Modem – A hardware device that uses telephone or cable lines to connect your computer to the Internet or allows you to communicate with other computers.

Pharming – "Pharming" involves the redirection of an Internet user from a legitimate commercial website to a bogus website. "Pharmers" set up bogus sites and shuttle users from legitimate websites by altering the domain name system or transmitting a virus.

Phishing – "Phishing" is a scam intended to obtain your passwords and other personal and confidential information that can be used to steal your identity. "Phishing" is conducted by fraudulently sending an e-mail that appears to be from a legitimate business. Usually the e-mail will contain a link to a fake (but legitimate-looking) Internet site. If you log on to the fraudulent site, the "phishers" will capture your user ID and password enabling them to access your account.

Search engine – A program that searches the Internet for specified keywords or phrases and returns a list of the documents containing the keywords or phrases. Google, Excite, and Yahoo are some well-known search engines.

Spam – "Spam" is the e-mail version of junk mail: unwanted e-mail messages from people you do not know seeking to sell you a product or service.

Spyware – Spyware is software that is installed on your computer without your consent. Spyware monitors or controls your computer use without your knowledge. It is also called "adware."

URL – Uniform Resource Locator. This is the address of a specific website. You can type the URL into your browser to take you directly to that site on the Internet. For example, www.ag.idaho.gov is the URL address for the Office of the Attorney General.

Virus – A file planted in your computer that can damage files and disrupt your computer.

Website – An Internet destination where you can look at and retrieve data.

This publication was prepared by the Attorney General's Consumer Protection Division and the Idaho Internet Crimes Against Children Task Force (Idaho ICAC).

Funds collected by the Attorney General's Consumer Protection Division as the result of enforcement actions paid for this pamphlet. No tax monies were used to pay for this publication.

If you have information about an Internet crime against a child or that you think will be useful in the fight against child exploitation, contact us through the National CyberTipline at www.cybertipline.com or by calling, toll-free (800) 843-5678.

The information you provide will be forwarded to the appropriate ICAC law enforcement agencies in Idaho or elsewhere in the United States.

Rev. 09/18