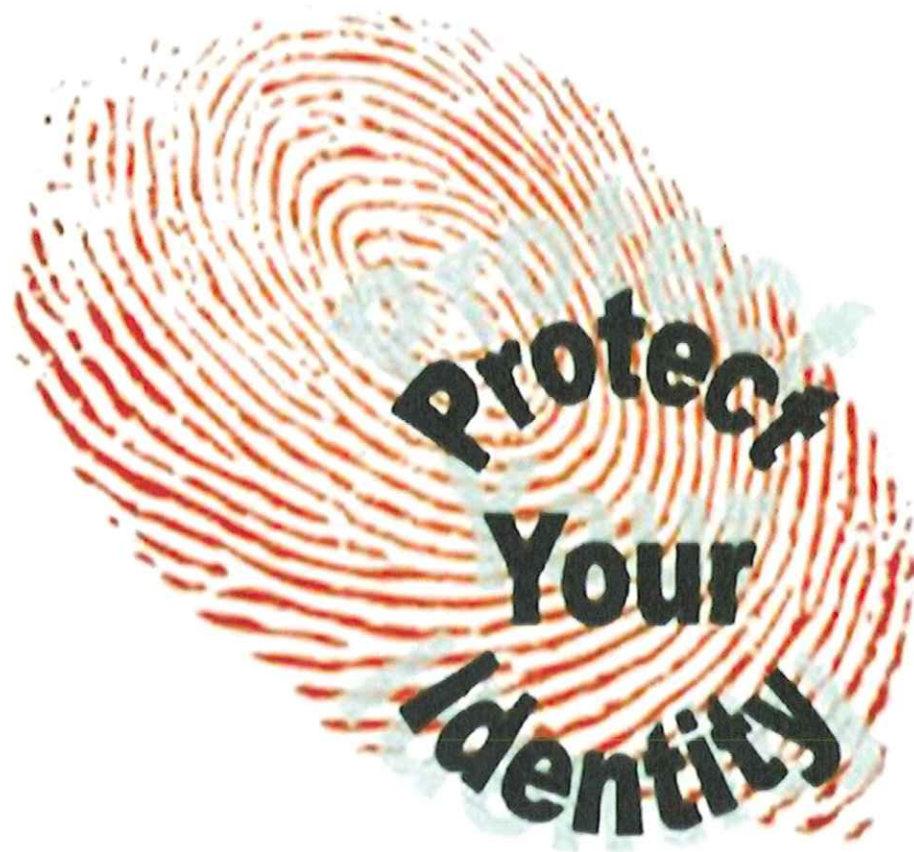
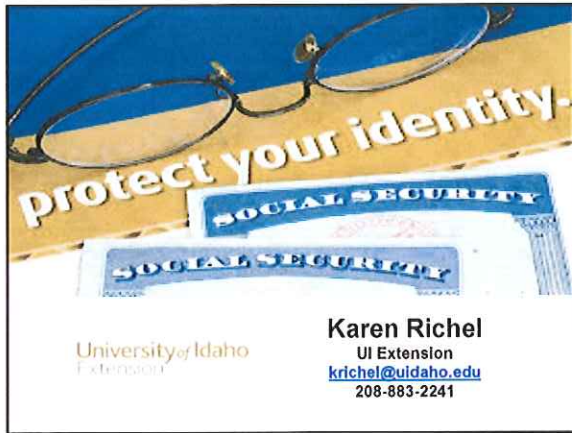


Protecting Your Personal Identity



Karen Richel
University of Idaho Extension
Latah County
(208) 883-2241
krichel@uidaho.edu

University of Idaho
Extension



protect your identity.

SOCIAL SECURITY


SOCIAL SECURITY

University of Idaho
Extension

Karen Richel
UI Extension
krichel@uidaho.edu
208-883-2241

Who are the Victims?

Have you or someone you know been a victim?



A collage of five small images: a woman in a hat, a baby, a man with a woman, a man in a vest, and a woman with a folder.

Identity Theft Happens . . .

- When someone STEALS your:
 - Name
 - Social Security Number
 - Driver's License Number
 - Credit Card Number
 - E-mail Address
 - Other personal information
- Then uses it to commit fraud or theft.



A cartoon burglar in a black mask and yellow pants holding a driver's license.

An Alarming Crime

- Identity Theft is top consumer complaint in the U.S.
 - Over 2 million complaints in 2012
 - Over 8 million complaints since 2007
 - Over \$1.5 billion in total losses in 2012
 - Median amount paid \$535



Idaho Statistics - 2012

- 7,598 Total Complaints
- 905 ID Theft Victims
- Location:
 - Boise area – 2832 Fraud and 438 ID Theft Victims
 - Coeur d'Alene – 717 Fraud and 88 ID Theft Victims
 - Idaho Falls – 433 Fraud and 73 ID Theft Victims



How Do Thieves Do It?

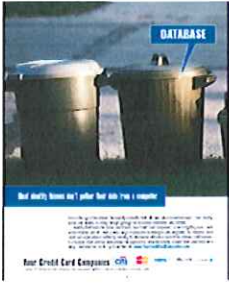
(Are there any you are not familiar with?)

- Steal a purse or wallet
- Randomly use SSN's
- Find personal information in homes
- Complete false change of address forms
- Obtain personal information from worksites
- Steal your mail



How Do Thieves Do It?


(Are there any you are not familiar with?)




- Use camera cell phones or digital cameras to "Shoulder Surf"
- Dumpster diving
- Fraudulently obtain credit reports
- "Skim" your credit or debit cards

How Do Thieves Do It?

(Are there any you are not familiar with?)



- "Phishing"
- "Pretexting"



Password change required!

Generic greeting, did not use my user name or actual name
Dear sir,

Misspelling, and incorrect grammar.
We recently have determined that different computers have logged onto your eBay account, and ~~multiple~~ password failures were present before the logons. We strongly ~~advise~~ **CHANGE YOUR PASSWORD.**

Created a sense of urgency
If this is not completed by **December 17, 2006**, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. Thank you for your cooperation.

[Click here to Change Your Password](#)

Direct link asking for my password (to imposter site)
Thank you for your prompt attention to this matter.
We apologize for any inconvenience.

Thank you for using eBay!

How Do Thieves Do It? (Are there any you are not familiar with?)



- Friends and Family

What Do the Thieves Do With Your Info?

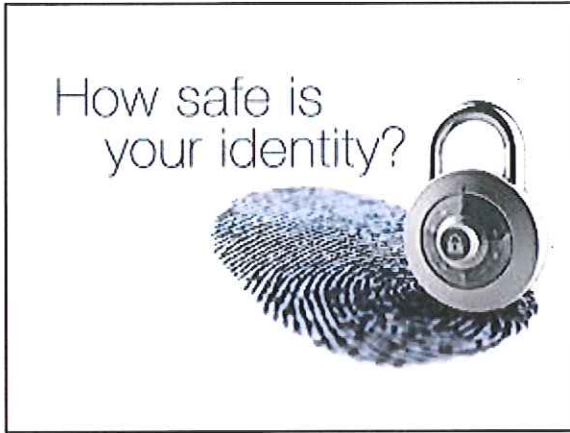
- An ID thief uses your information to:
 - Obtain new credit cards
 - Forge checks or debit cards & drain accounts
 - Open new bank accounts
 - Receive utilities
 - File a bankruptcy case
 - Commit crimes



What Is At Risk?

- Identity Theft can damage your credit rating and you could be:
 - Denied a job offer
 - Denied a loan
 - Denied housing
 - Denied utilities
 - Denied medical services
- Your wages garnished
- Your driver's license revoked
- Wasted time and money





Minimize Your Risk

- Protect your Social Security Number:
 - Do not use on checks, insurance or other cards
 - Memorize your number
 - Ask why when required to give your number
 - How will it be used?
 - How will it be protected?
 - Is it necessary?



Minimize Your Risk

- Carry only the credit cards you need
- Keep a copy of all your important account and phone numbers
- Safeguard personal information:
 - Place passwords on your
 - Credit/Debit cards
 - Bank accounts
 - Phone or online accounts
 - Have your photo placed on your credit and debit cards



Use Passwords on Accounts

- When placing passwords on your accounts do not use:
 - Mother’s maiden name
 - Your birth date
 - Last four digits of your SSN
 - A series of consecutive numbers
 - Your phone number
 - Your street address or zip code



Minimize Your Risk

- Obtain free credit report yearly.
 - www.annualcreditreport.com
 - One free credit report is available from each of the credit reporting agencies: Equifax, Experian, and TransUnion.
 - **1-877-322-8228**
 - Mail “Annual Credit Report Request” form to:
 - Annual Credit Report Request Service
 - P. O. Box 105283
 - Atlanta, GA 30348-5283



Minimize Your Risk

- Remove your name from pre-approved credit card mailing lists. You can do this by going to www.optoutprescreen.com or calling 1-888-5-OPTOUT.

OPT-OUT	<input checked="" type="checkbox"/>
OPT-IN	<input type="checkbox"/>

Minimize Your Risk

- Stop telemarketers from calling your home and cell phone numbers. You can do this by going to WWW.DONOTCALL.GOV or calling 1-888-382-1222.
- Your phone numbers will be removed for LIFE (No Longer Only 5 Years)!



Minimize Your Risk

- Reduce unwanted mail!
- Register with the Direct Marketing Association's Mail Preference Service
 - Free if you go to www.dmachoice.org
 - \$1 processing fee if you request by mail:

DMA choice
Direct Marketing Association
P.O. Box 643
Carmel, NY 10512



Minimize Your Risk

- FREEZE Your Credit!
 - Costs \$6 Per Credit Bureau in Idaho
 - Costs \$6 to "Thaw" /Unfreeze Credit
- One of the most successful tools to prevent financial Identity Theft!



Minimize Your Risk

- Sign up for Free Scam Alerts
 - www.consumerprotection.id.gov



Protect Your Information

- Do not provide personal information over the phone, through the mail, or over the Internet unless:
 - You placed the call, letter or email
 - You know the company's reputation is reputable and that the request is legitimate
- If you receive a call claiming you won a prize:
 - Do not provide or confirm any personal information
 - Do not provide credit card information
 - Ask for the phone number and ID of the caller
 - Do not send money



Protect Your Computer

- Update your virus protection software
- Install updates for your operating system
 - Protect against intrusions and infections such as "pharming"
- Do not open files, click on hyperlinks or download programs sent to you by strangers
- Use a firewall program
- Check for website security
- Do not store financial info on laptops
- Use a strong password
- If donating or discarding a computer clean it of all personal information



Protect Your "Public" Information

- Do not post personal information on the Internet
- Shred documents with any personal information
- Be careful with key cards



Protect Your Purse or Wallet

- Do not:
 - Hang your purse over the back of a chair or put it in a shopping cart
 - Carry more credit cards than you need
 - Carry your passport, visa, or birth certificate
 - Carry your passwords or PINS
 - Carry your SSN or card



Protect Your "Private" Information

- Review your credit and bank statements each month, report fraudulent activity immediately
- Use a locking mailbox or post office box for incoming mail
- Do not leave mail lying around
- Do not allow mail to pile up
- Use the U.S. Post Office or postal mailbox for outgoing mail
- Have new checks delivered to your bank



Protect Your Credit Cards

- Shield your credit cards from view
 - Watch out for shoulder surfers with camera cell phones
- Sign new cards when they arrive
- Total receipts, do not leave empty spaces where additional amounts can be added
- Keep receipt copies to compare with your monthly statements
 - Do not leave in shopping bags

Protect Your Bank Accounts

- When ordering checks:
 - Use initials for your first name
 - Use your work phone number
 - Use a PO Box instead of your home physical address
- Do not put full account numbers on the memo line
- Never sign blank checks
- Do not leave empty spaces on your checks
- Balance your checkbook monthly



Protect Your Account Numbers

- Cross out your credit card or bank account number on receipts when submitting for reimbursement to:
 - Charitable or professional organizations
 - Employers
 - Tax preparers
 - Product rebates





Signs of Identity Theft

- See unauthorized changes in financial accounts
- Fail to receive bills or other mail
- Receive credit cards you didn't request
- Receive credit denial
- Get calls from debt collectors
- Recognize unusual credit report activity
- Other Signs?

Discovering Identity Theft

- It takes 14 months on average before victims discover the theft
 - Fraudsters often divert bills to another address
- Victims who bank electronically find out faster
 - Paper statements – 114 days
 - Online – 8 days



Discovering Identity Theft

- Time = Money
 - Credit company or being denied credit
 - Average loss = \$12,021
 - Through paper statement review
 - Average loss = \$4,543
 - By electronic statements
 - Average loss = \$551



If You Are A Victim



- File a police report and get a copy of the report
- Alert credit card companies and bank immediately!
 - Contact all of your creditors:
 - Close all affected accounts
 - “Closed at the customer’s request”
 - Request that creditors contact you with “account activity”
- Stop payment on outstanding checks
- Change passwords or PINS
- Request new ATM cards

If You Are a Victim

Contact the 3 credit reporting agencies:



- Add a “fraud alert” and “victim’s statement” to your file
 - Place a fraud alert in your files *with caution*.
- Complete an ID Theft Affidavit
 - www.consumer.gov/idtheft/pdf/affidavit.pdf
- Request a free copy of credit report, to check for additional affected accounts.

If You Are A Victim

- Contact the Federal Trade Commission (FTC)
 - www.consumer.gov/idtheft
 - 1-(877)-ID-THEFT (FTC’s Identity Theft Hotline)
- You may also need to contact:
 - Department of Motor Vehicles
 - Internal Revenue Service
 - Passport Office
 - Social Security Administration
 - 1-800-269-0271 or www.ssa.gov
 - U.S. Postal Inspection Service
 - 1-202-268-2284 or www.usps.gov
 - U.S. Secret Service
 - www.ustras.gov/usss
 - U.S. Trustee’s Office



If You Are A Victim

- AND KEEP A PAPER TRAIL!!!

- Keep a record of all your contacts and correspondence regarding the theft

- Written
- Telephone



SHARING! and QUESTIONS?



Karen Richel
UI Extension
krichel@uidaho.edu
208-883-2241

What Is Identity Theft?

Tricks, Scams, and Ways to Stay Safe

Identity theft is when someone STEALS some piece of your personal information without your knowledge and uses that information to obtain – as YOU

\$ cash

\$ services

\$ get mortgage

\$ credit

\$ rentals

\$ utility accounts

\$ loans

\$ start business

\$ employment

THINGS TO WATCH OUT FOR:



“I keep my personal information to myself.” You may think you’re doing a good job, but identity thieves are resourceful: Their goal is to trick you into revealing personal information. If they can’t get it from you; they are breaching big and small companies’ data files to get that businesses customer’s information.

\$ Breaching Company’s Data file.

- o Your state law controls the rights you have if your information is lost in a data breach. When the organization that lost your information lets you know about the breach, they should explain your options.

\$ Scams by email

- o The Nigerian Scam and the like – You receive an email asking you to help “transfer” money from Nigeria to the States. The sum of money is enormous of which you will get a large portion for your time and effort in return. You send your banker’s name, telephone number, account number, and a signed letter accepting the deal. They have all they need to wipe your account clean.
 - Little tidbit...never share account numbers with anyone. These should be guarded. Explain what can be done with an account number. The people that need this information already have it.

THINGS TO WATCH OUT FOR: (CONTINUED)

- \$ **Phishing** is the practice of copying a company's logo and branding information to fool you into divulging personal information via email.
- o How many of you have seen these?
 - Citibank, SunTrust – your ATM/Debit card must be updated or your account will be closed due to large numbers of theft attempts.
 - U.S. Bank claims that your account has been suspended and needs your information via email to reactivate it.
 - Wells Fargo needs to "update" your information for your account.
 - The United States District Court is sending you a subpoena via email.
 - The CDC wants you to create a "vaccination profile".
 - All of these have a sense of "urgency". You must do this right away or something bad will happen. They also give you a convenient link so you can go right to their website to "correct" the "problem". Generally, you will get the email to "Dear Sir" or another generic greeting. And there will be typos throughout the text.

- \$ **Smishing** is the latest threat. It comes with text messaging to cell phones. Thieves send a text message, appearing to come from your own cell phone, to a family member or loved one with the instructions that you need some personal information like a pin number or bank account number. In addition, they can send links to websites that if activated will download malicious software onto your computer.



- \$ **Mail Fraud** is using the postal service to unlawfully obtain money or other valuables.
- o Non-delivery of mail-order purchase – You buy something, pay for it, it never comes or it has been misrepresented and isn't what you ordered.
 - o Promotional checks – You get a check in the mail for \$50 "free to do what you want with it...go to lunch...pay a bill". In the fine print, you have just been signed up for a long distance service or other "very useful" purchase that is difficult to cancel or return.
 - o Solicitations that look like invoices – Tricky wording that makes you think you need to pay a "bill" that is really solicitation for business.
 - o Work-at-Home scams – Assemble small products or stuff envelopes in your spare time and make a \$1,000 a week. Just send \$29.95 to get started.

Banks, financial institutions, businesses and government agencies DO NOT ask you for your information by email. In addition, the majority do not ask you for sensitive information via phone. If you receive a call or email, contact the sender using the number on your bill or start-up documentation to verify. Never use the number or respond to the email provided.

THINGS TO WATCH OUT FOR: (CONTINUED)

\$ **IRS Scams**

- Making Work Pay Refund – A refundable credit is available to workers, consumers and retirees that can be paid into the recipient's bank account if the recipient registers their account information with the IRS. Most taxpayers actually receive this in their paychecks and non-wage earners aren't eligible for this credit.
- Inherited Funds or Lottery Winnings – You have just won millions. The U.S. Department of the Treasury is notifying you that they have recovered funds, lottery winnings or a cash consignment in your name. You just have to send verification of who you are. In addition, they will need your phone number and email for future contacts. When the phony check is sent, you are asked to "deposit" 10 percent to pay taxes and fees. The check is fake and you are out your 10%.

\$ **Foreclosure Scams**

- Too many to mention. Scammers are attacking those that are at the weakest moment by stealing their homes right from underneath them.
 - Fake Counselor – the con-artist can save your home with your details
 - Bait-and-Switch – you sign a new "rescue" loan with con – he gets your title
 - Rent-to-Buy Scheme – you "rent" your home with the idea that the con will eventually sell your house back to you.

If it is too good to be true, it is.

\$ If it makes you feel funny in any way, say no.

\$ Take a second before you react. Don't do something just because someone else says that you "have to or else". Call local authorities, the actual creditor, etc. to verify the call.

\$ To verify, visit www.snopes.com for urban myths. Snopes will tell you all about phishing, tax fraud, telephone scams, sales scams, identity theft, distress scams, and more. Remember, however, that this is an Internet site as well. The organizers of this website "say" that they research this information.

\$ Contact the BBB website for more information on a companies if there is a question.

\$ If you are still unsure, call the Sheriff's office.



Clues That Someone Has Stolen Your Information, You see:

- Unexplained withdrawals from your bank account.
- You don't get your bills or other mail.
- Merchants refuse your checks.
- Business notifies you that your information was compromised by a data breach
- Debt collectors call you about debts that aren't yours.
- You find unfamiliar accounts or charges on your credit report.
- Medical providers bill you for services you didn't use.
- Your health plan rejects a medical claim since you've reached your benefits limit.
- The IRS notifies you that more than one tax return was filed in your name.
- IRS notifies you that you have income from an employer you don't work for.

Ways to Keep Personal Information Safe?

Source: Federal Trade Commission [FTC.GOV/IDTHFT](https://www.ftc.gov/idtheft)

Securing Your Social Security Number

Keep a close hold on your Social Security number and ask questions before deciding to share it.

Ask if you can use a different kind of identification. If someone asks you to share your SSN or your child's, ask:

- why they need it
- how it will be used
- how they will protect it
- what happens if you don't share the number



The decision to share is yours. A business may not provide you with a service or benefit if you don't provide your number.

Sometimes you will have to share your number. Your employer and financial institutions need your SSN for wage and tax reporting purposes. A business may ask for your SSN so they can check your credit when you apply for a loan, rent an apartment, or sign up for utility service.



**Your SSN is like a MASTER KEY,
With it, anyone can be you.**

Ways to Keep Personal Information Safe? (Continued)

Personal Information Secure Off-line

\$ Lock your financial documents and records in a safe place at home, and lock your wallet or purse in a safe place at work. Keep your information secure from roommates or workers who come into your home.

\$ Limit what you carry. When you go out, take only the identification, credit and debit cards you need. Leave your Social Security card at home.

\$ Make a copy of your Medicare card and black out all but the last four digits on the copy. Carry the copy with you — unless you are going to use your card at the doctor's office.

\$ Before you share information at your workplace, a business, your child's school, or a doctor's office, ask why they need it, how they will safeguard it, and the consequences of not sharing.

\$ Shred receipts, credit offers, credit applications, insurance forms, physician statements, checks, bank statements, expired charge cards, and similar documents when you don't need them any longer.

\$ Destroy the labels on prescription bottles before you throw them out. Don't share your health plan information with anyone who offers free health services or products.

\$ Take outgoing mail to post office collection boxes or the post office. Promptly remove mail that arrives in your mailbox. If you won't be home for several days, request a **vacation hold** on your mail.

\$ When you order new checks, don't have them mailed to your home, unless you have a secure mailbox with a lock.



Ways to Keep Personal Information Safe? (Continued)

Personal Information Secure On-line

\$ **Be Alert to Impersonators**

- Make sure you know who is getting your personal or financial information. Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or know who you're dealing with.
- If a company that claims to have an account with you sends email asking for personal information, don't click on links in the email. Instead, type the company name into your web browser, go to their site, and contact them through customer service. Or, call the customer service number listed on your account statement. Ask whether the company really sent a request.

\$ **Safely Dispose of Personal Information**

- Before you **dispose of a computer**, get rid of all the personal information it stores. Use a wipe utility program to overwrite the entire hard drive.
- Before you **dispose of a mobile device**, check your owner's manual, the service provider's website, or the device manufacturer's website for information on how to delete information permanently, and how to save or transfer information to a new device.
- Remove the memory or subscriber identity module (SIM) card from a mobile device. Remove the phone book, lists of calls made and received, voicemails, messages sent and received, organizer folders, web search history, and photos.



\$ **Encrypt Your Data**

- Keep your browser secure. To guard your online transactions, use encryption software that scrambles information you send over the internet.
- A "lock" icon on the status bar of your internet browser means your information will be safe when it's transmitted. Look for the lock before you send personal or financial information online.

\$ **Keep Passwords Private**

- Use strong passwords with your laptop, credit, bank, and other accounts.
- Be creative: think of a special phrase and use the first letter of each word as your password.
- Substitute numbers for some words or letters. For example, "I want to see the Pacific Ocean" could become 1W2CtPo.

\$ **Don't Overshare on Social Networking Sites**

- If you post too much information about yourself, an identity thief can find information about your life, use it to answer 'challenge' questions on your accounts, and get access to your money and personal information.
- Consider limiting access to your networking page to a small group of people.
- Never post your full name, Social Security number, address, phone number, or account numbers in publicly accessible sites.

Source: Federal Trade Commission FTC.GOV/IDTHEFT

Taking Charge of Your Credit Report

What Should You Do If Your Personal Information is Lost or Stolen?

Karen Richel
UI Extension Educator
krichel@uidaho.edu
208-883-2241

YOU HAVE LOST OR KNOW THAT YOUR PURSE/WALLET HAS BEEN STOLEN.

Right now someone, other than you, has most or all of your personal information and with those “numbers” they came become YOU and they don’t care what happens to your credit report or score.

Besides taking your money they can also take your good credit and throw it out the window – you have two options to possibly keep that window closed. You can place a Fraud Alert or a Credit Freeze on your credit file.



FRAUD ALERT –

Don’t wait for problems to show up on your credit report. As soon as you realize your information is lost or stolen, do something; be proactive when it comes to your credit report. When placing the alert, also request a current “free” copy of your credit report. Check it for possible issues or red flags that someone has already started using your name and credit.

You only need to contact one of the three credit reporting companies to have a fraud alert placed on your reports. There are three types of fraud alerts you can have placed on your credit file. In Idaho the three types are:

- A. A 90-day initial fraud alert (can be renewed if needed)
- B. A seven-year extended fraud alert, or
- C. An one-year active duty military alert

When a fraud alert is placed on your report by a Credit Reporting Company, they will include a message notifying the third-party creditor (i.e. Bank, Car Dealer, Loan Company) that they need to verify your identity before issuing NEW credit in your name.

A short coming of fraud alerts is that the third party creditor requesting your report is NOT required to contact you using information on the report from the credit reporting company. If the person requesting credit has enough of your information, the creditor will not see a need to question that person about if he or she is really you?



CREDIT “Security” FREEZE –

Idaho’s Credit Report Protection Act allows individuals to request a security “freeze” on their credit report kept by the credit reporting agencies at any time and for any reason means. If you have filed a police report concerning your personal information being lost or stolen, you can have your credit report frozen for free; otherwise there is a small fee (around \$6.00) for each agency to obtain a freeze.

CREDIT "Security" FREEZE – (Continued)

With a security freeze the Credit Reporting Companies are limited to whom they can share your report with. Most creditors will not give or authorize credit without first reviewing a person credit report. Making it difficult for someone with your stolen information to get new credit using your name.



Once you place a security "freeze" on your credit report, it will remain in effect until you ask the credit reporting company to lift it. A security freeze can be temporary or permanently lifted when you need a third-party creditor to have access to your report so you can get new credit. Ask your creditor which company they use and you can "un-freeze" just that company's credit report.

A credit freeze only effects information going out to creditor. Your personal credit information (bill payments, credit card balances, etc.) will continue to be received about your current credit use.

The freeze is useful in reducing the risk of an identify thief getting a new credit account using your stolen information.

For more information on Fraud Alerts and Security Freezes go to:

<http://www.ag.idaho.gov/consumerProtection/generalTopic/topicSubPages/creditFreezeFAQs.html>

REQUESTING AN ALERT OR FREESE – Be prepared to verify your identity.

Before contacting the Credit Reporting Agencies gather the information you think they may ask for to verify your identity. Call the agencies to learn what their recommended procedures are.

To obtain a security freeze you will most likely need to send in a written request to each company.

It is recommended that you send your information

- Via certified USPS mail with a return receipt requested
- When you sent your documentation make sure to keep a copy of all the document you send.
- Send it from your local post office, don't have your mail carrier pick it up from your box or mail from your business or employer address.

Equifax Security Freeze
P.O. Box 105788
Atlanta, Georgia 30348

Experian Security Freeze
P.O. Box 9554
Allen, Texas 75013

TransUnion Security Freeze
P.O. Box 6790
Fullerton, California 92834

Stop Identity Theft Cold by “Freezing Your Credit!”

Lyle Hansen, Jerome County Extension Educator

I am often asked “what is the best way to protect against identity theft?” My answer has been to use and follow the *Identity Theft Quick Tips* worksheet that Luke Erickson and I developed, which can be found here <http://www.extension.uidaho.edu/jerome/identity%20Theft/images/2012%20ID%20Theft%20Quick%20Tips.pdf> . Using the *Identity Theft Quick Tips* worksheet is a very effective way to monitor your identity and protect against identity theft. Now, there is the option of requesting a credit freeze (also called a security freeze), which is one of the most successful tools to prevent financial identity theft. A credit freeze is a great option for someone who doesn't frequently apply for credit and wants peace of mind when it comes to identity theft. A credit freeze means that your credit file cannot be seen by potential third-party creditors or employers conducting background checks unless you give permission. For example, if someone steals your identity and applies for a credit card, your credit report is not released to the credit card company because it is frozen and the thief is stopped. This added layer of security means that thieves can't establish new credit in your name even if they are able to take over other elements of your identity because they don't have your secret personal identification number or password.

You may request a credit freeze on your credit report, which will not lower your credit score, still allow you to obtain new credit, allow you to use your existing credit (credit cards), and receive your free credit reports at www.annualcreditreport.com. You can request a credit freeze regardless if you have become a victim of identity theft or not. A credit freeze is inexpensive, currently \$6 per credit bureau in Idaho and \$0 to \$20 per credit reporting agency depending on the state you live in. Victims of identity theft can have any fees waived, and seniors are often exempt from the fees in most states. Follow this link that lists the credit freeze costs per state: https://help.equifax.com/app/answers/detail/a_id/75/search/1.

To obtain a credit freeze, you simply go to each of the three main credit bureau websites (Please note that both spouses have to freeze their separate credit files):

- Experian (http://www.experian.com/consumer/security_freeze.html),
- Trans Union (<https://annualcreditreport.transunion.com>),
- Equifax (<https://www.freeze.equifax.com>), and complete the online forms.

You can also call the credit bureaus or submit a written request. Using the websites is not difficult and does not take long. When placing the credit freeze, you will be provided a personal identification number or password to use if you choose to temporarily authorize the remove (thaw) of the credit freeze for the release of your credit report for a specific purpose or time frame, such as applying for new credit or for a potential employer. Removing a temporarily credit freeze costs \$6 per bureau in Idaho and \$0-\$12 in other states.

Unfortunately, a credit freeze doesn't stop pre-approved credit offers or phone solicitors, but you can stop these by going to:

- www.optoutprescreen.com or calling 1-888-567-8688
 - Stops preapproved credit solicitations for life.
- www.donotcall.gov or calling 1-888-382-1222
 - Stops telemarketers from calling your home/cell phone number for life (no longer only five years).

A credit freeze has fees associated, but it is a very inexpensive option to protect against identity theft and is cheaper and more effective than paying for a credit protection service. It also will give you the peace of mind knowing your financial identity is safe.

For further information or questions you can contact Lyle Hansen, University of Idaho Extension Educator in Jerome County at 324-7578 or lhansen@uidaho.edu

Red Flags of Identity Theft

- mistakes on your bank, credit card, or other account statements
- mistakes on the explanation of medical benefits from your health plan
- your regular bills and account statements don't arrive on time
- bills or collection notices for products or services you never received
- calls from debt collectors about debts that don't belong to you
- a notice from the IRS that someone used your Social Security number
- mail, email, or calls about accounts or jobs in your minor child's name
- unwarranted collection notices on your credit report
- businesses turn down your checks
- you are turned down unexpectedly for a loan or job

IDENTITY THEFT



WHAT TO KNOW



WHAT TO DO



Taking Charge:

What To Do If Your Identity Is Stolen

Available online at ftc.gov/idtheft

Order free copies at bulkorder.ftc.gov

FEDERAL TRADE COMMISSION

FTC.GOV/IDTHEFT

1-877-ID-THEFT (438-4338)

FEDERAL TRADE COMMISSION

FTC.GOV/IDTHEFT

What is Identity Theft?

Identity theft is a serious crime. It can disrupt your finances, credit history, and reputation, and take time, money, and patience to resolve. Identity theft happens when someone steals your personal information and uses it without your permission.

Identity thieves might:

- go through trash cans and dumpsters, stealing bills and documents that have sensitive information.
- work for businesses, medical offices, or government agencies, and steal personal information on the job.
- misuse the name of a legitimate business, and call or send emails that trick you into revealing personal information.
- pretend to offer a job, a loan, or an apartment, and ask you to send personal information to “qualify.”
- steal your wallet, purse, backpack, or mail, and remove your credit cards, driver’s license, passport, health insurance card, and other items that show personal information.

How to Protect Your Information

- Read your credit reports. You have a right to a free credit report every 12 months from each of the three nationwide credit reporting companies. Order all three reports at once, or order one report every four months. To order, go to annualcreditreport.com or call 1-877-322-8228.
- Read your bank, credit card, and account statements, and the explanation of medical benefits from your health plan. If a statement has mistakes or doesn’t come on time, contact the business.
- Shred all documents that show personal, financial, and medical information before you throw them away.
- Don’t respond to email, text, and phone messages that ask for personal information. Legitimate companies don’t ask for information this way. Delete the messages.
- Create passwords that mix letters, numbers, and special characters. Don’t use the same password for more than one account.
- If you shop or bank online, use websites that protect your financial information with encryption. An encrypted site has “https” at the beginning of the web address; “s” is for secure.
- If you use a public wireless network, don’t send information to any website that isn’t fully encrypted.
- Use anti-virus and anti-spyware software, and a firewall on your computer.
- Set your computer’s operating system, web browser, and security system to update automatically.

If Your Identity is Stolen...

1 Flag Your Credit Reports

Call one of the nationwide credit reporting companies, and ask for a fraud alert on your credit report. The company you call must contact the other two so they can put fraud alerts on your files. An initial fraud alert is good for 90 days.

Equifax 1-800-525-6285

Experian 1-888-397-3742

TransUnion 1-800-680-7289

2 Order Your Credit Reports

Each company’s credit report about you is slightly different, so order a report from each company. When you order, you must answer some questions to prove your identity. Read your reports carefully to see if the information is correct. If you see mistakes or signs of fraud, contact the credit reporting company.

3 Create an Identity Theft Report

An Identity Theft Report can help you get fraudulent information removed from your credit report, stop a company from collecting debts caused by identity theft, and get information about accounts a thief opened in your name. To create an Identity Theft Report:

- file a complaint with the FTC at ftc.gov/complaint or 1-877-438-4338; TTY: 1-866-653-4261. Your completed complaint is called an FTC Affidavit.
- take your FTC Affidavit to your local police, or to the police where the theft occurred, and file a police report. Get a copy of the police report.

The two documents comprise an Identity Theft Report.



Free Credit Reports

On September 1, 2005, Congress passed legislation that enabled citizens throughout the United States to order a free copy of their credit report once a year from each of the three major credit reporting agencies. The following website and phone number have been set up to facilitate this process:

Website: www.annualcreditreport.com
Phone: (877) 322-8228

What is in your credit report?

- Your name and your spouse's name
- Where you live, where you work, and where you used to live and work
- Your social security number, phone number and birth date
- Whether you paid bills on time, and how much credit you have available
- If you've been late with rent or mortgage payments
- Whether and to whom you have made an application for credit or a loan
- Companies who obtained your credit report
- Bankruptcies, foreclosures, court judgments, convictions or tax liens

What if You Find an Error on Your Credit Report?

- Write a certified return-receipt letter to the three main credit reporting agencies about any errors in your report. Include copies of all documents that verify the facts outlined in your letter.
- Agency must conduct investigation into the accuracy of the information within 30 days.
- After the investigation is completed (30 days) agency must report back to you in 5 days.

- If the agency cannot verify the negative information they must delete it.
- Be careful about unrelated companies that promise swift and fast credit repair. This process takes time.

Credit Score

A credit score is a number lenders use to help them decide whether to provide a loan to you. A score is a snapshot of your credit risk, based on your credit report, at a particular point in time. The higher your score the lower the interest rate banks will charge you on your mortgage or other loans you take out. Factors like gender, race, religion, nationality and marital status are not considered in credit scoring.

Idaho Department of Finance's Financial Literacy Outreach Program

The Idaho Department of Finance provides speakers for high school classes, educational conferences, and community organizations throughout the State of Idaho. Topics of discussion include investing, securities fraud, identity theft, how to read your credit report, mortgage lending scams and credit card tips. Please call the Idaho Department of Finance at 208-332-8000 or toll free in Idaho at 888-346-3378 to schedule a speaker.

The Idaho Department of Finance provides a consumer affairs response program to assist consumers with problems or questions involving state regulated financial institutions, securities and investing, and licensed collection agencies. Staff is available Monday through Friday between the hours of 8:00 a.m. and 5:00 p.m. at 208-332-8000 local calls or toll free in Idaho at 888-346-3378.

Identity Theft

“Identity theft is one of the fastest growing crimes in the United States, costing victims over \$5 billion annually!”

Inside: How Idahoans can obtain their Free Credit Report.



Idaho Department of Finance

**800 PARK BOULEVARD, SUITE 200
BOISE, IDAHO 83712
finance.idaho.gov**

**TOLL FREE IN IDAHO
888-346-3378**

**LOCAL IN IDAHO
208-332-8000**

Identity Theft

Identity theft is used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. This is a serious crime that can take months or years and hard earned money to clean up the mess the thieves have made of your good name and credit record.

How Does the Criminal Get the Information?

- Steal wallets and purses
- Steal mail (credit card statements, new checks)
- Rummage through your trash (dumpster diving) looking for personal information
- Complete a "change of address form" to divert your mail to another location
- Use personal information you share on Internet
- Scan you through e-mail "phishing"
- Business record theft: steal files out of the office or bribe an employee
- Obtain your credit report by posing as a landlord, employer or someone else who has a legal right to the information.

What Does the Thief Do With the Information?

- Go on spending spree using your credit card
- Open new credit card accounts
- Open new checking accounts using your name, date of birth and social security number to write bad checks
- Change the address on your credit card accounts
- Take out auto loans in your name
- Rent a home in your name
- File for government benefits using your name (unemployment insurance)
- Give your name to police during an arrest
- Establish phone and wireless service in your name
- Declare bankruptcy in your name to avoid paying debts or eviction

Ways to Minimize Your Risk:

- Destroy private records and statements (tear/shred)
- Secure your mail: empty mailbox quickly or get a P. O. Box
- Safeguard your social security number: never carry your card with you, do not put your number on your checks
- Don't leave a paper trail (receipts)
- Never let your credit card out of your sight
- Take your name off marketer's hit list
- Monitor your credit report: order your once-a-year free credit report from the three main credit reporting agencies
- Review credit card statements carefully: call promptly if they do not arrive
- Use unusual passwords on your accounts. Never use your mother's maiden name, the last four digits of your social security number, your phone number or your birth date
- Carry only the identification information and the number of credit and debit cards that you will actually need
- Keep your virus protection up-to-date on your computer system
- Before you dispose of a computer or cell phone – delete any personal information

Avoid "Phishing" on the Internet

Scam artists on the Internet pose as banks, government agencies and service providers (AOL or Comcast) and ask you to verify account numbers, social security numbers and other confidential information they can use to loot your checking account or run up your credit card bill. If you have questions about an e-mail, call the company directly and ask about the e-mail or website. Always take time to review the information. Never respond to suspicious e-mails or provide personal information in response to an e-mail-no matter how official it may appear.

What to do if you are a victim of Identity theft

- Call the credit reporting agencies and put a fraud alert on your account. Get your credit report from the three agencies:

Equifax
www.equifax.com
800-525-6285
P. O. Box 740241
Atlanta, GA 30374-0241

Experian
www.experian.com
888-397-3742
P. O. Box 9532
Allen, TX 75013

TransUnion
www.transunion.com
800-680-7289
Fraud Victim Assistance Division
P. O. Box 6790
Fullerton, CA 92834-6790

- Call the police (in the area where the crime took place) and file a report.
- Contact your bank or credit card issuer about all of your accounts that have been stolen. Close all accounts that have been tampered with as well as all new accounts fraudulently opened in your name.
- Contact Federal Trade Commission (FTC) at www.ftc.gov or 877-382-4357 to report the crime so they can pursue the identity thefts.
- Keep records of all your contacts.

Resources:

Identity Theft Resource Center
www.idtheftcenter.org

Federal Trade Commission:
www.consumer.gov/idtheft

U.S. Department of Justice:
www.usdoj.gov/criminal/fraud/idtheft.html



Connecting Generations:

Microsoft

Collaborative research sponsored by AARP and Microsoft

AARP and Microsoft conducted a joint research project to examine how computers, mobile devices and the Internet are changing the way we communicate. What we discovered is that online communication and social networking are helping family members keep in touch, enriching their relationships and connecting generations in new ways. However, as more and more of us go online, people of all ages are increasingly concerned about Internet risks and want to learn more about staying safer online.

Going online increases quality and frequency of family communication

A majority of those surveyed (83 percent), including at least eight in 10 in each age group, considers going online to be a "helpful" form of communication among family members. Teenage respondents say the computer increases both the quantity (70 percent) and quality (67 percent) of their communication with family members living far away. Similarly, those age 39+ also embrace these sentiments (63 percent and 57 percent, respectively).



A majority of those surveyed (83 percent) considers going online to be a "helpful" form of communication among family members.

Bridging the generations: Online communication promotes understanding

Although more and better communication does not necessarily close the generation gap, a sizable number of respondents in all age groups says going online actually helps them to better understand other family members or helps other family members better understand them.

Follow me: People want their families to use social media more

Nearly one third (30 percent) of all respondents say they would like their family to communicate more through social networking sites. But, older family members should expect to feel some familial "peer pressure" coming from their younger relatives: Younger respondents (age 13-25) are significantly more likely than older ones to want their families to increase their use of social media for staying in touch (52 percent vs. 21 percent).



Of all respondents say they would like their family to communicate more through social networking sites.



3 in 10 grandparents (30 percent) and teens/young adults (29 percent) agree that connecting online has helped them better understand the other.

Teens <3 (heart) texting: The generations have different views on texting and emailing

Asked how they would like to stay connected with their families (regardless of current practices), 63 percent of those age 13-25 select text messaging over other modes of communication. But, their elders may LOL if young people want to text them: only 31 percent of those in the 39-75 age group want to use text messaging to communicate with family members. Segmenting this group further makes the generational pattern even more apparent: those age 39-58 are twice as likely to want to text family members versus those aged 59-75 (40 percent vs. 19 percent).

The generational pattern is reversed when it comes to email. The oldest age group (59-75) slightly prefers email more than the next-oldest (39-58) (60 percent vs. 56 percent), while email is apparently becoming passé to the two younger groups; 46 percent of those age 18-25 and 36 percent of those age 13-17 want to use email to communicate with family members.

The writing is on the (Facebook) wall: More communication is moving online

Online communication may only have been around for about a generation, but it is already closing in on the telephone as the most commonly used mode of communication, especially among young people.

Of those age 39-75, 75 percent name the phone and 54 percent name some type of computer as the "one or two devices" they use most often. A bellwether of things to come: the gap between computers (61 percent) and the phone (69 percent) is even narrower among teens and young adults (age 13-25).

Block that content: Both parents and children want to separate family and social life

Younger respondents are more private about their personal social-networking content compared to older respondents. Younger respondents are also split (47 percent) when it comes to how much information they share with their parents and how much content they restrict. Another 15 percent report not allowing their parents to access any of their social-networking content. Teens are also more likely than young adults to restrict how much of their content their grandparents can access (47 percent vs. 38 percent).

However, blocking is clearly a two-way street. Many parents (32 percent) restrict how much of their social-networking content they allow their teenage children to access, while a smaller proportion (14 percent) of parents of young adults impose such restrictions. The desire to keep a separation

between family life and social life is a widely cited reason – among all ages surveyed – for not wanting to share social-networking content with family members. Both parents and younger respondents report concerns that other people may post comments on their “wall” in a way they don’t like, and that their content is too personal to share. And, in fact, teens and young adults express a significantly greater concern than the older respondents (combined 30 percent vs. 4 percent) about being embarrassed by what their family might post on their sites or by what they might think of them.

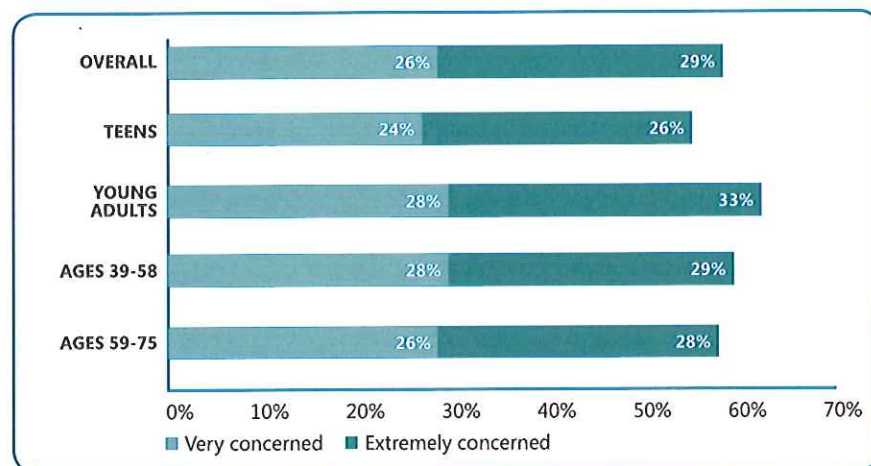
Risky business: All age groups concerned about online safety

Strikingly, almost all respondents (98 percent) across all age groups report feeling “at ease” going online.

Despite recognizing the positive aspects associated with going online and using social networks, some respondents have reservations about doing so. A majority (56 percent) of all respondents is extremely or very concerned about staying safe and secure online, with young adults expressing more concern than teenagers (60 percent vs. 50 percent). In addition, nearly two-thirds (64 percent) of parents and grandparents of teenagers report being extremely or very concerned about online safety risks such as identity theft, harassment, or malicious software potentially affecting them and their family.

In addition, the younger generation would like more general information than the older one about using social networks more safely (38 percent vs. 27 percent).

How concerned are you about staying safe and secure online?



The most frequently cited online safety items that respondents wish they knew more about include:

58% 
 How to keep sensitive personal information private

50% 
 How to safeguard their devices

37% 
 Protecting online assets such as reputation, photos, and rewards from loyalty programs

Who you gonna call? Parents overstate teens' willingness to discuss online safety with them

Interestingly, there is a divide between teens' behavior in dealing with uncomfortable online content and their parents' perception of how teens deal with this content. Nearly half (49 percent) of parents state that teens know to come to them when they see something online that makes them uncomfortable. Yet, fewer than a third (29 percent) of teens report having that knowledge.

Online safety is ageless: Teach yourself and your family about using Internet-connected devices and online technologies more safely

> Use social networks more safely

- Look for **Settings** or **Options** in services like Facebook and Twitter to manage who can see your profile or photos tagged with your name, how people can search for you and make comments, and how to block people.
- Don't post anything you wouldn't want to see on a billboard.
- Be selective about accepting friends. Regularly reassess who has access to your pages, and review what they post about you.

> Protect sensitive personal information

- Before you enter sensitive data, look for signs that a webpage is secure—a web address with https and a closed padlock (🔒) beside it.
- Never give sensitive info (like an account number or password) or call a number in response to a request in email or IM or on a social network.
- Think carefully before you respond to pleas for money from "family members," deals that sound too good to be true, or other possible scams.

> Parents and grandparents - have regular conversations with kids, keeping communications open

- Negotiate clear guidelines for web, mobile, and online game use that fit your children's maturity level and your family's values.
- Watch kids for signs of Internet bullying, such as being upset when online or a reluctance to go to school.
- Be the administrator of your home computer. Use age-appropriate family-safety settings to help keep track of what your kids are doing online.
- Pay attention to what kids do and who they meet online.

More info

For more online safety guidance and helpful tools, visit:

www.microsoft.com/security

www.facebook.com/saferonline

www.aarp.org/technology/safer-internet

www.twitter.com/aarptech

www.stopthinkconnect.org

This material is provided for informational purposes only. Microsoft makes no warranties, express or implied.

Source: "Connecting Generations," a 2012 study by AARP and Microsoft, available at aarp.org/technology/safer-internet.

STOP.THINK.CONNECT.™

Undergraduate Students Tip Card

DID YOU KNOW?

- 24% of all identity theft complaints made to the Federal Trade Commission are made by college students. ⁱ
- One in five U.S. teenagers who regularly log on to the Internet say they have received an unwanted sexual solicitation via the Web. ⁱⁱ
- 45% of employers use social networking sites to research job candidates. ⁱⁱⁱ

SIMPLE TIPS

- Protect all devices, such as computers, smart phones, and gaming systems that connect to the Internet from viruses and malware; only connect over a secure network.
- Keep social security numbers, account numbers, and passwords private as well as specific information about yourself, such as full name and birthdate.
- Own your online presence: set secure privacy settings on social networking websites and think twice about what you are posting and saying online.
- When banking and shopping, make sure the site is security enabled with “https://” or “shttp://.”
- Think before you act: be wary of messages that implore you to act immediately, offer something that sounds too good to be true, or ask for personal information.
- Speak up. If you see something in appropriate, let the website know.

RESOURCES AVAILABLE TO YOU

- *OnGuardOnline.gov*
 - Learn the experts’ tips for protecting your information and your computer while online, including mobile app basics and securing your wireless network.
- *StaySafeOnline.org*
 - Read tips and advice for college students on how to keep your devices and information safe.
- *IDtheftcenter.org*
 - Access dedicated identity theft resources along with victim and consumer support help.

IF YOU ARE A VICTIM OF ONLINE CRIME

- Immediately change all passwords; financial passwords first. Do not use that password in the future.
- Disconnect your computer from the Internet.
- Restart your computer in safe mode and back up your data.
- Report stolen finances or identities and other cybercrime to the Internet Crime Complaint Center at <http://www.ic3.gov>.
- Report the attack to your university and the local authorities.
- File a report with the U.S. Computer Emergency Readiness Team at <http://www.us-cert.gov> and the Federal Trade Commission at <http://www.ftccomplaintassistant.gov>.



**Homeland
Security**



STOP | THINK | CONNECT™

Stop.Think.Connect. is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family, and your community. For more information visit <http://www.dhs.gov/stopthinkconnect>.

ⁱ ITRC Solution 26 – College Students and Identity Theft Identity Theft Resource Center. February 2, 2010.
http://www.idtheftcenter.org/artman2/publish/c_guide/Solution_26_-_College_Students_and_Identity_Theft.shtml

ⁱⁱ Crimes Against Children Research Center

ⁱⁱⁱ 2009 Careerbuilder Survey

<http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr519&sd=8/19/2009&ed=12/31/2009>



**Homeland
Security**



STOP | THINK | CONNECT

STOP.THINK.CONNECT.™

Young Professionals

DID YOU KNOW?

- Young adults aged 20-39 collectively made up 45% of all identity theft victims in 2010. ⁱ
- Only 44% of adults aged 18-29 limit the amount of personal information they share online, and 33% of adults aged 30-49 do the same. ⁱⁱ
- 45% of employers use social networking sites to research job candidates. ⁱⁱⁱ
- Nearly 33% of young adults work for a company that has a policy about self-presentation online. ^{iv}

SIMPLE TIPS

- Protect all devices that connect to the Internet: Along with computers, smart phones, gaming systems, and other web-enabled devices also need protection from viruses and malware.
- Own your online presence: Set secure privacy settings on social networking websites and think twice about what you are posting and saying online.
- When banking and shopping, check to be sure the sites is security enabled with “https://” or “shttp://”
- Think before you act: Be wary of messages that implore you to act immediately, offer something that sounds too good to be true, or ask for personal information.
- Encourage your colleagues, families, and communities to be web wise.

RESOURCES AVAILABLE TO YOU

- *US-CERT.gov*
 - US-CERT provides tips for both individuals and organizations on how to protect against cyber threats. Visit <http://www.us-cert.gov/cas/tips/> for more information.
- *Justice.gov*
 - The Department of Justice Computer Crime and Intellectual Property Section (CCIPS) tells you where to report hacking, password trafficking, spam, child exploitation and other Internet harassment. Visit <http://www.justice.gov/criminal/cybercrime/reporting> for more information.
- *OnguardOnline.gov*
 - This website, run by the Federal Trade Commission, is a one-stop shop for online safety resources available to individuals of all ages.
- *Staysafeonline.org*
 - The National Cyber Security Alliance offers instruction on security updates, free antivirus software, malware software removal, and other services.

IF YOU ARE A VICTIM OF ONLINE CRIME

- Immediately notify your local authorities and file a complaint with the Internet Crime Complaint Center at <http://www.ic3.gov>.
- If you think a site has collected your personal information in a way that violates the law, report it to the FTC at <http://www.ftc.gov/complaint>.
- If someone has had inappropriate contact with you or a colleague, report it to <http://www.cybertipline.com> and they will coordinate with the FBI and local authorities.



Homeland
Security



STOP THINK CONNECT™

Stop.Think.Connect. is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family, and your community. For more information visit <http://www.dhs.gov/stopthinkconnect>.

ⁱ <http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/national-data.html>

ⁱⁱ <http://pewinternet.org/Presentations/2010/Jun/Four-or-More--The-New-Demographic.aspx>

ⁱⁱⁱ 2009 Careerbuilder Survey,

<http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr519&sd=8/19/2009&ed=12/31/2009>

^{iv} <http://pewinternet.org/Presentations/2010/Jun/Four-or-More--The-New-Demographic.aspx>



**Homeland
Security**



STOP | THINK | CONNECT

STOP.THINK.CONNECT.™

Looking for a Job? Cyber Tips for Young Professionals Stop.Think.Connect.™ Campaign

WHAT DOES YOUR ONLINE BRAND SAY ABOUT YOU?

As a young professional, you have grown up using computers and the Internet. However, as information you share on the Internet becomes increasingly accessible to others, what steps are you taking to protect yourself? Young professionals must now tailor their Internet behavior to protect themselves and their budding careers. It's important to determine how you will portray yourself—your personal brand—online as you look for a new job or as you grow in your current one. The Department of Homeland Security's (DHS) Stop.Think.Connect. Campaign offers you suggestions for enhancing your online brand and avoiding potential embarrassing mistakes and security pitfalls to ensure you can have a smarter, safer online experience.

56% of companies use social media sites to screen potential job candidates, according to a 2011 survey by the Society of Human Resource Management

Many young professionals are in the process of looking for a job. However, according to a 2011 survey by Microsoft, 84% of U.S. recruiters think it's proper to consider personal data posted online when evaluating a candidate and to do online research using search engines and social networking sites. When *looking for a new job*, be sure to remember these tips:

- **Rethink the Internet.** The first step in achieving a successful online presence is to understand the Internet isn't a boundless cyber-playground for you and your best friends to swap pictures and make weekend plans. Cyber criminals are lurking. Your former and future employers are likely surfing the web to find out more about you; even your grandparents may be online checking up on you. What you say and do is visible to others, and it's not erasable. With newer digital applications, even your music tastes are visible to others. Make smart choices and think about how those online decisions might influence other's opinions of you.
- **Set-up Privacy Restrictions.** Your online social media network has likely expanded to include managers and colleagues who, depending on your privacy settings, have access to your photos, comments, check-ins, and status updates. Take the time to set up the appropriate settings for the various members of your network—keep your worlds separate by customizing what your best friends see versus what your work and peripheral friends see.
- **Manage your Online Brand.** Have you checked yourself out recently online? Performing a quick search of yourself online is important to see what is being posted about you by others on the Internet. Consider setting up RSS feeds and alerts for searches on different variations of your name with your school(s), place(s) of employment, and other distinguishing details. For your social media accounts, regularly scan to see what pictures and contents others are posting about you. Make sure to get rid of any evidence of questionable behavior, whether it be in college or high school.

ON THE JOB? CYBER TIPS FOR YOUNG PROFESSIONALS

It is important to consider the consequences of bad cyber hygiene when *you're on the job*. You should be sure to remember these tips:

- **Be Device Savvy.** It's important to protect all of your devices that connect to the Internet, including computers, smart phones, gaming systems, and other web-enabled devices, from viruses and malware by avoiding phishing schemes and installing trusted anti-virus software. Also, be careful when you intermix your work and personal devices (e.g. hooking your personal phone to your work laptop). Find out your employer's rules on syncing work email to your personal smart phone to ensure that does not pose a security threat.
- **Navigate Safely.** When you're doing online banking and shopping from your office, check to be sure the sites you navigate are secure. One quick clue to determine whether a website is safe is if the URL begins with "https://." Also, when using a public computer—such as one at your local library—avoid typing personal information because of key loggers and ensure you properly log out if you check your employee webmail.
- **Think Before You Act.** You should be wary of messages that implore you to act immediately or offer something that sounds too good to be true. Never willingly provide personal information or data on your organization, including its structure and networks. When you receive suspicious e-mails like these, do not respond and delete them. Also, find out if your employer wants you to notify the IT department when you receive these types of e-mails via the company network.
- **Spread the Word.** You will be considered a cyber-savvy individual—and looked upon appreciatively by your employer—if you encourage your colleagues and clients, as applicable, to be web wise. Educate them about the Stop.Think.Connect. Campaign's efforts and suggest they get involved by sharing the information offered below.

HOW TO GET INVOLVED

Help the Campaign educate and empower the American public to take steps to protect themselves and their families online. To get involved, become a *Friend* of the Campaign by visiting <http://www.dhs.gov/stopthinkconnect>. Once you are a *Friend*, there are many ways to stay involved:

- Blog, tweet, or post about Stop.Think.Connect. and safe practices when it comes to new technology.
- Spread the word. Promote Stop.Think.Connect. messages and resources within your offices and social groups.
- Volunteer within your community to mentor kids and teens on the basics of online safety.
- Consider a career in cybersecurity if you enjoy science, technology, engineering or math.

For more information on the Stop.Think.Connect. Campaign, click [here](#). For more information about the Cyber Week Program, click [here](#).



Homeland
Security



STOP THINK CONNECT™

STOP.THINK.CONNECT.™

Parents and Educators

DID YOU KNOW?

- 95% of parents think it is necessary to talk about online security risks and behaviors with their children, but only 65% have had the “Internet talk”.ⁱ
- 68% of teens surveyed say that they have downloaded a program or software without their parent's permission.ⁱⁱ
- One in five U.S. teenagers who regularly log on to the Internet say they have received an unwanted sexual solicitation via the Web and only about 25% tell a parent or adult about it.ⁱⁱⁱ

SIMPLE TIPS FOR PROTECTING KIDS

- Create an open and honest environment with kids.
- Start conversations regularly about practicing online safety.
- Emphasize the concept of credibility to teens: not everything they see on the Internet is true and people on the Internet may not be who they appear to be.
- Watch for changes in behavior- if you child suddenly avoids the computer- it may be a sign they are being bullied online.
- Review security settings and privacy policies for the websites kids frequent. These settings are frequently updated so check back regularly.

RESOURCES AVAILABLE TO YOU

- *Cybersecurity Awareness Volunteer Education Program (C-SAVE)*
 - The National Cybersecurity Alliance developed the C-SAVE program that is accessible online at staysafeonline.org/in-the-classroom/c-save. There are age-appropriate resources to discuss Internet safety in the classroom or an assembly with all students.
- *OnguardOnline.gov*
 - This website, run by the Federal Trade Commission, is a one-stop shop for online safety resources available to parents, educators, kids, and others.
- *Cybertipline.com*
 - The Congressionally-mandated CyberTipline, which is part of the National Center for Missing and Exploited Children (NCMEC), receives online child solicitation reports 24-hours a day, seven days a week. Submit an online report or call 1-800-843-5678.
- *Staysafeonline.org*
 - The National Cyber Security Alliance offers instruction on security updates, free antivirus software, malware software removal, and other services.

IF YOU OR A CHILD IS A VICTIM OF ONLINE CRIME

- Notify your local authorities and file a complaint with the Internet Crime Complaint Center at <http://www.ic3.gov>.
- If you think a site has collected information from your kids or marketed to them in a way that violates the law, report it to the FTC at www.ftc.gov/complaint.
- If someone has had inappropriate contact with your child, or a child you know, report it to <http://www.cybertipline.com> and the police.



Homeland
Security



STOP | THINK | CONNECT™

Stop.Think.Connect. is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family, and your community. For more information visit <http://www.dhs.gov/stophinkconnect>.

ⁱ <http://www.comcast.com/MediaLibrary/1/1/About/PressRoom/Documents/pdf/InternetSurveyChartsOct2011.pdf>

ⁱⁱ Ibid.

ⁱⁱⁱ Consumer Electronics Products and Services Usage Report, Accenture, March 2009



**Homeland
Security**



STOP THINK CONNECT™

STOP.THINK.CONNECT.™

Older Americans Tip Card

DID YOU KNOW?

- Those over the age of 65 continue to trail the national average in broadband adoption (35%), however nearly half (48%) of senior citizens are Internet users, regardless of connection type.
- Baby boomers embrace new technologies 20 times faster than members of Gen Y, including social sites, podcasts and blogs. ⁱ
- Seniors are defrauded at twice the rate of the rest of the population. ⁱⁱ

SIMPLE TIPS

- Install and regularly update firewall, antivirus, and anti-spyware programs.
- Do not open attachments, click links, or respond to email messages from unknown senders or companies that ask for your personal information.
- Do not reveal personally identifiable information such as your full name, telephone number, address, social security number, insurance policy number, credit card information, or even your doctor's name.
- Shred bank and credit card statements before throwing them in the trash; talk to your bank about using passwords and photo identification on credit cards and bank accounts.
- Beware of "free" gifts or prizes; if something is too good to be true, then it probably is.

RESOURCES AVAILABLE TO YOU

- *AARP.org*
 - What is a firewall and how do I get one? The AARP provides technology how-to guides designed specifically for you that address computer basics.
- *FBI.gov*
 - For a list of common fraud schemes aimed at older Americans, visit the Federal Bureau of Investigation (FBI) at <http://www.fbi.gov/scams-safety/fraud/seniors/>.
- *SeniorNet.org*
 - SeniorNet offers computer training at senior centers, public libraries, schools, and hospitals as part of their mission to provide older adults computer technology education.

IF YOU ARE A VICTIM OF ONLINE CRIME

- Notify your local authorities and file a complaint with the Internet Crime Complaint Center at <http://www.ic3.gov>.
- If you have been a victim of identity theft, follow the steps provided by the Federal Trade Commission (<http://www.ftc.gov>) to recover and respond to identity theft.

Stop.Think.Connect. is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family, and your community. For more information visit <http://www.dhs.gov/stopthinkconnect>.

ⁱ Consumer Electronics Products and Services Usage Report, Accenture, March 2009

ⁱⁱ National Association of Triads, Inc.



Homeland
Security



STOP THINK CONNECT™

STOP.THINK.CONNECT.™

Cyber Tips for Older Americans

WHAT IS CYBERSECURITY

Cybersecurity is general Internet safety, which includes protection of anything connected to or accessible by the Internet- from networks themselves to the information stored in computers. Technology has changed tremendously in the past 25 years, and it only continues to advance. The Internet has brought us so many benefits; email, electronic messaging, and personal websites allow us to stay connected, informed, and involved with family and friends. The Internet also provides an easy way to shop, plan travel, and manage finances. However, with these increased conveniences comes increased risk.

Baby boomers embrace new technologies 20 times faster than members of Gen Y, including social sites, podcasts, and blogs. ⁱ

Just like any other public environment, the Internet requires awareness and caution. Just as you use locks to keep criminals out of your home, you also need safeguards to secure your computer. Many of the crimes that occur in real life are now done - or at least facilitated - through the Internet. Theft, abuse, and more can be and are being done online. Many scammers target older Americans via emails and websites for charitable donations, dating services, auctions, health care, and prescription medications.

Below are some common sense rules from the real world that apply in the online world.

- **Don't judge a book by its cover.** Cyber criminals hide behind the anonymity of the Internet. What you say and do online is visible to others, and it's not erasable. Don't communicate or reveal any personal information to strangers online. Personal information includes your name, address, age, phone number, birthday, email address, social security number, and insurance policy numbers – even your doctor's name.
- **Look before you leap.** Don't enter contests, join clubs, or share your personal information for any reason, unless you know you are on a reputable website. Do not open attachments, click links, or respond to email messages from unknown senders or companies that ask for your personal information. Most organizations – banks, charities, universities, companies, etc. - don't ask for your personal information over email. Beware of requests to update or confirm your personal information.
- **All that glitters is not gold.** Be wary of emails offering “free” gifts, prizes, or vacations. These are tricks designed to get you to give up personal information. Personal information can be pieced together to steal identities, money, or credit.
- **A chain is as strong as its weakest link.** Once we understand the dangers we face online, we need to tell other people who might not be as cyber smart and savvy. Every Internet user, no matter how young or old, is our Nation's first line of defense against people who might want to do harm. If we all become more aware of who we talk to, what we say, and what we share online we can all make a big difference.



Homeland
Security



STOP THINK CONNECT™

Protecting Against Online Fraud

Be sure to remember these tips when navigating the Internet to avoid fraud.

- **Seeking Medical Advice.** When you go to any medical-related website, be sure to consider: How current is the information? Check to see when the information was released. Do not rely on a single website for information, consult a few sources and be sure to check who exactly is providing the information. Many pharmaceutical companies create websites with information to sell products. Look for sites ending in .edu (for education) or .gov (for government).
- **Banking.** When using online banking services, check to be sure the sites you navigate are secure. One quick clue to determine whether a website is safe is if the URL begins with “https://.” When using a public computer—such as one at your local library—avoid typing your personal information. Look for the padlock icon at the bottom of your browser, which indicates the site uses encryption. Also, type website URLs directly into the address bar, do not follow links.
- **Shopping.** If you shop online, check your credit card statements as often as possible and use a credit card for online purchases. Credit cards have some protections that debit cards do not, such as the ability to question unusual charges.

Seniors are defrauded at twice the rate of the rest of the population. ⁱⁱ



Look for this padlock icon in your Internet browser when shopping and banking online.

HOW TO GET INVOLVED

Help the Campaign educate and empower the American public to take steps to protect themselves and their families online. To get involved, become a Friend of the Campaign by visiting <http://www.dhs.gov/stopthinkconnect>. Once you are a Friend, there are many ways to stay involved:

- Impress your children or grandchildren. Blog, tweet, or post about Stop.Think.Connect. and safe online behavior.
- Spread the word. Promote Stop.Think.Connect. messages and resources within your families and communities.
- Encourage your local community center, library, or to hold an educational cybersecurity program.
- Download and distribute Stop.Think.Connect. materials, such as the brochure, bookmark, and poster, in your neighborhoods and communities.
- Lead or host a cyber awareness activity in your places of work, school, recreation, or worship.
- Discuss the importance of cybersecurity with your friends and family.
- Inform your community about the Stop.Think.Connect. Campaign and available resources.
- Get your local senior center or library involved and informed on cybersecurity.

For more information on the Stop.Think.Connect. Campaign, visit <http://www.dhs.gov/stopthinkconnect>. For more information about the Cyber Tour Program, visit <http://stopthinkconnect.org/get-involved/homeland-security-campaign/cyber-week-program>.

i. Accenture

ii. National Association of Triads, Inc.

STOP.THINK.CONNECT.™

Small Business Tip Card

DID YOU KNOW?ⁱ

- 40% of all cyber-attacks target business with fewer than 500 employees.
- Only 52% of businesses have a cybersecurity plan, and 40% of businesses do not have a response plan.
- 74% of small and medium businesses reported attacks from 2009 to 2010 with an average cost of about \$190,000 per attack.

SIMPLE TIPS

- Use and regularly update antivirus and antispyware software on all computers.
- Secure your Internet connection by using a firewall, encrypt information, and hide your Wi-Fi network.
- Establish security practices and policies to protect sensitive information; educate employees and hold them accountable to the Internet security guidelines and procedures.
- Require that employees use strong passwords and regularly change them.

RESOURCES AVAILABLE TO YOU

- FCC.gov/cyberforsmallbiz
 - The Federal Communications Commission (FCC), in collaboration with government agencies and industry leaders, created the Small Biz Cyber Planner, an easy-to-use, free online tool that will help you create a customized planning guide to protect your organization from cybersecurity threats.
- US-CERT.gov
 - US Computer Emergency Readiness Team (US-CERT) distributes bulletins and alerts for both technical and non-technical users, shares cybersecurity tips, and responds to incident, phishing, and vulnerabilities report.
- USChamber.com
 - The U.S. Chamber of Commerce has an Internet Safety Toolkit that teaches employees how to help protect company information, customer data, and their own personal information.

IF YOU'VE BEEN COMPROMISED

- Inform local law enforcement of the state attorney general as appropriate.
- Report stolen finances or identities and other cybercrime to the Internet Crime Complaint Center at <http://www.ic3.gov>.
- Report fraud to Federal Trade Commission at www.ongaurdonline.gov/file-complaint. Report computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or <http://www.US-CERT.gov>.

Stop.Think.Connect. is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family, and your community. For more information visit <http://www.dhs.gov/stopthinkconnect>.

ⁱ 2009 National Small Business Cybersecurity Study, co-sponsored by the National Cyber Security Alliance (NCSA) and Symantec



STOP.THINK.CONNECT.™

Cybersecurity 101

At home, at work, and at school, our growing dependence on technology demands greater security online. Individuals are our country's first line of defense in guarding against online risks. For this reason, cybersecurity is a shared responsibility, requiring awareness and vigilance from every citizen, community, and country.

Cybersecurity is the protection of computers and computer systems against unauthorized attacks or intrusion.

The Stop.Think.Connect.™ Campaign is a national public awareness effort to guide the nation to a higher level of Internet safety by challenging the American public to be more vigilant about practicing safer online habits. The Stop.Think.Connect. Campaign's overarching goal is to help Americans understand not only the risks that come with using the Internet, but also the importance of practicing safe online behavior.

To understand and practice cybersecurity, individuals must be able to recognize risks, threats, and vulnerabilities that exist online and their impact at a national and individual level.

CYBER RISKS

- **Who:** Malicious actors intend to cause harm in cyberspace, such as a hacker stealing personal information. Benign actors accidentally cause harm to a network, system, or the Internet, such as an employee who accidentally downloads malware onto their company's network.
- **What:** Malicious actors exploit the anonymity and vulnerabilities of the Internet using methods that range in sophistication from botnets to viruses. Benign actors introduce threats through simple actions that can range from clicking on an unknown link to using a USB drive.
- **When:** It is impossible to predict when a cyber incident will occur.
- **Where:** Cyberspace, often interchanged with "the Internet," is created by and accessible through computer networks that share information and facilitate communication. Unlike the physical world, cyberspace has no boundaries across air, land, sea, and space.
- **Why:** Benign actors unintentionally and often unknowingly cause harm while malicious actors may have a range of motives, including seeking confidential information, money, credit, prestige, or revenge.

There are many risks online, some more serious than others. The majority of cybercriminals are indiscriminate; they target vulnerable computer systems regardless of whether they are part of a government agency, Fortune 500 company, a small business, or belong to a home user.

CYBER TIPS

No citizen, community, or country is immune to cyber risk, but there are steps you can take to minimize your chances of an incident:

- Set strong passwords, change them regularly, and don't share them with anyone.
- Keep your operating system, browser, and other critical software optimized by installing updates.
- Maintain an open dialogue with your friends, family, and colleagues about Internet safety.
- Use privacy settings and limit the amount of personal information you post online.
- Be cautious about offers online – if it sounds too good to be true, it probably is.

You have the opportunity to join in cybersecurity awareness efforts across the country. If you, your family, or your organization is interested in more information about cybersecurity and Stop.Think.Connect., please visit www.dhs.gov/stophinkconnect.



STOP.THINK.CONNECT.™

CYBER INCIDENT RESPONSE

Take Immediate Action

The extent, nature, and timing of cyber incidents are impossible to predict. There may or may not be any warning. Some cyber incidents take a long time (weeks, months, or years) to be discovered and identified. If you are a victim of a cyber incident, follow the steps below to mitigate and recover from the incident.

Immediate Actions	<ul style="list-style-type: none">• Check to make sure the software on all of your systems is up-to-date.• Run a scan to make sure your system is not infected or acting suspiciously.• If you find a problem, disconnect your device from the Internet and perform a full system restore.
If at Home	<ul style="list-style-type: none">• Disconnect your device (computer, gaming system, tablet, etc.) from the Internet. By removing the Internet connection, you prevent an attacker or virus from being able to access your computer and perform tasks such as locating personal data, manipulating or deleting files, or using your device to attack others.• If you have anti-virus software installed on your device, update the virus definitions and perform a manual scan of your entire system. Install all of the appropriate patches to fix known vulnerabilities.
If at Work	<ul style="list-style-type: none">• If you have access to an IT department, contact them immediately. The sooner they can investigate and clean your computer, the less damage to your computer and other computers on the network.• If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.
If at a public place (school, library, etc.)	<ul style="list-style-type: none">• Immediately inform a librarian, teacher, or manager in charge. If they have access to an IT department, contact them immediately.

Report the Incident

After taking immediate action, notify the proper authorities:

- File a report with the local police so there is an official record of the incident.
- Report online crime or fraud to your local [United States Secret Service \(USSS\) Electronic Crimes Task Force](#) or [Internet Crime Complaint Center](#).
- Report identity theft and consumer fraud to the [Federal Trade Commission](#).

Get Informed & Involved

To be on alert for current cyber news and threats, you can:

- Sign up for the United States Computer Emergency Readiness Team (US-CERT) mailing list to receive the latest cybersecurity information directly to your inbox. Written for home and business users, alerts provide timely information about current security issues and vulnerabilities. [Sign up here](#).
- Become a *Friend* of the Department of Homeland Security's Stop.Think.Connect. Campaign and receive a monthly newsletter with cybersecurity current events and tips. [Sign up here](#).



STOP | THINK | CONNECT



STOP THINK CONNECT

Keep a Clean Machine.

- **Keep security software current:** Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.
- **Automate software updates:** Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option..
- **Protect all devices that connect to the Internet:** Along with computers, smart phones, gaming systems, and other web-enabled devices also need protection from viruses and malware.
- **Plug & scan:** "USBs" and other external devices can be infected by viruses and malware. Use your security software to scan them.

Protect Your Personal Information.

- **Secure your accounts:** Ask for protection beyond passwords. Many account providers now offer additional ways for you verify who you are before you conduct business on that site.
- **Make passwords long and strong:** Combine capital and lowercase letters with numbers and symbols to create a more secure password.
- **Unique account, unique password:** Separate passwords for every account helps to thwart cybercriminals.
- **Write it down and keep it safe:** Everyone can forget a password. Keep a list that's stored in a safe, secure place away from your computer.
- **Own your online presence:** When available, set the privacy and security settings on websites to your comfort level for information sharing. It's ok to limit how and with whom you share information.

Connect with Care.

- **When in doubt, throw it out:** Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.
- **Get savvy about Wi-Fi hotspots:** Limit the type of business you conduct and adjust the security settings on your device to limit who can access your machine.
- **Protect your \$\$:** When banking and shopping, check to be sure the sites is security enabled. Look for web addresses with "https://" or "shttp://", which means the site takes extra measures to help secure your information. "Http://" is not secure.

Be Web Wise.

- **Stay current. Keep pace with new ways to stay safe online.** Check trusted websites for the latest information, and share with friends, family, and colleagues and encourage them to be web wise.
- **Think before you act:** Be wary of communications that implores you to act immediately, offers something that sounds too good to be true, or asks for personal information.
- **Back it up:** Protect your valuable work, music, photos, and other digital information by making an electronic copy and storing it safely.

Be a Good Online Citizen.

- **Safer for me more secure for all:** What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.

- **Post only about others as you have them post about you.**
- **Help the authorities fight cybercrime:** Report stolen finances or identities and other cybercrime to <http://www.ic3.gov> (Internet Crime Complaint Center), the Federal Trade Commission at <http://www.onguardonline.gov/file-complaint>.

Visit <http://www.stopthinkconnect.org> for more information.



STOP THINK CONNECT

Safety Tips for Mobile Devices

Keep a Clean Machine.

Mobile devices are computers with software that needs to be kept up-to-date (just like your PC, laptop or tablet). Security protections are built in and updated on a regular basis. Take time to make sure all the mobile devices in your house have the latest protections. This may require syncing your device with a computer.

- **Keep security software current:** Having the latest mobile security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.
- **Protect all devices that connect to the Internet:** Computers, smart phones, gaming systems, and other web-enabled devices all need protection from viruses and malware.

Protect Your Personal Information.

Phones can contain tremendous amounts of personal information. Lost or stolen devices can be used to gather information about you and, potentially, others. Protect your phone like you would your computer.

- **Secure your phone:** Use a strong passcode to lock your phone.
- **Think before you app:** Review the privacy policy and understanding what data (location, access to your social networks) on your device an app can access before you download it.
- **Only give your mobile number out to people you know and trust** and never give anyone else's number out without their permission.
- **Learn how to disable the geotagging feature on your phone** at <http://icanstalku.com/how.php#disable>.

Connect with Care.

Use common sense when you connect. If you're online through an unsecured or unprotected network, be cautious about the sites you visit and the information you release.

- **Get savvy about Wi-Fi hotspots:** Limit the type of business you conduct and adjust the security settings on your device to limit who can access your phone.
- **Protect your \$\$:** When banking and shopping, check to be sure the sites is security enabled. Look for web addresses with "https://" or "shttp://", which means the site takes extra measures to help secure your information. "Http://" is not secure.
- **When in doubt, don't respond.** Fraudulent texting, calling and voicemails are on the rise. Just like email, requests for personal information or to immediate action are almost always a scam.

Be Web Wise.

Stay informed of the latest updates on your device. Know what to do if something goes wrong.

- **Stay current. Keep pace with new ways to stay safe online.** Check trusted websites for the latest information, and share with friends, family, and colleagues and encourage them to be web wise.
- **Know how to cell block others.** Using caller ID, you can block all incoming calls or block individual names and numbers.
- **Use caution when meeting face-to-face with someone who you only "know" through text messaging.**

Even though texting is often the next step after online chatting, that does not mean that it is safer.

Be a Good Online Citizen.

It is easy to say things from via phone or text that you would never say face to face. Remind your kids to maintain the same level of courtesy on the phone as they would in the real world.

- **Safer for me more secure for all:** What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.
- **Text to others only as you would have them text to you.**
- **Only give your mobile number out to people you know and trust** and never give anyone else's number out without their permission.
- **Get permission before taking pictures or videos of others with your phone.** Likewise, let others know they need your permission before taking pictures or videos of you.

STOP. Before you use the Internet, take time to understand the risks and learn how to spot potential problems.

THINK. Take a moment to be certain the path is clear ahead. Watch for warning signs and consider how your actions online could impact your safety, or your family's.

CONNECT. Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer.

Visit <http://www.stopthinkconnect.org> for more information.



Annual Credit Report Request Form

You have the right to get a free copy of your credit file disclosure, commonly called a credit report, once every 12 months, from each of the nationwide consumer credit reporting companies, Equifax, Experian and TransUnion.

For instant access to your free credit report, visit www.annualcreditreport.com.

For more information on obtaining your free credit report, visit www.annualcreditreport.com or call 877-322-8228.

Use this form if you prefer to write to request your credit report from any, or all, of the nationwide consumer credit reporting companies. The following information is required to process your request. Omission of any information may delay your request.

Once complete, fold (do not staple or tape), place into a #10 envelope, affix required postage and mail to:
Annual Credit Report Request Service P.O. Box 105281 Atlanta, GA 30348-5281.

Please use a Black or Blue Pen and write your responses in PRINTED CAPITAL LETTERS without touching the sides of the boxes like the examples listed below:



Social Security Number:

Date of Birth:

Month

Day

Year

Fold Here

Fold Here

First Name

M.I.

Last Name

JR, SR, III, etc.

Current Mailing Address:

House Number

Street Name

Apartment Number / Private Mailbox

For Puerto Rico Only: Print Urbanization Name

City

State

ZipCode

Previous Mailing Address (complete only if at current mailing address for less than two years):

House Number

Street Name

Fold Here

Fold Here

Apartment Number / Private Mailbox

For Puerto Rico Only: Print Urbanization Name

City

State

ZipCode

Shade Circle Like This →

Not Like This →

I want a credit report from (shade each that you would like to receive):

- Equifax
- Experian
- TransUnion

Shade here if, for security reasons, you want your credit report to include no more than the last four digits of your Social Security Number.



If additional information is needed to process your request, the consumer credit reporting company will contact you by mail.

Your request will be processed within 15 days of receipt and then mailed to you.

