

# Crime Prevention News

## IDENTITY FRAUD



What's on your Facebook? A commonly used social network known as Facebook is used by thousands of college students in the United States. But, how safe is it? There have been reports of identity theft as well as stalking and even sexual assaults associated with the web site due to the types of information listed on it. Listings that include full names, addresses, dates of birth, high school locations, and cell phone numbers add to this dangerous mix.

Reports of identity theft continue to increase in the United States due to the advances in technology. There were ten million people in the United States that fell victim to identity theft in 2003. Identity theft really is a case of identity fraud because in reality the only thing that someone *can't* steal from you is your personal identity.

**“But he that filches from me my good name/ Robs me of that which not enriches him/And makes me poor indeed.” - Shakespeare, *Othello*, act iii. Sc. 3.**

precautions to protect yourself from identity theft.

Unlike your fingerprints which are unique to you and cannot be given to someone else for their use your personal data such as your Social Security number, your bank account or credit card number, your telephone calling card number, and other valuable identifying data - can be used if they fall into the wrong hands to personally profit at your expense.

In the United States and Canada many people have reported that unauthorized persons have taken funds out of their bank or financial accounts and in the worst cases, taken over their identities altogether running up vast debts and committing crimes while using the victim's names.

---

**10 Million ID theft cases**

**were reported in 2003.**

**Victims spent an average**

**of \$1800.00 and 105 hours**

**to correct the damage.**

---

In many cases, a victim's losses may include not only out-of-pocket financial losses, but substantial additional financial costs associated with trying to restore his or her reputation in the community and correcting erroneous information for which the criminal is responsible.

In one notorious case of identity theft, the criminal, a convicted felon, not only incurred more than \$100,000 of credit card debt, obtained a federal home loan, and bought homes, motorcycles, and handguns in the victim's name, but called his victim to taunt

him saying that he could continue to pose as the victim for as long as he wanted because identity theft was not a federal crime at that time.

Before filing for bankruptcy, also in the victim's name, the victim and his wife spent four years and more than \$15,000 of their own money to restore their credit and reputation. The criminal served a brief sentence for making a false statement to procure a firearm, but made no restitution to his victim for any of the harm he had caused. This case, and others like it, prompted Congress in 1998 to create a new federal offense of identity theft.

(1)



University of Iowa  
Police

323 S. Madison St.  
Iowa City, IA. 52242  
Ph. (319) 335-5022

The short answer is that identity theft is a crime. Identity theft and identity fraud are terms 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 issue of the Crime Prevention News is intended to explain why you need to take

### **How can I minimize my risk?**

When it comes to identity theft, you can't entirely control whether you will become a victim. But there are certain steps you can take to minimize your risk.

### **Credit report:**

Order a copy of your credit report. An amendment to the federal Fair Credit Reporting Act requires each of the major nationwide consumer reporting companies to provide you with a free copy of your credit reports, at your request, once every 12 months.

To order your free annual report from one or all the national consumer reporting companies, visit [www.annualcreditreport.com](http://www.annualcreditreport.com), call toll-free 877-322-8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print the form from [ftc.gov/credit](http://ftc.gov/credit). Do not contact the three nationwide consumer reporting companies individually; they provide free annual credit reports only through [www.annualcreditreport.com](http://www.annualcreditreport.com), 877-322-8228, and Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Under federal law, you're also entitled to a free report if a company takes adverse action against you, such as denying your application for credit, insurance or employment, and you request your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the consumer reporting company that supplied the information about you. You're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; you're on welfare; or your report is inaccurate because of fraud. Otherwise, a consumer reporting company may charge you up to \$9.50 for any other copies of your report.

### **To buy a copy of your report, contact:**

Equifax: 800-685-1111; [www.equifax.com](http://www.equifax.com)

Experian: 888-EXPERIAN (888-397-3742); [www.experian.com](http://www.experian.com)

TransUnion: 800-916-8800; [www.transunion.com](http://www.transunion.com)

Under state law, consumers in Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, and Vermont already have free access to their credit reports.

If you ask, only the last four digits of your Social Security number will appear on your credit reports.

### **Secure your passwords.**

Place passwords on your credit card, bank, and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number or your phone number, or a series of consecutive numbers. When opening new accounts, you may find that many businesses still have a line on their applications for your mother's maiden name. Ask if you can use a password instead.

Secure personal information in your home, especially if you have roommates, employ outside help, or are having work done in your home.



[www.uowa.edu/~pubsfty](http://www.uowa.edu/~pubsfty)

*University of  
Iowa  
Police  
323 S. Madison  
St.  
Iowa City, IA.  
Ph. (319) 335-  
5022*

*Crime Prevention  
News*

## Crime Prevention News

Volume 5, Issue 1, January/February 2006

### **Obtain information to secure your identity.**

Ask about information security procedures in your workplace or at businesses, doctor's offices or other institutions that collect your personally identifying information. Find out who has access to your personal information and verify that it is handled securely. Ask about the disposal procedures for those records as well. Find out if your information will be shared with anyone else. If so, ask how your information can be kept confidential.

Don't give out personal information on the phone, through the mail, or on the Internet unless you've initiated the contact or are sure you know who you're dealing with. Identity thieves are clever, and have posed as representatives of banks, Internet service providers (ISPs), and even government agencies to get people to reveal their Social Security number, mother's maiden name, account numbers, and other identifying information. Before you share any personal information, confirm that you are dealing with a legitimate organization. Check an organization's website by typing its URL in the address line, rather than cutting and pasting it. Many companies post scam alerts when their name is used improperly. Or call customer service using the number listed on your account statement or in the telephone book.

### **Treat your mail and trash carefully.**

Deposit your outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox. Promptly remove mail from your mailbox. If you're planning to be away from home and can't pick up your mail, call the U.S. Postal Service at 1-800-275-8777 to request a vacation hold. The Postal Service will hold your mail at your local post office until you can pick it up or are home to receive it.

To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you're discarding, and credit offers you get in the mail. To opt out of receiving offers of credit in the mail, call: 1-888-5-OPTOUT (1-888-567-8688). The three nationwide consumer reporting companies use the same toll-free number to let consumers choose not to receive credit offers based on their lists. **Note:** You will be asked to provide your Social Security number which the consumer reporting companies need to match you with your file.

### **Don't carry your Social Security number card; leave it in a secure place.**

Give your Social Security number only when absolutely necessary, and ask to use other types of identifiers. If your state uses your Social Security number as your driver's license number, ask to substitute another number. Do the same if your health insurance company uses your Social Security number as your policy number. Carry only the identification information and the credit and debit cards that you'll actually need when you go out.

Be cautious when responding to promotions. Identity thieves may create phony promotional offers to get you to give them your personal information.

Keep your purse or wallet in a safe place at work; do the same with copies of administrative forms that have your sensitive personal information.

When ordering new checks, pick them up from the bank instead of having them mailed to your home mailbox.

#### **I have a computer and use the Internet. What should I be concerned about?**

You may be careful about locking your doors and windows, and keeping your personal papers in a secure place. Depending on what you use your personal computer for, an identity thief may not need to set foot in your house to steal your personal information. You may store your Social Security number, financial records, tax returns, birth date, and bank account numbers on your computer. These tips can help you keep your computer – and the personal information it stores – safe.

Virus protection software should be updated regularly, and patches for your operating system and other software programs should be installed to protect against intrusions and infections that can lead to the compromise of your computer files or passwords. Ideally, virus protection software should be set to automatically update each week. The Windows XP operating system also can be set to automatically check for patches and download them to your computer.

Do not open files sent to you by strangers, or click on hyperlinks or download programs from people you don't know. Be careful about using file-sharing programs. Opening a file could expose your system to a computer virus or a program known as "spyware," which could capture your passwords or any other information as you type it into your keyboard.

Use a firewall program, especially if you use a high-speed Internet connection like cable, DSL or T-1 that leaves your computer connected to the Internet 24 hours a day. The firewall program will allow you to stop uninvited access to your computer. Without it, hackers can take over your computer, access the personal information stored on it, or use it to commit other crimes.

Use a secure browser – software that encrypts or scrambles information you send over the Internet – to guard your online transactions. Be sure your browser has the most up-to-date encryption capabilities by using the latest version available from the manufacturer. You also can download some browsers for free over the Internet. When submitting information, look for the "lock" icon on the browser's status bar to be sure your information is secure during transmission.

Try not to store financial information on your laptop unless absolutely necessary. If you do, use a strong password with a combination of letters (upper and lower case), numbers and symbols. A good way to create a strong password is to think of a memorable phrase and use the first letter of each word as your password, converting some letters into numbers that resemble letters. For example, "I love Felix; he's a good cat," would become 1LFHA6c. Don't use an automatic log-in feature that saves your user name and password, and always log off when you're finished. That way, if your laptop is stolen, it's harder for a thief to access your personal information.

Before you dispose of a computer, delete all the personal information it stored. Deleting files using the keyboard or mouse commands or reformatting your hard drive may not be enough because the files may stay on the computer's hard drive, where they may be retrieved easily. Use a "wipe" utility program to overwrite the entire hard drive.

Look for website privacy policies. They should answer questions about maintaining accuracy, access, security, and control of personal information collected by the site, how the information will be used, and whether it will be provided to third parties. If you don't see a privacy policy or if you can't understand it consider doing business elsewhere.

# THE UNIVERSITY OF IOWA POLICE

## Crime Prevention News

Volume 5, Issue 1, January/February 2006

### Identity Fraud - *continued*

Page 5

#### **What is an active duty military alert?**

If you are a member of the military and away from your usual duty station, you may place an active duty alert on your credit reports to help minimize the risk of identity theft while you are deployed. Active duty alerts are in effect on your report for one year. If your deployment lasts longer, you can place another alert on your credit report.

When you place an active duty alert, you'll be removed from the credit reporting companies' marketing list for pre-screened credit card offers for two years unless you ask to go back on the list before then.

The process for getting and removing an alert, and a business's response to your alert, are the same as that for an initial alert. You may use a personal representative to place or remove an alert.

#### **Are companies allowed to print my entire credit card number on my receipt?**

Beginning December 5, 2006, companies must not print your credit or debit card expiration date or more than the last 5 digits of your card number on your electronic receipt. Some businesses must make this change sooner, depending on the way they process credit card transactions. The law will allow receipts that are hand written or mechanically imprinted to show your entire number and expiration date, even after December 4, 2006.

#### **How can I stop companies from using my personal information for marketing?**

More organizations are offering consumers choices about how their personal information is used. For example, many let you "opt out" of having your information shared with others or used for marketing purposes. You also can visit Privacy Initiatives and the National Do Not Call Registry.

#### **When should I give out my Social Security number?**

Your employer and financial institutions will need your Social Security number for wage and tax reporting purposes. Other businesses may ask you for your Social Security number to do a credit check if you are applying for a loan, renting an apartment, or signing up for utilities. Sometimes, however, they simply want your Social Security number for general record keeping. If someone asks for your Social Security number, ask:

Why do you need my Social Security number?

How will my Social Security number be used?

How do you protect my Social Security number from being stolen?

What will happen if I don't give you my Social Security number?

If you don't provide your Social Security number, some businesses may not provide you with the service or benefit you want. Getting satisfactory answers to these questions will help you decide whether you want to share your Social Security number with the business.

The decision to share is yours.



## Crime Prevention News

Volume 5, Issue 1, January/February 2006

### *Identity Fraud - continued*

#### **Should I buy identity theft insurance?**

Some companies offer insurance or similar products that claim to give you protection against the costs associated with resolving an identity theft case. Be aware that most creditors will only deal with you to resolve problems, so the insurance company in most cases will not be able to reduce that burden. As with any product or service, make sure you understand what you're getting before you buy. If you decide to buy an identity theft insurance product, check out the company with your local Better Business Bureau, consumer protection agency and state Attorney General to see if they have any complaints on file.

#### **How not to get hooked on a "phishing" scam**

**"We suspect an unauthorized transaction on your account.  
To ensure that your account is not compromised,  
please click the link below and confirm your identity."**

**"During our regular verification of accounts, we couldn't verify your information.  
Please click here to update and verify your information."**

Have you received email with a similar message? It's a scam called "phishing" — and it involves Internet fraudsters who send spam or pop-up messages to lure personal information (credit card numbers, bank account information, Social Security number, passwords, or other sensitive information) from unsuspecting victims.

According to the Federal Trade Commission (FTC), the nation's consumer protection agency, phishers send an email or pop-up message that claims to be from a business or organization that you may deal with — for example, an Internet service provider (ISP), bank, online payment service, or even a government agency. The message may ask you to "update," "validate," or "confirm" your account information. Some phishing emails threaten a dire consequence if you don't respond. The messages direct you to a website that looks just like a legitimate organization's site. But it isn't. It's a bogus site whose sole purpose is to trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

#### **The FTC suggests these tips to help you avoid getting hooked by a phishing scam:**

- If you get an email or pop-up message that asks for personal or financial information, do not reply. And don't click on the link in the message, either. Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization mentioned in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address yourself. In any case, don't cut and paste the link from the message into your Internet browser — phishers can make links look like they go to one place, but that actually send you to a different site.
- Use anti-virus software and a firewall, and keep them up to date. Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge. Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically. A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection. Operating systems (like Windows or Linux) or browsers (like Internet Explorer or Netscape) also may offer free software "patches" to close holes in the system that hackers or phishers could exploit.

## Crime Prevention News

Volume 5, Issue 1, January/February 2006

### *Identity Fraud - continued*

- Don't email personal or financial information. Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
- Review credit card and bank account statements as soon as you receive them to check for unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security.
- Forward spam that is phishing for information to [spam@uce.gov](mailto:spam@uce.gov) and to the company, bank, or organization impersonated in the phishing email. Most organizations have information on their websites about where to report problems.

If you believe you've been scammed, file your complaint at [ftc.gov](http://ftc.gov), and then visit the FTC's Identity Theft website at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft). Victims of phishing can become victims of identity theft. While you can't entirely control whether you will become a victim of identity theft, you can take some steps to minimize your risk. If an identity thief is opening credit accounts in your name, these new accounts are likely to show up on your credit report. You may catch an incident early if you order a free copy of your credit report periodically from any of the three major credit bureaus. See [www.annualcreditreport.com](http://www.annualcreditreport.com) for details on ordering a free annual credit report.(2)

You can learn other ways to avoid email scams and deal with deceptive spam at [ftc.gov/spam](http://ftc.gov/spam).

#### **RULES TO REMEMBER:**

**NEVER THROW CREDIT CARD OFFERS IN THE TRASH- SHRED THEM.**

**LIMIT YOUR INFORMATION ON FACEBOOK AND LIMIT WHO CAN READ YOUR PROFILE.**

**DON'T GIVE OUT PERSONAL INFORMATION OVER THE PHONE OR COMPUTER IF YOU ARE NOT 100% SURE WHO'S REQUESTING THE INFORMATION.**

**DON'T GIVE PERSONAL INFORMATION TO MAGAZINE SALESPEOPLE.**

**GUARD YOUR PERSONAL INFORMATION AND CREDENTIALS WHEN TRAVELLING, ESPECIALLY WHEN VISITING HIGH DESTINATION LOCATIONS WHILE ON SPRING BREAK.**

Sources: 1. United States of America, Department of Justice, "Identity Theft and Fraud" 9th January 2006, 20th. January 2006 <http://www.usdoj.gov/criminal/fraud/idtheft.html>

2. United States of America, Federal Trade Commission, " How Not to Get Hooked by a "Phishing" Scam" June 2005, 20th January 2006 <http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.pdf>