



UNIVERSITY OF HOUSTON
Learning. Leading.™

INFORMATION TECHNOLOGY

JULY 2006

KEEPING YOUR COMPUTER SAFE IDENTITY THEFT AND FRAUD • ISSUE #3

IT SUPPORT CENTER

PHONE SUPPORT

713.743.1411

24 hours a day, 7 days a week
(except University holidays)

WALK-UP SUPPORT

Philip Guthrie Hoffman Hall
(PGH), Room 116
Monday through Friday
8 a.m. to 8 p.m.
(except University holidays)

EMAIL SUPPORT

support@uh.edu

You can also request IT support from any computer by using the online support form at

www.uh.edu/infotech/help

CUSTOMER FEEDBACK

We're constantly seeking ways to better serve you, so if you have any thoughts or ideas as to how we can better support you through new or existing IT products or services, please let us know.

To provide feedback, please contact the IT Support Center at 713.743.1411 or email support@uh.edu

“How serious are Identity Theft and Fraud, and what can I do to protect myself from them?”

ID Theft and Fraud Statistics

This third—and final—newsletter in our series on identity theft and fraud focuses on how to avoid becoming a crime victim, and what you can do if you find yourself in the unfortunate circumstance of being one.

But first, here are some updated facts about identity theft and fraud, which are on the increase in the U.S. and worldwide:


- Identity theft affects nine million Americans annually (up from seven million just two years ago).
- Identity theft again topped the Federal Trade Commission's (FTC) fraud complaint list in 2005.
- The financial costs associated with identity theft are dramatic, exceeding \$52.6 billion in 2004, according to FBI statistics.
- Because identity theft is often misclassified, thieves have about a one in 700 chance of being caught by federal authorities. (Gartner Group, July 2003).

Numbers and statistics cannot adequately measure the destructive impact these crimes have on victim's lives. Interviews with hundreds of victims have found that the emotional impact of identity theft parallels that of victims of violent crimes. The fact that the average victim spends nearly 600 hours and \$6,383 striving to recover from the consequences of identity theft and fraud may help explain why.

Make Secure Online Purchases

As increasing numbers of us are turning to the Internet for online purchases because of convenience and price, huge opportunities have opened up for online thieves. Cybercrimes related to online transactions are skyrocketing, and recent surveys indicate that the majority of these crimes involve the opening of a credit card or a takeover of a card account.

In order to practice safe online transactions, the FTC suggests these protections:

- Use a browser that uses a Secure Sockets Layer (SSL), an Internet security protocol used by browsers and Web servers to transmit sensitive information. You can confirm you're on a SSL by checking the URL: the "http://" at the beginning of the address will change to "https://" on a secure site.
- Look for digital certificates that authenticate the company you're dealing with. Web sites that sell items or services online often include the VeriSign logo. Clicking on the logo assures that the site is legitimate, instead of a clone set up to collect your personal and financial information. 
- Deal with recognized retailers and vendors, and be wary of companies with unfamiliar names and vendors who identify themselves using an online nickname.
- Only use one credit card for all your online purchases.
- Never give out passwords or user ID information online unless you know who you're dealing with and why the information is needed.
- Keep good records of your Internet transactions and review your credit card statements to make sure charges are correct.
- Check your email after you've made an online purchase, as merchants often send confirmation emails about orders.

Defend Yourself: FBI Tips

The FBI offers these additional safe-computing tips to help you reduce your risks from identity theft and fraud:

- Be cautious when receiving an unsolicited email that asks you, either directly or through a Web site, for personal, financial, or identity information (Social Security number, passwords, or other identifiers).

Continued on back

- Take note of the header address on the Web site. Most legitimate sites will have a short Internet address that usually depicts the business name followed by “.com” or “.org.”
- If you have any doubts about an email or Web site, contact the company directly.
- If you’ve been victimized, contact your local police or sheriff’s department and file a complaint with the FBI’s Internet Fraud Complaint Center at www.IFCCFBI.gov.

Additional Recommendations

Here are other actions you should take to protect yourself and your computer from identity thieves:

- Keep your virus protection software updated, and make sure patches for your operating system (OS) and other software programs are installed and kept up to date.
- Never open files sent to you by strangers, or click on hyperlinks or download programs from people you don’t know.
- Use unique passwords on devices containing your personal information (PDAs, cell phones, laptops/desktops) and change your passwords every three or four months.
- Use email-based account alerts to monitor money transfers, payments, low balances, and withdrawals.
- Be careful about using file-sharing programs that can expose your system to viruses or spyware, which can capture your passwords or other personal information.
- Use a firewall program, especially if you use a high-speed Internet connection (cable, DSL, or T-1) that has your computer connected to the Internet 24 hours a day.
- Don’t store financial information on a laptop unless absolutely necessary. Laptops are prime targets for thieves.
- Don’t use an automatic login feature that saves your user name and password, and always logoff when you’re done.
- Cancel paper bills and statements wherever possible; instead pay bills and check financial statements online.

When You Realize You’re a Victim

If you know—or suspect—that you’re a victim of identity theft or fraud you need to take action as quickly as possible. Armed with your stolen information, a thief will work quickly to cash in on it. Any delay on your part gives him (or her) a head start toward wrecking your finances.

1. Report the crime to the police and get a copy of your police report or case number, as most credit card companies, banks, and other institutions request this information in order to confirm that a crime has actually occurred.
2. Contact your credit card issuers and close your existing accounts. Get replacement cards with new numbers, and ask that your old accounts show that they were closed at the consumer’s request for credit reporting purposes.
3. Contact the agency that issued your lost or stolen driver’s license and other government-issued identification and have the documents cancelled. Request a replacement, and ask that your file be flagged so that no one else can obtain a license or other identification document in your name.
4. File a complaint with the FTC by contacting their Consumer Response Center at 1-877-ID-THEFT (438-4338), or by downloading a complaint form at www.ftc.gov/ftc/complaint.htm.
5. Call the toll-free number of any of the three nationwide consumer reporting companies and place an initial fraud alert on your credit reports. The companies are:

Equifax (www.equifax.com), 1-888-766-0008.

Experian (www.experian.com), 1-888-EXPERIAN.

TransUnion (www.transunion.com), 1-800-680-7289.

Request that your accounts be flagged with a “fraud alert,” which prevents someone from setting up a new account in your name without the creditor first calling you. This flag, also known as a “victim’s statement,” is the best way to prevent unauthorized accounts from being opened.

6. Monitor your financial records for several months after you’ve discovered the crime, and check your credit reports every three months in the first year of the theft and once a year thereafter. **Note:** The Fair Credit Reporting Act requires each of the major consumer reporting companies to provide you with a free copy of your credit report, at your request, once every 12 months.
7. Close any accounts a thief has opened in your name. If you open new accounts, request that they be password protected, and make sure your passwords are unique and hard to guess....not your mother’s maiden name, a pet’s name, or the last four digits of your Social Security number.
8. Keep a detailed log of all conversations you have with authorities and financial entities; keep detailed records of all actions you take; make and keep copies of all documentation you provide; and create and maintain a contact list of everyone you speak to.

Your Rights as a Victim

According to the FTC’s Consumer Response Center, the Fair Credit Reporting Act (FCRA) gives you specific rights when you are, or believe you are, the victim of identity theft. Detailed information can be found on the FTC Identity Theft Web site at www.consumer.gov/idtheft, or by calling 1-877-ID-THEFT.

Other Resources

The following additional resources provide a wealth of useful information about identity theft and fraud for consumers:

Federal Trade Commission’s Identity Theft Web site at www.consumer.gov/idtheft. *The FTC serves as the government’s central clearinghouse for identity theft and fraud information.*

U.S. Treasury Department at www.ustreas.gov/ offers a free 80 minute DVD, “Identity Theft: Outsmarting the Crooks.” *This DVD explains the topic, and includes ways to protect against fraud as well as what to do if you’re victimized.*

Texas Attorney General Web site at www.oag.state.tx.us/. *This site offers useful information, including how to file a complaint and how to report possible illegal online activity.*

U.S. Department of Justice Identity Theft and Fraud Web site at www.usdoj.gov/criminal/fraud/idtheft.html. *This site provides a large amount of general and specific information and resources for consumers.*

Want Information About IT?

ASKSHASTA, at www.uh.edu/askshasta, is a good place to start for questions about IT-related issues.

Information Technology contact information is located on the front page.