



UNIVERSITY OF HOUSTON
Learning. Leading.™

INFORMATION TECHNOLOGY

FEBRUARY 2006

KEEPING YOUR COMPUTER SAFE IDENTITY THEFT AND FRAUD • PART 2

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 by calling
713.743.1411 or emailing
support@uh.edu

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

Conventional Crimes

Last November's issue of the IT Newsletter, (read the online version at www.uh.edu/infotech/news/story.php?story_id=842.) introduced the subject of identity theft and fraud. It provided definitions and statistics for these crimes, including this sobering statistic: nearly 20,000 people become victims of identity theft crimes each day.

The newsletter showed how easy it is for thieves to steal your information, what they can do with it once they have it, and the fact that the rich and famous aren't the only targets of identity thieves and fraudsters.

The focus of that newsletter was on traditional identity theft and fraud, which includes, among other things, dumpster diving, stolen documents, copied credit card numbers, and the removal of financial papers from mailboxes. This focus was taken because statistics indicate that the majority of identity thefts (68.2 percent) occur through “conventional” methods.

Computer-Related Crimes

However, due to UH's large concentration of computers and computer users, and because computer-related identity theft and fraud has become such a major threat, the focus of this and the next issue of the IT Newsletter is on computer-related crimes.

Identity fraud crimes committed via computers are an increasingly serious problem. According to Federal Trade Commission (FTC) figures, last year 11.6 percent of all reported cases of identity theft and fraud were committed through the use of computers. This translates to over two million adult U.S. Internet users who were victimized. And in 2005, computer-related identity thefts again topped the list of fraud complaints reported to the FTC, with Internet-related complaints accounting for nearly half (46 percent) of the reports.

Academic Institutions

Academic institutions present a special security problem because of their need to maintain the free exchange of ideas and information between faculty, students, and researchers, both on campuses and between universities.

Unlike corporations, which can set up elaborate cyber-defenses to fend off attacks from hackers, universities cannot rely entirely on the use of enterprise firewalls to keep computer identity thefts and other security threats out. “Universities try to foster a more open environment, so individuals have freedom to do things like collaborate on research or do things with other universities,” said Michael Gavin, a senior analyst at Forrester Research. “Universities, as a result, are reluctant to put in security measures that would prevent people from collaborating.”

Because of their need for “open environment” computing, U.S. universities were prime targets of hackers last year. A number of major security incidents occurred at U.S. universities, including one at the University of North Texas, where hackers accessed the housing and financial aid records of nearly 39,000 students and alumni.

With so many instances of hackers exploiting vulnerabilities within universities computer systems, it's important that UH users do their part to mitigate these threats.

Virtual Identity Thieves

The goal of virtual identity thieves is the same as with conventional identity thieves: they want to steal your personal information, create a new identity based on this information, then use “your” new identity for their illegal purposes and gain.

Protection from virtual thieves requires the same diligence as for conventional identity thieves, only from a technical approach. For example, you're very conscient-

Continued on back

tious about locking the windows and doors of your home and auto. But a virtual thief doesn't need to set foot in your house or break your car's window to steal your information. Storing your Social Security number, financial records, tax returns, birth date, and bank account numbers on your computer places you at risk.

Armed with just a one or two items of personal information, virtual thieves can do the same things to you-in your name-that conventional thieves can, including:

- Contact your credit card issuer to change the billing address on your account, then run up charges.
- Open new credit card accounts, then use the cards to run up large bills.
- Establish phone, wireless, or utilities services.
- Authorize electronic transfers and quickly drain your account.
- File for bankruptcy to avoid paying debts incurred under your name.
- Purchase a car by taking out an auto loan.
- Obtain a job, file fraudulent tax returns, or falsely obtain medical care.
- Give your name to the police during an arrest.

Spyware

Spyware messages are a primary method computer identity thieves use in order to infiltrate and compromise computers and steal information from them. Spyware is delivered in many forms, including hijackers, worms, Trojan Horses, and viral marketing programs. However it shows up on your computer, spyware is engineered to self-install without your knowledge or consent in order to monitor and/or control your computer use. Once installed, spyware can be used to send you pop-up ads, redirect your computer to Web sites you haven't selected, monitor your Internet surfing, or record your keystrokes. Any of these can lead to identity theft.

Spyware is so ubiquitous that in late 2004, the number of infected computers reached an all-time high of 92 percent, and 89 percent of users of these computers had no idea the malware was present according to data from Consumer SpyAudit.

Individuals, universities, and corporations all receive spyware on a regular basis, and governmental entities are not immune from the problem, either. In one notable incident, an Oklahoma sheriff's department was attacked by spyware that allowed a hacker unauthorized access to sensitive information about prisoner transfers, personnel files, and more importantly, U.S. Homeland Security information.

Since the odds favor your computer being infected with spyware, you need to be aware of these warning signs:

- You start receiving a barrage of pop-up ads.
- Your browser suddenly takes you to sites other than those you type into the address box.
- You experience a change to your Internet home page, with new and unexpected toolbars suddenly appearing.
- You notice new and unexpected icons on the system tray at the bottom of your computer screen.
- Your keyboard keys start acting erratically.
- You start receiving random error messages.
- Your computer exhibits sluggish and slow performance.

You also need to take specific actions to reduce your risk of spyware infections. The FTC recommends the following:

- Update your operating system (OS) and Web browser software, and keep both up-to-date.
- Download free software (shareware) only from sites you

know and trust.

- Don't install software without knowing exactly what it is, what it does, and who it came from.
- Minimize "drive-by" downloads by setting your browser security setting to medium or higher.
- Never click on links within pop-up windows.
- Never click on a link in a spam message that claims to offer anti-spyware software. Doing so may actually install spyware on your system.
- Install a personal firewall to prevent uninvited users from accessing your computer.

For more information about spyware, and its close cousin adware, go to the story on the IT News Web site at www.uh.edu/infotech/news/story.php?story_id=743.

Phishing Messages

If you've received a message like this—"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information," or "Please contact us immediately about your account"—you very likely were the recipient of a "phishing" message.

Phishing messages are usually delivered in the form of spam or pop-ups that appear to originate from businesses or organizations you do business with. These can include financial institutions, Internet service providers (ISPs), online bill payment services, your employer, or even a government agency. Phishing messages almost always contain a link to an authentic, legitimate-looking Web site that's engineered to entice you into divulging your credit card numbers, bank account information, Social Security number, passwords, or other sensitive personal information. Phishers are so effective in their deception that in 2004, according to Gartner estimates, 2.4 million online shoppers were fooled into losing money as a direct result of phishing.

For more information on phishing schemes, including actions you can take to avoid getting hooked by a phisher, read our story on the IT Web site at www.uh.edu/infotech/news/story.php?story_id=802.

Other Malware

Trojan horses, which had the biggest growth last year among malware programs, pretend to be legitimate software but actually carry out hidden, harmful functions. Recent Trojans have arrived as email messages with attachments appearing as Microsoft security updates, but turn out to be viruses that attempt to disable antivirus and firewall software.

Keyloggers, and worms with "bot" code, are two other popular methods used by hackers to steal sensitive personal data. All of these threats are mitigated by safe computing practices, which rely on user interventions and precautions.

Next Newsletter

The final installment in this three-part series on identity theft and fraud will provide information on how to make secure online purchases, give you even more tips on how to defend yourself from computer-related identity theft, and tell you what actions to take in case you become a victim of the crime. It will also point you to Web and print resources that you can access in order to find out more about these threats.

Want More Information?

ASKSHASTA is a good place to start. www.uh.edu/askshasta.

IT contact information is located on the front page.