

We're on the  
Web!

See us at:  
[www.bc.edu/audit](http://www.bc.edu/audit)

### ***In This Issue:***

Alumni Association Receives BC 2003 Internal Control Best Practices Award	1
Welcome to Our Newest Staff Member!	1
Identity Theft	2
Becoming Spam Aware	3
Web Privacy	4
Business Ethics Hotline	4

Produced by:  
BC Internal Audit

671-552-8689

## Alumni Association Receives Boston College 2003 Internal Control Best Practices Award

The mission of the Boston College Alumni Association is to provide meaningful opportunities for alumni to connect or reconnect with the mission of Boston College. The role of the Alumni Association is to cultivate relationships with alumni, to provide leadership opportunities for alumni, and to support and help further the mission of Boston College. In December 2002, Internal Audit reviewed Alumni business operations. Under

the direction of the Executive Director, Grace Regan and the new Alumni Association management team, controls over business

operations significantly improved. The cooperation of the entire staff made for a very smooth audit of a complex organization.



P. Oakes, J. Soto, P. Jerskey, G. Regan, J. Moynihan

### **Welcome to Our Newest Staff Member!**

The Internal Audit Department welcomes Shay Atar as the newest member in our department. Shay previously worked at John Hancock Financial Services where he was a Senior Auditor. His duties at John Hancock consisted of planning, performing and managing financial, operational,

compliance and fraud audits. At BC, he will be reviewing and evaluating the adequacy, effectiveness, and proper application of accounting, financial, and other operating controls for business operations. Additionally, he will determine the level of compliance with controls and other established

policies, plans, and procedures, and determine the extent to which University assets are accounted for and safeguarded from losses.



*“Identity theft is one of the fastest growing crimes of our time.”*

### Agencies

Federal Trade Commission  
1-877-ID-THEFT  
[www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)

US Postal Service  
[http://www.usps.com/postalinspectors/idthft\\_ncpw.htm](http://www.usps.com/postalinspectors/idthft_ncpw.htm)

Social Security Fraud Hotline  
1-800-269-0277

### Credit Bureaus

Equifax  
<http://www.equifax.com/>  
P.O. Box 105873  
Atlanta, Georgia 30348-5873  
Telephone 1-800-997-2493

Experian Information Systems (TRW)  
<http://www.experian.com/>  
P.O. Box 949  
Allen TX 75013-0949  
Telephone 1-888-397-3742

TransUnion  
<http://www.transunion.com/>  
P.O.Box 390  
Springfield, PA 19064-0390  
Telephone 1-800-916-8800

## IDENTITY THEFT

by: Gene Neault, Lieutenant/Detective, BC Police

You know who you are. You are a law-abiding person. You follow the rules, go to work, and pay your bills. Early one morning you answer the door. Several federal agents question why a credit card issued in your name has been used to purchase computers, satellite phones and other high tech devices being shipped to suspected terrorists in Asia. You are a victim of identity theft.

You are a newlywed sitting down with your spouse to sign the mortgage papers on your first new house. The bank representative tells you your credit has been rejected. You find out that a court in a state you have never visited has entered a judgment against you for failure to pay. You are victim of identity theft.

The facts behind these two stories were taken from cases BCPD have investigated in recent years. Identity theft is one of the fastest growing crimes of our time. What used to be a low tech, low profit crime has become a highly profitable, technologically enhanced crime. Organized international and national gangs as well as individuals with a computer are involved. Once discovered, it may take months or even years and thousands of dollars for a victim to clear their name.

Criminals obtain personal information several ways that include:

- stealing laptops with personal information stored on it.
- stealing wallets or purses containing Ids, Credit or Bank cards.
- stealing mail, especially bank statements and pre-approved credit card offers.
- stealing trash, commonly called ‘Dumpster Diving’.
- using personal information you share on the internet.
- e-mailing scams, sometimes posing as legitimate businesses.
- offers that are too good to be true (Have you ever been offered millions to help the widow of some poor third world official?).
- hacking into your computer.

More organized groups may steal information from banks, insurance companies or other businesses. It is important to minimize your risk. Protect and manage your personal information at home and at work by:

- checking your credit rating annually (In Massachusetts, you can have one free credit rating annually).
- not giving out personal information on the phone, over the internet or by mail.
- shredding any papers with personal information on it.
- canceling all financial cards if your wallet or purse is stolen. (Hint: use the copy machine to duplicate all contents of your wallet and keep those copies in a safe place).
- giving out your social security number only when necessary.
- not using your social security number on your driver’s license.
- paying attention to your bills, especially if one does not arrive when expected.
- practicing safe computer skills
  - Update your virus protection.
  - Do not download files or open unknown attachments.
  - Use a firewall and a secure browser.
  - Do not store personal and/or financial information on a laptop or work computer.

If you suspect that you are a victim:

- Report the crime to BCPD or your local police department.
- Notify all three Credit Bureaus and have a fraud alert placed on your account.
- Create a log and document all your actions.

BCPD has a great deal of experience with Identity Theft. They are willing to assist you in reporting the crime and contacting the agencies able to aid you in clearing your name.

## BECOMING SPAM AWARE

by: Patricia O'Donnell

Credit companies spend \$.37 on postage when mailing credit card offers. A telemarketing call offering the latest product has even less expensive marketing operating costs. But sending junk e-mail costs a miniscule fraction of a penny for companies. That is why spammers can afford to send out millions of messages and make money getting only a handful of responses. However, the cost of unwanted email in terms of delivery, storage and processing can be billions of dollars each year for corporations. These messages can also create potential security holes, through which viruses and fraudulent mail can pass, and compromise sensitive personal or corporate information.

As a consumer you are probably frustrated with the amount of spam and junk mail that you receive. There is no way of accurately getting rid of all spam since spammers themselves will always be trying new tricks to bypass your "spam filters". However, individuals should follow these three steps to decrease the amount of spam received and also to protect against identify theft:

- 1) **Keep your email address secret** - Whenever you use your e-mail address publicly, you run the risk that your e-mail address will be saved for inappropriate use. You can create a special address for your public uses, such as a free e-mail site. Once it starts getting too much spam, you can disable the account and create a new one.
- 2) **Do not release friends' emails** - Spammers will try to trick you and your friends into giving them your e-mail

address. Any web page that asks you for other people's e-mail addresses is probably doing so for the purpose of sending unsolicited e-mail.

- 3) **Filtering Spam** - A lot of spam is not addressed to you. Spammers send out their spam to hundreds or thousands of individuals at a time. You can tell your e-mail program to "divert" any message that is not address to you. Divert it into a special spam folder, and, every once in a while, check this spam folder for legitimate mail.

A new way for spammers to solicit sensitive information is through "**phishing**." Phishing is a high tech scam that uses spam to mislead individuals into disclosing sensitive information, such as credit card numbers, bank account information, social security numbers, and passwords. The individual will receive an email that appears to be from a business with which they currently do business (i.e. bank, credit card company). The spam email informs the recipient that their account information needs to be updated or validated to resume business. The email may also even direct the individual to a look-alike website of the legitimate business. Unknowingly, consumers submit their financial information to the scammers, who use it to order goods and obtain credit.

To avoid being a victim of "PHISHING," follow these steps offered by the Federal Trade Commission, the

nation's consumer protection agency:

- If you receive an email that requests you to reconfirm your billing information, contact the company cited in the email using a telephone number that you know to be legitimate.
- Avoid emailing personal and financial information. Before submitting financial data through a website, look for the "lock" icon on the browser's status bar. It signals that your information is secure during transmission.
- Review credit card and bank account statements upon receipt. If the statement is late by more than a few days, call your credit card company or bank to confirm your billing address and account balances.
- Report suspicious activity to the Federal Trade Commission. Send the actual spam to [uce@ftc.gov](mailto:uce@ftc.gov). The FTC works for the customer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers avoid them.

#### Sources:

"Hitting Spammers Where It Hurts," by Stephen H. Wildstrom, *Business Week*, May 19, 2003, page 20.

"How Not to Get Hooked by a Phishing Scam," Federal Trade Commission – Consumer Alert, <http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm> July 2003.

"Avoiding Spam," <http://help.sandiego.edu/Articles/spam.shtml>




---

*A new way for spammers to solicit sensitive information is through "phishing."*

## BUSINESS ETHICS HOTLINE

University employees should be reminded to watch for certain warning signs, also known as "RED FLAGS" that may lead to fraudulent activity in the work place. Common red flags to watch for are:

- Marked Personality Changes in Employees
- Financial Pressures on Employees;
- Employee Living Beyond His/Her Means
- Employee Having Outside Business Interests
- Poor Internal Controls
- Rising Department Expenses
- Too Much Control in Key Employees

In accordance with the University Professional Standards and Business Conduct Policy, each University employee is expected to report any instance of suspected ethical misconduct to the Director of Internal Audit. If presented with reasonable evidence of a suspected ethical misconduct, the Director of Internal Audit will conduct an audit to determine if the reported suspicions of fraud are valid.

**A Business Ethics Hotline (2-3194)** has been established for employees to convey their concerns to the Director of Internal Audit.

## WEB PRIVACY: ADS THAT SNOOP

by: John Soto

### Unwelcome Visitor

Did you know that you may have snooping software on your computer? When you start up your computer, a software program might silently be running that keeps track of Web sites you visit or make purchases at. Later when you go to other Web sites, the snooping software looks at your web surfing history and shows "pop up" ads. These ads are tailored to your particular interests, based on a database of your Web-surfing history that the software has been keeping. When PC owners detect that the program is embedded in their computer, they are understandably appalled, and feel that their privacy has been violated.

### Spyware

Advertisers are refining new ways of putting their software onto your computer, so that they can carefully target specific marketing to you. You might not be aware that when you download programs that are offered for free via the web, that you may also be downloading "spyware". When the consumer goes back online, the software sends the spyware company information via the Internet on which Web sites are being visited.

Spyware isn't just an issue for consumers. While many companies want to target consumers more precisely, there are other companies that have filed suits against spyware makers. They argue that spyware is violating copyright and trademark laws by popping up ads when people visit their sites.

Spyware represents a variation on a simple form of tracking technology called "cookies."

Cookies stirred fears over Internet privacy several years ago. Cookies are snippets of text that are automatically downloaded when a computer visits a web site and stores information about your visit, such as which link you accessed and how long you looked at it. This file is placed on your workstation's hard drive. The next time you visit that site, the server looks for a file on your workstation and reads the previous information. Spyware, by contrast, can track each click you make as you surf the Net.

### Gator Corporation

Gator Corporation is one of the companies using new spyware technology to target pop-ups and other online ads. Gator touts itself as "one of the world's largest behavioral marketing networks and software distributors." Gator states that "it has the ability to anonymously monitor user behavior throughout their Web travels without ever collecting personally identifiable information. We do not transmit to our servers personally identifiable information like email addresses, last name, street addresses, or phone numbers." Gator does use the following kinds of anonymous information: (1) some web pages viewed, (2) time spent at some web sites, (3) standard web log information (excluding IP Addresses) and system settings, (4) software on your personal computer, (5) first name, country, city, and five digit ZIP code, (6) non-personally identifiable information on Web pages and forms, and (7) software usage characteristics and preferences.

Gator is presently facing legal action initiated by some Web-site operators. Hertz, for instance, was angered when it noticed that some people calling up its Web site would be greeted by Gator-generated pop-ups touting rival car rental companies. Hertz filed a lawsuit accusing Gator of infringing its trademarks and copyrights. The case is pending in the U. S. District Court for northern Georgia.

### Conclusion

The public uproar over unwelcome and annoying telemarketing phone calls led to the creation of a national registry, whereby consumers can list their phone numbers on a "Do Not Call" list. This service promises to block commercial telemarketing calls as of October 1<sup>st</sup>, 2003. In the meantime, the email "spam" controversy has reached a fevered pitch, and some members of Congress are considering introducing "anti-spam" legislation to curtail it. This is great progress, however, we're still vulnerable to the dangers of spyware, since presently there are currently no laws or court decisions that outlaw it. However, there is something that we can do to boot spyware out of our computers and lives. There are several companies that supply purging programs for irritated consumers, such as Spybot Search & Destroy, Ad-aware and Pest Patrol. Spybot - Search & Destroy can detect and remove a multitude of ad ware files and modules from your computer. Software can be found at: <http://download.com.com/3000-2144-10122137.html>

**Source:** "New Battleground in Web Privacy War: Ads that Snoop," by James R. Hagerly and Dennis K. Berman, *The Wall Street Journal*, 8-27-03, page A1.