Spring 2004
Volume XXXVI

AuditNews

We're on the Web!
See us at:
www.bc.edu/audit

In This Issue:

Produced by:
BC Internal Audit

671-552-8689

BUSINESS ETHICS

by: Pamela Jerskey

Questionable accounting practices and allegations of financial fraud have recently dominated the headlines. Because of these situations, Congress passed the *Sarbanes-Oxley Act of 2002*, which created new rules for corporate governance and responsibility for public companies. The *Act* does not apply to institutions of higher education, or other public or not-for-profit entities, however, the issues that are covered are universal. While Boston College may not be directly affected by *Sarbanes-Oxley*, the fundamental best practices of corporate governance, auditor independence, and a sound internal control structure have been adopted by Boston College.

Internal controls are designed to provide reasonable assurance that (1) operations are effective and efficient, (2) financial reporting is reliable, and (3) Boston College complies with laws and regulations. Additionally, Boston College has issued policies and procedures designed to provide guidance to employees concerning employee code of conduct and business ethical issues. These policies and procedures should be thoroughly reviewed to ensure an understanding of the code of conduct required of Boston College employees.

Sound business practice requires that Boston College employees and students assume responsibility for safeguarding and preserving assets and resources of the University, particularly those for which he or she is responsible. 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 Internal Audit Department.

An **anonymous Business Ethics Hotline (2-3194)** has been established for employees and students to convey their concerns to Internal Audit. If you believe that fraud or ethical misconduct has occurred, you should contact the Business Ethics Hotline at extension 2-3194. The suspected abuses will be investigated and an examination of supporting documentation will be performed. If, based on our review, we conclude that there is reasonable evidence of exploitation; we will schedule an immediate audit.

This Business Ethics Hotline ***should not be used for technology abuses.*** The mission of Information Technology's Computer Policy and Security group is to create an environment in which the community's need to protect information is balanced with the community's need for privacy. Send an email to security@bc.edu if you:

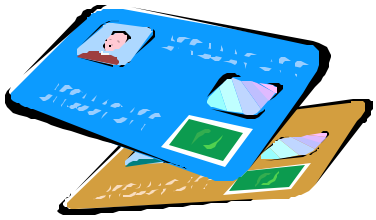
- suspect or know that your **computer/server** has or is being attacked.
- have received offensive or threatening **email** or **voice mail**.
- suspect that someone knows or is using your **PIN** or **password** for a Boston College system.
- are aware of **software copyright violations** here at Boston College.

For detailed information go to:
http://www.bc.edu/offices/its/support/policysecurity/

Additionally, the Boston College Police have set up a variety of resources for University faculty, staff and students to seek assistance in subjects ranging from traffic and parking issues to lost property on campus. For details go to:
http://www.bc.edu/offices/bcpd/services/

BEWARE OF CREDIT CARD SCAMS

by: Tricia O'Donnell



The media has recently reported that fraudsters posing as VISA and MasterCard representatives are calling individuals at home. Both VISA and MasterCard have confirmed that the following scam is currently being worked throughout the Midwest, with some variance as to the product and amount.

Both credit card companies have advised individuals to hang up immediately if they receive the following call:

The fraudster calling says, "This is (any name) and I'm calling from the Security and Fraud department at VISA. My Badge number is 12460. Your card has been flagged for an unusual purchase pattern, and I'm calling to verify. This would be on your VISA card issued by 5/3 bank. "Did you purchase an Anti-Telemarketing Device for $497.99 from a marketing company based in Arizona?"

When the individual says "No," the caller continues with, "Then we will be issuing a credit to your account. This is a company we have been watching and the charges range from $297 to $497, just under the $500 purchase pattern that flags most cards. Before your next statement, the credit will be sent to (gives the home address), is that correct?"

When the individual confirms their address, the caller continues, "I will be starting a fraud investigation. If you have any questions, you should call the 800 number listed on your card 1-800-VISA and ask for Security. You will need to refer to this Control #." The caller then gives a 6 digit number. The caller then says he "needs to verify you are in possession of your card. Turn the card over. There are 7 numbers; first four are 1234 (whatever) the next 3 are the security numbers that verify you are in possession of the card. These are the numbers you use to make internet purchases to prove you have the card. Read me the 3 numbers."

Then he says "That is correct." I just needed to verify that the card has not been lost or stolen, and that you still have your card. Do you have any other questions? Don't hesitate to call back if you do."

The individual never supplies the card number, but the fraudster only wants the 3 digit number on the back of the card. Once the fraudster obtains the number, the charges are made to the account every few days. By the time the statement is received, the individual thinks the credit is coming. But instead, a series of unauthorized charges have been made, and the time lag makes it harder to actually file a report.

"The Internet is an excellent tool for fraudsters."

Agencies

FBI: Common Fraud Scams
http://www.fbi.gov/majcases/fraud/fraudschemes.htm

SEC: Internet Fraud
http://www.sec.gov/investor/pubs/cyberfraud.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

COLLEGE SCHOLARSHIP SCAMS

by: Shay Atar

Eager to find new ways to fund your college education? Don't fall prey to college scholarship scams and seminars promising big payoffs and access to millions of dollars worth of unclaimed grants. Many students and parents turn to scholarship search services or other companies that take advantage of consumers by guaranteeing often impossible results. Unfortunately, in their efforts to pay the bills, many students and parents are falling prey to scholarship and financial aid scams. According to the Federal Trade Commission (FTC), corrupt companies guarantee or promise scholarships, grants or fantastic financial aid packages. Many of these companies use high pressure sales pitches at seminars where you are required to pay immediately or risk losing out on the "opportunity." They typically charge fees ranging from $50 to more than $1,000, but do little, if anything, to help students find financial aid. There are lots of scholarships available, but no one can secure a scholarship for you but you.

continue on page 3.....

…..College Scholarship Scams from page 3

The FTC cautions students to look and listen for these tell-tale lines:

- "The scholarship is guaranteed or your money back."
- "You can't get this information anywhere else."
- "I just need your credit card or bank account number to hold this scholarship."
- "We will do all the work."
- "The scholarship will cost some money."
- "You have been selected by a national foundation to receive a scholarship" - or "You are a finalist in a contest you never entered. "

Fraudulent scholarships can take many forms. According to the web site, www.finaid.org, common types of scams are:

"Scholarships that Never Materialize. Many scams encourage you to send them money up front, but provide little or nothing in exchange. Usually victims write off the expense, thinking that they simply didn't win the scholarship.

The Advance-Fee Loan. This scam offers you an unusually low-interest educational loan, with the requirement that you pay a fee before you receive the loan. When you pay the money, the promised loan never materializes. Real educational loans deduct the fees from the disbursement check. They never require an up-front fee when you submit the application. If the loan is not issued by a bank or other recognized lender, it is probably a scam.

The Scholarship Prize. This scam tells you that you have won a college scholarship worth thousands of dollars, but requires that you pay a "disbursement" or "redemption" fee or the taxes before they can release your prize. If someone says you have won a prize and you don't remember submitting an application, be suspicious.

The Guaranteed Scholarship Search Service. Beware of scholarship matching services that guarantee you will win a scholarship or they will refund your money. They may simply pocket your money and disappear, or if they do send you a report of matching scholarships, you will find it extremely difficult to qualify for a refund.

Free Seminar. You may receive a letter advertising a free financial aid seminar or "interviews" for financial assistance. Sometimes the seminars do provide some useful information, but often they are cleverly disguised sales pitches for financial aid consulting services, investment products, scholarship matching services and overpriced student loans. "

If you attend a seminar on financial aid or scholarships, the FTC has the follow advice to protect you from scams:

- "Take your time. Don't be rushed into paying at the seminar. Avoid high-pressure sales pitches that require you to buy now or risk losing out on the opportunity. Solid opportunities are not sold through nerve-racking tactics.
- Investigate the organization you are considering paying for help. Talk to a guidance counselor or financial aid advisor before spending your money. You may be able to get the same help for free.
- Be wary of "success stories" or testimonials of extraordinary success - the seminar operation may have paid someone to give glowing stories. Instead, ask for a list of at least three local families who have used the services in the last year. Ask each if they are satisfied with the products and services received.
- Be cautious about purchasing from seminar representatives who are reluctant to answer questions or who give evasive answers to your questions. Legitimate business people are more than willing to give you information about their service.
- Ask how much money is charged for the service, the services that will be performed and the company's refund policy. Get this information in writing. Keep in mind that you may never recoup the money you give to an unscrupulous operator, despite stated refund policies."

Sources:

Federal Trade Commission
http://www.ftc.gov/bcp/conline/edcams/scholarship/

FinAid: the Smart Student Guide to Financial Aid
http://www.finaid.org/

To investigate a company or report a scam, contact the following organizations:

National Fraud Information Center (NFIC): http://www.fraud.org/ or NFIC hotline 1-800-876-7060.

Federal Trade Commission: http://www.ftc.gov or call 1-877-FTC-HELP (1-877-382-4357).

IMPROVING YOUR LISTENING SKILLS

by: John Soto

"One of the best ways to persuade others is with your ears—by listening to them."
Dean Rusk, Secretary of State in President John F. Kennedy's administration

As students, faculty and administrators, we must be able to write, speak, and listen effectively. Of these, listening is the most crucial because we are required to do it so often. Unfortunately, listening may be the most difficult to master. A recent article in the ***Internal Auditing Magazine*** discusses several tips for improving one's listening skills. The author had the internal audit profession in mind; however, its listening tips are universal, and can help anyone become a better communicator. Hence, I would like to share these valuable tips with the BC community:

Concentrate on What Others are Saying

Most individuals speak at the rate of 175 to 200 words per minute. However, research suggests that we are very capable of listening and processing words at the rate of 600 to 1,000 per minute. This unused brainpower can be a barrier to effective listening, causing misinterpretation of what others are saying. It is important to actively concentrate on what others are saying so that effective communication can occur.

Send the Nonverbal Message that you are Listening

Your body language transmits the message that you are listening (e.g. eye contact, nodding your head, and leaning forward). Most communication experts agree that nonverbal messages can be three times as powerful as verbal messages. Effective communication becomes difficult anytime you send a nonverbal message that you're not listening.

Avoid Early Evaluations

Because a listener can listen at a faster rate than most speakers talk, there is a tendency to evaluate too quickly. That tendency is perhaps the greatest barrier to effective listening. It is especially important to avoid early evaluations when listening to a person with whom you disagree. When listeners begin to disagree with a sender's message they tend to misinterpret the remaining information and distort its intended meaning so that it is consistent with their own beliefs.

Avoid Getting Defensive

Careful listening does not mean that you will always agree with the other party's point of view, but it does mean that you will try to listen to what the other person is saying without becoming overly defensive. Effective listeners can listen calmly to another person even when that person is offering unjust criticism.

Practice Paraphrasing

Paraphrasing is the art of putting into your own words what you thought you heard and saying it back to the sender. It is a great technique for improving your listening and problem-solving skills. First, you have to listen very carefully if you are going to accurately paraphrase what you heard. Second, the paraphrasing response will assure the sender that the listener received the message correctly, and encourage the sender to expand on what he or she is trying to communicate.

Listen (and observe) for Feelings

When listening, we should concentrate not only on the words, but also on the manner of delivery. The way a speaker is standing, the tone of voice and inflection he or she is using, and what the speaker is doing with his or her hands are all part of the message that is being sent. A person who raises his or her voice is probably angry or frustrated. A person looking down while speaking is probably embarrassed or shy. Long pauses may suggest fear or lack of confidence.

Ask Questions

Effective listeners make certain they correctly heard the message. Ask questions to clarify points or to obtain additional information. Open-ended questions are the best. They require the speaker to convey more information. The more information that you as a listener have, the better you can respond to the sender's communication.

Listen Actively

Individuals who use "active" listening will likely become much better listeners. Active listening demands that the receiver of a message put aside the belief that listening is easy and that it happens naturally, and realize that effective listening requires hard work and effort. The result of active listening is more efficient and effective communication.

Source:

"7 Tips for Effective Listening," by Tom D. Lewis and Gerald Graham, *Internal Auditing,* August 2003, p.23-25.

RISING UNIX/LINUX SECURITY BREACHES

by: Tricia O'Donnell

As computer users, we are often aware of the security holes and known viruses associated with the Microsoft Windows operating systems. But, lower profiled operating systems, such as UNIX and Linux, are gaining more attention because of their security breaches. In September 2002, the Linux.Slapper worm emerged and caused significant disruption. Along with Slapper, a number of highly sophisticated UNIX and Linux viruses have emerged in recent months. These threats have demonstrated that malicious code writers are developing a high level of sophistication and familiarity with these systems. Specifically, the upswing in Linux attacks has been attributed to misconfigured systems and to a lack of standard security practices in the open source environment.

UNIX/Linux based software vulnerabilities are among those currently listed as the top 10 most critical vulnerabilities by the SANS Institute and the FBI:

1. Remote Procedure Calls (RPC)
2. Apache Web Server
3. Secure Shell (SSH)
4. Simple Network Management Protocol (SNMP)
5. File Transfer Protocol
6. R-Services – Trust Relationships
7. Line Printer Daemon (LPD)
8. Sendmail
9. BIND/DNS
10. General UNIX Authentication – Accounts with no passwords or weak passwords

The SNMP and Sendmail vulnerabilities are considered to be the two most important vulnerabilities to research, test, and quickly patch to prevent hostile attacks, reduce spam, and keep systems running. Sendmail is the program that sends, receives and forwards most electronic mail processed on UNIX and Linux machines. While most Sendmail exploits are successful only against older versions of the software, there remain many outdated or misconfigured versions still in use today, making Sendmail one of the most frequently attacked services.

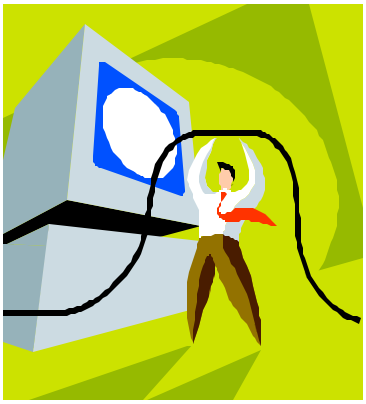
A problem that resonates across the Linux platform is that everyone has access to the source code. While this attribute is what makes the operating system appealing and cost-effective to many, it can also be the core of what makes the operating system so much easier for hackers to exploit.

Over the past decade, many public and private organizations have adopted the UNIX/Linux systems to reduce network and data center costs. Many have agreed that open source operating systems have directly improved stability and security. However, those managing UNIX/Linux (as well as Windows) systems can reduce end-user downtime and minimize risk to business systems by developing and implementing patch management as a key element of vulnerability procedures.

For more information on open source vulnerability remediation, go to www.opensource.org.

Reference:

Andrew, Chris; Patch Management: An Effective Line of Defense for UNIX and Linux; Information Systems Control Journal, Volume 6, 2003



Internal Audit Staff:

Pamela Jerskey
Director
2-8689
pamela.jerskey.1@bc.edu

John Soto
Manager
2-3113
john.soto.1@bc.edu

Patricia O'Donnell
Senior Internal Auditor
2-4336
patricia.odonnell.1@bc.edu

Shay Atar
Senior Internal Auditor
2-3294
shay.atar.1@bc.edu