

Save the Date.....

Wednesday, April 25th, 10-11:30
Identity Theft and Fraud: A Guide to
Protecting Yourself and Boston College
(McElroy Conference Room)

Identity theft and fraud are "hot" topics in today's world, and they're not likely to fade any time soon. The challenge for us, as Boston College employees, as well as in our personal life, is taking preventative action so that they don't happen. In this interactive session, we address types of identity theft, fraud, and ethical issues.

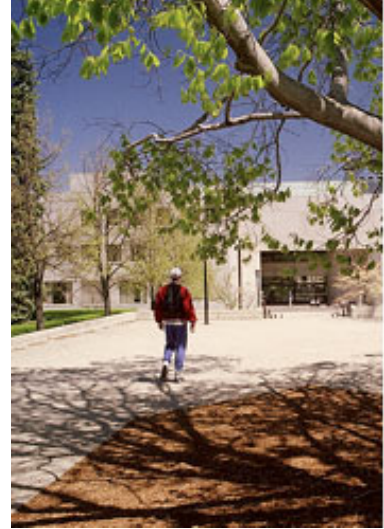
Who Should Attend?

Anyone who wants to learn more to maintain high professional and ethical standards in their work environment.

To register, email employee.development@bc.edu or call x28532.

The purpose of this newsletter is to provide the BC community with articles on good business practices, internal controls and responsibilities. Each issue will provide insights to internal control techniques. We have also included an "Ask the Auditor" section to give you an opportunity to obtain answers to specific questions. Additionally, we will provide information on recent items in the news.

We hope that by providing this array of information, we can help you implement effective controls in your area of operations.



Contents

Maintaining Data Security.....	1
Concepts of Fraud Prevention	3
In the News	4

Maintaining Data Security is Everyone's Responsibility.

On Jan. 17, TJX revealed that a hacker had broken into its computers, potentially compromising millions of credit- and debit-card numbers and drivers license data; it's been reported that thieves have used the numbers to make fraudulent purchases from Florida to Hong Kong. Security breaches can cause:

- loss of confidence, respect or trust.
- loss of reputation due to publicity of breach.
- network service stoppage or degradation.
- prosecution.

Here are some data security best practices to help you keep your sensitive information safe:

1. Physically secure your area, files, and equipment before leaving them unattended.
 - Check doors, drawers, and windows.
 - Lock up any sensitive materials before you leave your area.
 - Never share your lock code, access card, key, etc.



Continue on Page 2...



2. Don't keep important data on portable devices (laptops, CDs/floppys, memory sticks, PDAs, phones, etc.) unless you know how to properly protect it. These items are extra vulnerable to theft or loss.
3. Do not install unknown or unsolicited programs on computers, such as programs you find out about through email.
4. Lock, log off, or put your computer to sleep before leaving it unattended.
 - *<ctrl> <alt> <delete> on a PC*
 - *Apple menu on a Mac*
5. Your computer should require a password to start up or wake-up.
6. Use hard-to-guess passwords and keep them private.
7. Don't click on website addresses in email unless you REALLY know where you're going. If an email is unsolicited or even slightly suspicious, look up the website yourself and go there directly instead of clicking on an email link.
8. Ensure that authorized people use confidential information appropriately. Don't divulge sensitive information, passwords, etc. over the phone, Internet or email, even to people claiming to need it. Be aware of the potential for others to overhear communications about sensitive information in public places.
9. The Internet is not private. Don't provide personal, sensitive or confidential information to Internet sites, surveys, or forms unless you are using a trusted, secure web page.
10. Do not leave paper documents containing sensitive information unattended (e.g., fax, copy machine). Store sensitive paper documents in a locked file cabinet. Shred confidential paper documents that are no longer needed.



Useful website for computer security tips:

United States Computer Emergency Readiness Team:
<http://www.us-cert.gov/cas/tips/>

Carnegie Mellon University, CERT Program:
http://www.cert.org/tech_tips/home_networks.html

CyberSmart Education Company
http://www.cybersmart.org/for/top_ten.asp

Did You Know??

Most copy machines are now full-blown IT devices, with network and E-mail server connectivity. The increased use of embedded operating systems in these machines--including versions of Microsoft Windows--also means copiers can be infected by vulnerabilities more commonly associated with computers, making them perfect targets for hackers or thieves. Additionally, employees normally have unrestricted access to copiers and the information stored on them. Copiers can also be used to scan sensitive personal documents such as medical records, birth certificates, or financial forms. Since these sophisticated copiers have hard drives and can store copied data for an indefinite period of time, employees should be aware of the information they are working with. Securing these multifunction devices is the same as securing other network devices such as servers and desktops. The most important security mechanism is using common sense when working with sensitive data.

Concepts of Fraud Prevention

It is important to distinguish between **Internal Audit's role** and **University management's role** concerning fraud. Many individuals believe that frauds and other transgressions are only the concern of Internal Audit and Campus Police. However, this is incorrect. University management is responsible for maintaining an adequate system of internal control by analyzing and testing controls. Internal Audit's role is to independently evaluate the adequacy of the existing system of internal control. We also perform fraud investigations, and promote a positive control environment throughout the University.

Fraud takes many forms. Some examples include: embezzlement, kickbacks, theft, fraudulent financial reporting, environmental crimes, software piracy, bid rigging, computer-related crime, identity theft, credit card fraud, check fraud, fraudulent workers compensation claims, ghost employee schemes, expense report schemes, "dummy" vendors, unreported conflicts of interest, etc.

Most people who commit fraud against their employers are not career criminals. The vast majority are trusted employees. So the question is, what factors cause these otherwise normal, law abiding persons, to commit fraud?



WHO SHOULD I CALL ABOUT AN ALLEGED FRAUD?

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

<http://www.bc.edu/offices/audit/hotline/>

To understand why individuals commit fraud, we must understand the fraud triangle. The risk of fraud occurring is contingent upon a combination of factors affecting an employee: pressure, rationalization, and opportunity.

Pressure can be due to personal financial problems, personal vices such as gambling, drugs, etc, or a desire for status symbols.

Rationalization occurs when an individual develops a justification for their fraudulent activities. Some examples include:

- "I really need this money and I'll put it back when I get paid."
- "I just can't afford to lose everything—my home, car, everything!"

Opportunity is generally provided through weaknesses in internal controls. Some examples include:

- Lack of supervision and review
- No separation of duties
- Inadequate approvals

There are two approaches to help reduce fraud risk: **prevention** and **detection**. The best approach is to prevent illegal and inappropriate acts from occurring in the first place. As a BC employee, you are responsible for ensuring departmental funds, property and equipment are safeguarded from loss. The following procedures can be adopted to help reduce the risk of fraudulent activity:

- Ensure that transactions are accurate and complete.
- Create adequate documentation for all critical processes.
- Provide adequate separation of duties.
- Establish sufficient safeguards over all assets.
- Institute formal policies and procedures.
- Perform periodic physical inventories.
- Ensure that only authorized personnel have access to critical transactions.
- Confirm that funds are collected and deposited to the appropriate account.
- Establish procedures to reconcile all accounts.

It is important to recognize that as a Boston College employee, you have stewardship responsibility for safeguarding University assets under your purview.

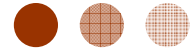
Each University employee is further expected to report any instance of suspected fraud to the Director of Internal Audit. If an instance of suspected fraud is reported instead to a supervisor, chairperson, director, dean, vice president, or other responsible person, that person is to report the instance to the Director of Internal Audit.

Related useful websites:

Boston College Professional Standards and Business Conduct General Policy
<http://www.bc.edu/offices/policies/meta-elements/doc/policies/1/1-100-010/1-100-010.shtml>

BC Reporting of Fraud Policy
<http://www.bc.edu/offices/policies/meta-elements/doc/policies/1/1-100-015.shtml>

Boston College Research Policies:
<http://www.bc.edu/research/osp/policies.html>



In the News.....

Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access and in most (but not all) cases the attacker never comes face-to-face with the victim.

Listed below are some common methods of social engineering:

1. *Phone calls*: Someone pretends to be in authority and asks for sensitive information. If you can't verify the identity of the source asking for your personal information, you should be very cautious about the transaction.
2. *Voice mails*: Someone may leave a message from an "official" agency asking you to call a number or go to a particular website. Never provide personal information unless you have initiated the contact and have confirmed the business or person's identity.
3. *Mail*: Bogus mail solicitations (i.e., sweepstakes) ask for private information that could be used to steal your identity. Be skeptical of offers that seem "too good to be true". They usually are.
4. *E-mail*: Emails can be sent from a fraudster. Such phony emails are disguised as legitimate, and often include company logos that look real. Do not provide sensitive data to someone via email.
5. *Physical Presence*: Someone pretends to be a part of the organization and gains access to restricted areas. For example, ask for ID and know who you are letting access your computer for repair.
6. *Free Goodies*: Free computer hardware or software can contain virus or key logging software. For example, a free USB thumb drive could contain a Trojan that, when run, can collect passwords, logins and machine-specific information from the user's computer, and then email the information back to the fraudster. Know who you are getting your software and hardware from.

IS YOUR PORTABLE DEVICE SECURE?

Portable devices include Blackberry communication devices, PDAs such as Palm and IPAQs, and cell phones. Blackberries pose a significant threat if they are not properly secured. The most common failing is the lack of a password on a Blackberry. A simple test to check that a blackberry has a password is to shut the Blackberry off and turn it back. If it does not prompt you for a password, then this device can be easily compromised. Blackberries are often carried in a jacket pocket. The jacket may be hung on a door where someone can steal the device from the pocket. PDAs and some cell phones also contain sensitive data. The new Palm Treo combines a cell phone with a PDA and is very similar to a Blackberry. Many people use their personal PDAs or cell phones with Pocket PC, such as the Treo, for business purposes. When they leave the company, this corporate data may go with them. The chip in the PDA will also greatly increase the storage capacity, so the possibility of large amounts of confidential data being in the hands of a disgruntled terminated employee arises. Hence, the use of personal PDAs, cell phones and other similar devices for business use should be limited and monitored.



Source: <http://www.canaudit.com/Perspectives/Volume7-Issue1.pdf>