

Save the Date.....

**Thursday, November 18th
10-11:30**

Identity Theft and Information Technology Best Practices: A Guide to Protecting Yourself and Boston College

(Walsh Hall Function Room)

Identity theft is a "hot" topic in today's world, and it is 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. In this interactive session, we will also outline best practice information technology controls to assist in protecting yourself and Boston College.

Among the topics discussed:

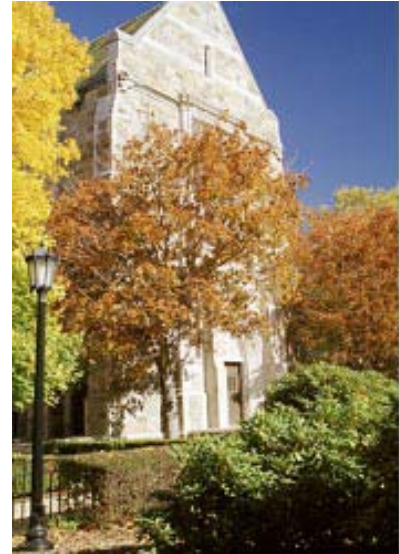
- common types and warning signs of identity theft
- ways in which you can identify risks that may result in identity theft
- the appropriate actions to deal with identity theft as well as fraud issues, and how to resolve each concern
- electronic and physical data security
- external threats / Internet safety

To register, email

employee.development@bc.edu or call x28532.

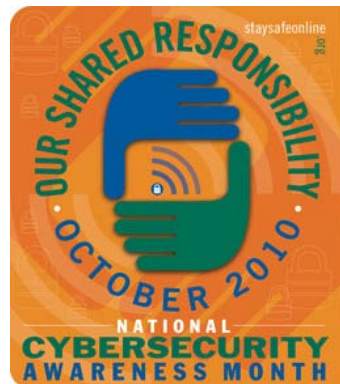
The purpose of this newsletter is to provide the BC community with articles on good business practices, internal controls and responsibilities. Each issue will provide insights to internal control techniques. We have also included an "In the News" section to highlight key topics for discussion.

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



Contents

In the News	2
What is Business Ethics?	3
Bluetooth Technology	4
Hot Topics	4



October is National Cyber Security Awareness Month

National Cyber Security Awareness Month (NCSAM) has been conducted every October since 2001. It is a national public awareness campaign to encourage everyone to protect their computers and the nation's critical cyber infrastructure. This year's theme is **"Our Shared Responsibility"**.

As the Internet becomes pervasive, individuals are online from home, school, work, and in between on mobile devices. The economy and much of the everyday infrastructure we rely on uses the Web. Ultimately, the cyber infrastructure is only as strong as the weakest link. No individual, business, or government entity is solely responsible for cyber security. Everyone has a role and everyone needs to share the responsibility to secure their part of cyber space and the networks they use.

Read more at: <http://www.staysafeonline.org/>



Check out the University Data Security Policy at:

<http://www.bc.edu/offices/policies/meta-elements/pdf/policies/I/1-100-200.pdf>

In the News.....



What is Computer Security?

Computer security includes protection of information and property from theft or corruption, while allowing the information and property to be accessible and productive to its intended users. Prevention measures help to stop unauthorized users (also known as "intruders") from accessing any part of your computer system.

Why should I care about computer security?

We use computers for everything from communicating through email and social networking, to banking and investing. You may not consider your communications "top secret", however, you probably do not want strangers reading your email, using your computer to attack other systems, sending forged email from your computer, or examining personal information stored on your computer.

System intruders may not care about your personal identity. Often they want to gain control of your computer so they can use it to launch attacks on other computer systems. Once they have control of your computer, they have the ability to hide their true location as they launch attacks, often against high-profile computer systems such as government or financial systems.

Where should I store my University related data to ensure it is backed up and secure?

All University related data should be stored on your department's server. If you do not currently have access to a central server, then contact your Technology Consultant to gain access. The Technology Consultant is responsible for ensuring that all data is backed up regularly and secure.

Data can also be stored on the University's MyFiles.

<http://www.bc.edu/offices/help/essentials/backup/myfiles/about.html>

How can I protect my computer and the information stored on it?

- Keep operating system software, application software (i.e. Microsoft Office), and all browser plug-ins (Java, Flash, RealPlayer, etc.) up-to-date.
- Help shield your computer from vulnerabilities, viruses, worms, and other threats as they are discovered by using up-to-date anti-virus software.
- Use of unsecured wireless networks can put you at risk. Use a secure and reliable wireless network that encrypts wireless data transmissions.
- Don't open unknown email attachments.
- Don't run programs of unknown origin.
- Use strong passwords or strong authentication technology to help protect your personal information.

- Evaluate your software's settings. The default settings of most software enable all available functionality. However, attackers might be able to take advantage of this functionality to access your computer. Use the highest level of security available that will still give you the functionality you need.
- Avoid unused software programs. If you have programs on your computer that you do not use, consider uninstalling them. Unused programs consume system resources and may contain vulnerabilities that, if not patched, may allow an intruder into your computer.

How do I set my computer screen to logout if I leave my computer unattended?

Windows machines allow you to password protect your computer after being unattended for a predetermined amount of time. Right click on the Desktop, and select Personalize. Go to the Screen Saver link. Select a Screen Saver of your preference. We recommend that Wait should be anywhere from 5 to 15 minutes. This will not log you out of any applications running unless those applications have a similar lockout built in.



What is Business Ethics?

Ethics is today's "hot" topic in the business world. But unlike other business fads that come and go, the recent attention focused on ethics is not likely to fade any time soon. Business ethics refers to the value structure that guides individuals in the decision making process when they are faced with a dilemma of how to behave within their business or professional lives. An ethical code can provide guidance to employees on how to handle situations that pose a dilemma on the right course of action, or when faced with pressure to consider right and wrong.

So, what can an organization do to ensure that its employees get business ethics just right? Organizations, both for-profit and non-profit, typically adopt ethics programs that contain the following factors:

- Establishment of compliance standards and procedures that are reasonably capable of reducing the prospect of criminal conduct.
- Identification of high-level personnel within the organization, and assignment of overall responsibility to oversee compliance with standards and procedures.
- Use of due care not to delegate discretionary authority to individuals whom the organization knew or should have known had a propensity to engage in illegal behavior.
- Effective communication of the organization's standards and procedures to employees.

- Taking reasonable steps to achieve compliance with standards by utilizing auditing and monitoring systems; put into place and publicize a reporting system whereby employees can report criminal conduct without fear of retribution.
- Consistent enforcement of compliance standards through uniform disciplinary action, thereby establishing common expectations about business conduct in all business units.
- Taking reasonable steps, if an offense is detected, to prevent further similar offenses, including any necessary modification to the program to prevent and detect violations of the law.

Ethics can also encompass values that include such traditional virtues as trust, loyalty and commitment, honesty and respect for one another, and avoiding conflicts of interest. Each employee should be familiar with the general and specific operating policies and procedural guidelines that cover the business activities that are his or her responsibility.



To read more about Professional Standards and Business Conduct -- General Policy go to:
<http://www.bc.edu/offices/policies/meta-elements/pdf/policies/I/1-100-010.pdf>

To read more about Professional Standards and Business Conduct -- Reporting of Fraud go to:
<http://www.bc.edu/offices/policies/meta-elements/pdf/policies/I/1-100-015.pdf>

To read more about Professional Standards and Business Conduct -- Use of University Technological and Information Resources go to:
<http://www.bc.edu/offices/policies/meta-elements/pdf/policies/I/1-100-025.pdf>



Understanding Bluetooth Technology

Bluetooth is a technology that allows devices to communicate without lines or wires. This technology has exploded in recent years, and nearly every new electronic device maintains this capability. Examples of such products include: laptops, mobile devices, and smart phones. The Bluetooth technology requires short-range radio frequency, and allows for multiple communication mediums between disparate devices.

As with most technology, the security of Bluetooth is largely dependent on its individual configuration. Bluetooth allows for encryptions as well as key authentication. Unfortunately, as with most mobile devices, the technology frequently relies on short PIN's that are easy to decode. There are two primary risks to Bluetooth technology. First, a hacker can access your account and incur significant fees as a result of overuse. Even worse, an attacker could compromise your existing data, or distribute to other parties at a profit.

Below are some of the recommended protection measures when employing Bluetooth technology:

- Reject Bluetooth communication from unknown parties
- Disable Bluetooth when you are not actively using it
- Investigate and deploy the security options offered by your technology
- Be leery of utilizing Bluetooth when in public places where users can more easily access your connection

Refer to <http://www.us-cert.gov/cas/tips/ST05-015.html> for additional information surrounding this topic.

Hot Topics.....

Copy Machine Security

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.

For those areas handling confidential data, there are now software packages for about \$250.00 that can be added to copiers to reduce the risks. For more information, and to see if your copier can be equipped with such software, please contact the BC Copier provider, IKON Office Solutions at jkoslowsky@ikon.com.

Protecting Portable Devices

Many computer users, especially those who travel for business, rely on laptops and other portable devices to perform daily business tasks including: document creation, electronic messaging, and storage of sensitive information. As a result, these devices are often targeted by criminals. Below is an abbreviated listing of some steps you can take to ensure the protection of your mobile device:

- Password Protect your Computer and your mobile device.
- Backup your files to ensure business continuity in the event of a theft.
- Do not save sensitive files on the local hard drive. Instead, ensure sensitive information is stored on a secure server.
- Be cognizant of public wireless access points, and the types of information transmitted across these networks.