Save the Date…..

Tuesday, April 1st, 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 fraud won’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.

Did You Know That…..

The University enacted a Data Security Policy in May 2007. See: http://www.bc.edu/datasecricypolicy for the full text of the policy.

The purpose of the policy is to “outline essential roles and responsibilities within the University community for creating and maintaining an environment that safeguards data from threats to personal, professional and institutional interests.”

The policy concerns all physical documents, electronic databases, or other collections of information collected, stored or used by any department or person in connection with University operations. Information covered in the policy is classified into three categories, according to the level of security required. These security classifications are “Confidential,” “Internal Use Only,” and “Public.”

- **Confidential Information** includes sensitive personal and institutional information, and must be given the highest level of protection against unauthorized access, modification or destruction.

- **Internal Use Only Information** includes data that is less sensitive than Confidential information, but that, if exposed to unauthorized parties, may have an indirect or possible adverse impact on Boston College.

- **Public Information** is information that is generally available to the public, or that, if it was to become available to the public, would have no material adverse effect on Boston College.

Continue on page 2....
Data Security

Data Security Officers have been appointed by each Dean or VP to a Data Security Working Group to help develop procedures and guidelines, and to assist the University in the implementation of the policy.

Violations of the policy will lead to appropriate disciplinary action, which could include temporary or permanent restrictions on access to certain information or networks. For more information on this policy, contact your Data Security Officer or Vice President.

Minimizing the Effects of Malware

From http://onguardonline.gov/malware.html

OnGuardOnline.gov provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information.

Malware, is short for “malicious software.” This software could include viruses and spyware programs installed without your consent to monitor or control computer actions. These programs are created to steal personal information, send spam, and commit fraud. Websites are created to entice you to click on a link that could download malware. OnGuardOnline.gov says consumers can minimize the havoc malware can cause.

You may be infected if you notice that your computer has significantly slowed down, won’t shutdown or restart, or displays a lot of pop-up ads. If you suspect malware is on your computer:

- Stop online activities that involve user names, passwords, or other sensitive information. Your personal information may not be going to where you think it is going.

- Verify that your security software is active and current. Check for anti-virus and anti-spyware software. Once you confirm that your security software is up-to-date, run it to scan your computer for viruses and spyware. Delete everything the program identifies as a problem.

- If you are still experiencing problems, contact your technology consultant.

- To minimize malware infections in the future (1) don’t click on a link in email or open an attachment unless you know who sent it and what it is, and (2) don’t download and install software unless you know the website and trust it.
In the News......

What is a phishing attack?

In computing, phishing is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. eBay, PayPal and online banks are common targets. Phishing is typically carried out by email or instant messaging, and often directs users to enter details at a website, although phone contact has also been used.1

When users respond with the requested information, attackers can use it to gain access to the accounts.

How do you avoid being a victim?

- Do not reveal personal or financial information in an email, and do not respond to email solicitations for this information. This includes following links sent in an email.
- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Don’t send sensitive information over the Internet before checking a web site's security policy or looking for evidence that the information is being encrypted. Signs of encryption include a URL that begins with “https:” and a padlock icon in the bottom of your browser window.
- Pay attention to the URL of a web site. Malicious web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person’s authority to have the information.
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a web site connected to the request; instead, check previous statements for contact information. More information about phishing is available from the Anti-Phishing Working Group at: http://www.antiphishing.org/ or OnguardOnline at http://www.onguardonline.gov/phishing.html.
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic.

From the BCITS Help Center: Watch a video to find out more about phishing e-mail scams and how they are used for identity theft: http://www.microsoft.com/athome/security/email/phishing/video1.mspx

Take a phishing quiz: http://www.sonicwall.com/phishing/

Cash/Check Handling Control Tips...

Following are some tips to ensure that all cash and check transactions are accurately recorded in the University financial system and the money has been deposited intact in the bank.

- **Count Cash on Hand:** A manager, separate from the custodian of the cash, should verify that the mode of payment (cash/check) for the cash receipts agrees with the check and cash composition of the funds that the custodian is collecting. Make sure that all checks have been stamped “for deposit only” immediately upon receipt.
- **Verify Record Keeping:** Make sure that all revenue transactions have been accurately recorded (either manually, or by computer cash registers) into the appropriate account on the University financial system.
- **Verify Bank Deposits:** Ensure that your department receives a receipt from the Cashier’s Office or Armored Car pickup. Verify that the mode of payment for all transactions recorded on the receipt agrees with the check and cash composition.
- **Reconciliation:** Validate your receipts with your monthly financial system reports.
- **Voids:** Verify that all voided documents are properly accounted for, controlled, and reconciled.
- **Budget:** Ensure that all revenue sources and fees have been identified and included in your budget so that you will know if checks or cash has not been received for a particular activity. Monitor the budget versus actual revenue received.
- **Physical Security:** Ensure the safe or vault combination is changed periodically and that safe combinations have not been written down anywhere in the office. Verify that access to safes or vaults is limited to the least practical number of employees.
- **Write-Offs:** Ensure that all write-offs are authorized, approved, and properly documented.

1 http://en.wikipedia.org/wiki/Phishing
Should Boston College Departments be Concerned About PCI Compliance?

YES! The Payment Card Industry Data Security Standard (PCI DSS) applies to any department that collects, stores, processes, or transmits credit or debit card information. If your department does any of the above, PCI Compliance is not a request, or suggestion, it is now a requirement. The University is working to implement new systems to ensure compliance. However, departments still have an ongoing responsibility to protect credit card data. For the University to maintain compliance, we must adhere to the following:

- not storing credit cards on your PC. If you need to keep credit card data, it should be kept in an approved PCI system.
- restricting access to payment card account numbers on a need to know basis.
- authenticating with the use of a unique username and password. DO NOT SHARE PASSWORDS!
- protecting credit card information against unauthorized access including paper or fax copies.
- never storing the contents of any track information including the three digit card validation code.
- properly disposing of cardholder data when no longer needed. Shred paper and delete files from your computer.
- not entering into an agreement with any third party vendor that collects credit card data from your customers without an appropriate contract.

Why do I need to document anything? I know what I’m doing with my work.

Documentation is a specific set of instructions to explain and maintain your processes and controls. For example, often one person in a department develops and implements certain departmental processes. The successful use of these processes and the production of specialized data may depend on the continued presence of a single individual. If that person leaves the University, specific knowledge about that process may be lost.

If I don’t properly document my work, what could happen?

Inadequate documentation can result in:

- loss of processing time
- loss of records/files necessary to support an operation
- over-reliance on knowledge of only one key individual

How extensive should my documentation be?

Documentation serves as communication to employees on how to handle a particular process and why. This aids in the consistent application of processing (efficient and effective) transactions and how to address unauthorized, incomplete, or erroneous transactions. Providing the “why” information assists employees in identifying what critical information needs to be maintained should a new system or changes within a federal regulation, state statute or University policy occur.

Documenting procedures is essential for communication, analysis, accountability and control. Adequate documentation permits correct accounting and helps prevent errors in processing and recording. Basic documentation should include:

- a summary of the process including key controls.
- specific procedures for running a program or processing records.
- a list of file names or system descriptions needed to process certain records.
- decisions that are made and agreed upon by management to alleviate future misunderstandings.