AuditNews

Produced by: Internal Audit (617) 552-8689 **Spring 2005** Volume XXXVIII

Hot Off the Press…….

Identity thieves' new ploy: `pharming'

First online crooks went "phishing," and now they're getting into "pharming" to reap their harvest of potential identity-theft victims. Pharming is a new scam that automatically directs computer users from a legitimate Web site to a fraudulent copy of that site -- without any warning signs. The fraudulent site collects passwords, credit card numbers or other private information for potential misuse. Security experts say such attacks are rare so far but could grow in the coming months in much the same way phishing scams have exploded.

http://www.siliconvalley.com/mld/siliconvalley/news/local/11324938.htm

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

What is Business Ethics?	2
What is Conflict of Interest?	2
In the News: Identity Thief	3
Ask the Auditor!	3
Fraud Prevention Measures	4
More News…..	4

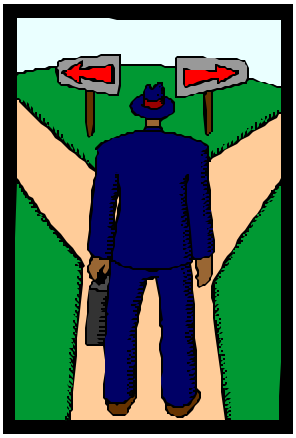
Improving Computer Security

Just one weak link in the chain of computer security can allow an attacker to gain a foothold to the network. There are ways to improve the overall security of your computer and confidentiality of data to make it less vulnerable.

S	**ecurity is Everyone's Responsibility**. Everyone has a responsibility to ensure that computers and the data they contain are safe.
E	ach person should manage data in a way that reflects its sensitivity, whether it is displayed on a screen, downloaded or printed.
C	omputers can store any information that you type. Be careful when entering sensitive data such as credit cards onto computers in laboratories and cyber cafes.
U	se a hard-to-guess password; typically a combination of alpha and numeric characters. Passwords should not be written down or given to another employee.
R	emember to back up your computer data and keep those backups in a safe place.
I	ntruders are always discovering new vulnerabilities (informally called "holes") to exploit in computer software. Install patches, or correctly configure the software to operate more securely.
T	hink before sharing your user id and password with someone (hacking often begins with someone posing as technology support requesting your password).
Y	ou should be careful about individuals "phishing" for your personal information. Do not give out private information that could be used for identity theft

T	reat the Internet as the "Wild West". Presume any messages sent over the Internet are available to the public.
I	ndividuals may inadvertently place files with sensitive personal information in their directory of files to be shared. Sharing access to your computer with strangers can be risky.
P	rotect your system. Use "anti-virus software" and keep it up to date.
S	cam artists use email attachments to compromise your computer. Do not open email attachments or click on links in emails from someone you do not know or trust.

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.

BENEFITS OF MANAGING ETHICS IN THE WORKPLACE

Ethics programs

- cultivate strong teamwork and productivity.
- support employee job growth.
- can assist management to ensure that policies are being followed.
- help avoid criminal acts.
- promote a strong public image.

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.

What is Conflict of Interest?

The basis for Conflict of Interest rules is the desire to promote integrity and preserve public trust by avoiding bias.

Conflicts of interest often relate to situations where an employee uses influence with the University for personal gain.

The basis for Conflict of Interest rules is the desire to promote integrity and preserve public trust by avoiding bias.

A possible conflict of interest exists if an employee (or an employee's family member):

- has an existing or potential financial or other interest that impairs a person's independent judgment when performing University responsibilities.
- has a significant business relationship with a person or firm engaging in, or seeking to engage in, business with the University.
- has a significant ownership interest, and may receive financial or other benefits from knowledge or information confidential to the University.

On an annual basis, all University officers, deans, directors, and those employees designated by the President because of their respective duties and responsibilities are required to disclose to the University all business interests, affiliat and/or relationships that reasonably give rise to a conflict of interest.

In the News: Identity Theft

"Take Charge: Fighting Back Against Identity Theft," February 2005, The FTC.

The Federal Trade Commission (FTC) has produced instructions to help remedy the effects of an identity theft.

"Despite your best efforts to manage the flow of your personal information or to keep it to yourself, skilled identity thieves may use a variety of methods to gain access to your data by:

- stealing records or information while they're on the job
- bribing an employee who has access to these records
- hacking these records
- conning information out of employees
- stealing mail, including bank and credit card statements
- rummaging through trash
- stealing your wallet
- completing a "change of address form" to divert your mail to another location
- stealing personal information from you through email or phone by posing as a legitimate company

If you've lost personal information or identification, or if it has been stolen from you, taking certain steps quickly can minimize the potential for identity theft.

Close accounts, like credit cards and bank accounts, immediately. When you open new accounts, place passwords on them. Avoid using your mother's maiden name, your birth date, the last four digits of your Social Security number (SSN) or your phone number, or a series of consecutive numbers.

If your information has been misused, file a report about the theft with the police, and file a complaint with the Federal Trade Commission.

While dealing with problems resulting from identity theft can be time-consuming and frustrating, most victims can resolve their cases by being assertive, organized, and knowledgeable about their legal rights. Some laws require you to notify companies within specific time periods. Don't delay in contacting any companies to deal with these problems, and ask for supervisors if you need more help than you're getting."

For detailed information about Identify Theft, go to http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm

Ask the Auditor!

Can an audit be requested?

Yes, an internal audit can be very beneficial especially if there has been a change in either the management of the area or in key personnel. An audit can (1) provide an assessment of current internal controls, (2) evaluate business risks, and (3) assist in the modification of procedures. An audit will provide an independent appraisal of the effectiveness and efficiency of an area's activities.

What are business risks?

Business risks are simply those circumstances (events or activities) that can adversely affect the achievement of the University's objectives. Some examples include: misappropriation or unauthorized use of funds or assets, false entries to payroll or expense accounts, receipt of substandard supplies, and purchases made from suppliers related to buyers or other employees.

What if I suspect fraud?

Any person who suspects or has knowledge of fraud or unethical activities at the University should contact the Director of Internal Audit. If presented with reasonable evidence of a suspected fraud, the Director will conduct an audit to determine if the reported suspicions of fraud are valid. The Director will also inform the supervisor of any employee under investigation. If, based on the results of the audit, the Director has reason to believe that fraudulent activities have occurred; he or she will report the findings to the President, the Executive Vice President, the Financial Vice President and Treasurer, and the Controller.

Can I remain anonymous if I suspect fraud?

You will not be required to identify yourself, but you will be asked to provide as much detailed information as you can about the alleged wrongdoing so that an adequate and appropriate investigation can be performed.

Does Internal Audit ever conduct surprise Audits?

Usually the area to be audited will be notified. However, sometimes surprise audits are conducted.

Fraud Prevention Measures

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/

It is important to distinguish between Internal Audit's role and University management's role concerning white-collar crime. 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 by analyzing and testing controls. We also perform fraud investigations, and promote a positive control environment throughout the University.

Internal controls can be categorized as ***accounting controls*** or ***administrative controls***.

Accounting controls are designed to safeguard University assets and ensure the accuracy of financial records. Administrative controls are designed to promote operational efficiency and adherence to University policies and procedures.

Signals of Fraud:

- alteration of documents
- duplicate payments
- journal entries without documentation
- failure of employees to take vacations
- significant increases or decreases in account balances
- products or services purchased in excess of needs
- missing documentation

Fraud Prevention Checklist:

- review company contracts
- create periodic job rotation
- track unsuccessful attempts to access a computer
- encrypt data files and data transmissions
- maintain appropriate backup of files
- request an information system security review

For more information on fraud prevention, go to:

http://www.bc.edu/offices/audit/fraud/

More News.....

Mobile Virus Moves to New Level
A new mobile virus is spreading by pretending to be a returned message from a friend. The Mabir.A virus affects Symbian Series 60 phones and is sufficiently similar to the first mobile phone virus Cabir to make some experts think it has the same author. But rather than just relying on Bluetooth to spread Mabir.A uses incoming messages to spread, making it potentially more virulent.
http://www.vnunet.com/news/1162311

Building a Hacker-Proof Network
Scientists see answer in quantum cryptography. David Pearson is attempting to build an un-hackable network. Pearson is a division scientist at BBN Technologies, a private research company in Cambridge, Mass., which is most famous for building, in 1969, the first few nodes of a computer network connecting its headquarters to Harvard University and Boston University that over time would evolve into the Internet. Now the firm has built a network it says is impervious to hackers.
http://www.msnbc.msn.com/id/7394350/

What Search Sites Know About You
For most people who spend a lot of time online, impulsively typing queries into a search engine has become second nature. Chances are the queries will unearth some enlightening information. But while search engines are quite up front about sharing their knowledge on topics you enter in the query box, it's not so clear what they know about you.
http://www.wired.com/news/privacy/0,1848,67062,00.html