R·I·T

Institute Audit, Compliance & Advisement

the Quaestor Quarterly

Volume 6, Issue 2 Summer 2011

quaes·tor [kwes'tôr] 'one who asks questions'

Ten Tips for Safer Social Networking

Did you know you're a target every time you go online? Did you know that cyber criminals are targeting social networking sites? Do you know how to recognize a phishing attempt? Following these tips will help make your use of social networking sites safer. While there's no way to guarantee that social networking sites are safe, following these tips will help make your use of them safer.

Tip #1: Use strong passwords/passphrases.

It's important to use strong passwords because automated "cracking" programs can break weak passwords in minutes. At a minimum, you should follow the RIT Password Security Standard, with a minimum of 8 characters, mixing upper and lower case letters and numbers. Many websites also allow the use of longer passwords and special characters. Incorporating special characters into your password will make them more difficult to crack. You'll also want to use different passwords on different accounts. Using a password safe such as LastPass will help you manage these passwords by generating strong passwords and then supplying them when needed.

Tip #2: Keep up to date.

Attackers take advantage of vulnerabilities in software in order to place malware on your computers. Keeping up to date with patches/updates helps thwart attackers from using "exploits" to attack known vulnerabilities. It's important to keep both your Operating System (Windows, Mac OS, Linux, etc.) and your applications (Microsoft Office, Adobe, QuickTime) patched.

Tip #3: Use security software.

It's a good practice to follow the requirements of the RIT Desktop and Portable Computer Security Standard on personally-owned computers as well as RIT computers. Among other elements, the standard requires use of a firewall, antivirus, and anti-spyware programs. Many security suites contain all of the elements needed to protect your computer. (Your Internet Service Provider may also provide security software.)

Tip #4: Learn to recognize phishing attacks.

You've all seen phishing attacks. They're typically emails that appear to come from a financial institution that ask you to verify information by providing your username and password. Never respond to these requests. Your financial institution should not need your password.

(continued on p. 2)

IACA's Mission

Institute Audit, Compliance & Advisement promotes a strong internal control environment by objectively and independently assessing risks and controls; evaluating business processes for efficiency, effectiveness, and compliance; providing management advisory services; and offering training to the University community. We focus on preserving the resources of the University for use by our students as they prepare for successful careers in a global society.

Inside This Issue **Page**

IACA Institute Audit, Compliance & Advisement

Ten Tips for Safer Social Networking (continued from p. 1)

Tip #5: Think before you post.

Don't post personal information (contact info, class schedule, residence, etc.), as a talented hacker can see this even if you've restricted your privacy settings! Don't post potentially embarrassing or compromising photos. Be aware of what photos you're being "tagged" in—don't hesitate to ask others to remove photographs of you from their pages.

Regarding placing of RIT Private or Confidential Information on social networking/media sites, the RIT Information Access and Protection Standard forbids storage of Private or Confidential Information on social networking/ media sites that are not administered by RIT. Please use discretion when considering placing Internal Information on these sites.

Tip #6: Remember who else is online.

Did you know that most employers "Google" prospective employees? Have you seen the stories of people's homes being burglarized because they've posted their vacation plans online? Many people other than your friends use these sites.

Tip #7: Be wary of others.

You can't really tell who's using a social network account. If you use Facebook, you've certainly seen posts by your "friends" whose accounts have been compromised. Don't feel like you have to accept every friend request, especially if you don't know the person.

Tip #8: Search for your name.

Have you ever done a "vanity search?" Put your name in a search engine and see what it finds. Did you know that Google allows you to set up an Alert that will monitor when your name appears online? Setting this up with daily notifications will help you see where your name appears.

Tip #9: Guard your personal information.

Using information you share, identity thieves can put together a profile to help them impersonate you. Be especially careful of Facebook applications. They may collect information that they sell to marketing companies and their databases could be compromised. Do they really need the information they're requesting?

Tip #10: Use privacy settings.

Default settings in most social networks are set to share all information. Adjust the social network's privacy settings to help protect your identity. Show "limited friends," a cut-down version of your profile. Choose the strongest privacy settings and then "open" them only if needed.

~~ Contributed by Ben Woelk
Policy and Awareness Analyst,
Information Security Office, RIT

Control of the Quarter

In the last newsletter we discussed the five interrelated components of internal control which are designed to help the organization and its management achieve operational objectives. The control components, which are derived from the way management runs an organization, include:

1. Control Environment
2. Risk Assessment
3. Control Activities
4. Information and Communication
5. Monitoring

The ***control environment*** sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. The control environment encompasses many factors including:

- ✓ The integrity, ethical values and competence of the entity's people
- ✓ Management's philosophy and operating style
- ✓ The way management assigns authority and responsibility, and organizes and develops its people
- ✓ The attention and direction provided by the board of directors

According to the Institute of Internal Auditors, the most efficient and cost-effective way to implement and assess internal control is to develop "control consciousness" throughout the organization. While every employee in the RIT community has a personal and professional obligation to put forth a good faith effort to protect the university's assets and resources, a manager has a particular responsibility to ensure that the control environment in his/her business unit/department is aligned with the expectations of the university. Examples include:

- ✓ Ensuring that employees understand the organization's objectives and know how his/her actions contribute to their achievement
- ✓ Defining key areas of authority and responsibility for operating activities
- ✓ Ensuring that employees understand they are accountable for their actions and that their activities have a direct impact on the internal control system

(continued on p. 4)

"I believe in evidence. I believe in observation, measurement, and reasoning, confirmed by independent observers.

I'll believe anything, no matter how wild and ridiculous, if there is evidence for it.

The wilder and more ridiculous something is, however, the firmer and more solid the evidence will have to be."

- Isaac Asimov, scientist and writer (1920-1992)

Control of the Quarter

(continued from p. 3)

To assist employees in understanding their roles and responsibilities related to internal control, the Controller's Office offers several training workshops throughout the year including the "Accounting Practices, Procedures and Protocol (P^3)" workshop series which includes a specific "Internal Controls and Fraud in the Workplace" class, as well as the "Sponsored Programs Accounting and Regulatory Certification (SPARC)" workshop series. Managers should encourage employees involved in any aspect of financial administration to attend these workshops – ongoing training for employees is essential to achieving the objectives of the organization. Information about our training workshops is available on the Controller's Office web site: http://finweb.rit.edu/controller/training/. The schedule for the upcoming fiscal year will be available soon.

In the next newsletter we'll review the major principals related to the achievement of control objectives at the risk assessment level including identifying, analyzing and managing risks.

~~ Contributed by Lyn Kelly
Controller and Assistant Treasurer

Training Opportunities Provided by IACA

IACA's Internal Controls and Fraud in the Workplace classes have been merged into one effective February 1, 2011. This new class is two and one half hours in length and is a required class to receive the RIT Accounting Practices, Procedures and Protocol Certificate of Completion.

To learn more about these important topics, sign up for IACA's Internal Controls and Fraud in the Workplace class at the CPD website: http://finweb.rit.edu/cpd/leadership/internalcontrolsandfraud.html

Upcoming Sessions:

October 13, 2011 1:30 - 4:00 pm 2140 Louise Slaughter Hall	January 17, 2012 1:30 - 4:00 pm 2140 Louise Slaughter Hall	April 4, 2012 9:00 - 11:30 am 2140 Louise Slaughter Hall

Word on the Street

I recently had the pleasure of acting as a key contact for a team of auditors. I imagine most people would assume that must be a joke; audits are usually portrayed as the next best thing to a colonoscopy. However, I am sincere. Several of our programs and accounts in the Saunders College of Business (SCB) were examined as part of RIT's Office of Institute Audit, Compliance & Advisement's (IACA) continuing charge. The purpose behind these audits, as I believe is true almost 100% of the time, is to help the departments and programs being examined. Yes, to help US. While it's certainly true that if it was discovered that we were doing anything inconsistent with policy or practice (doing anything "wrong") the auditors would need to further investigate and understand it. It was clear from the outset through the end-of-audit reception that the goal of the audit team was to help us improve our operations and success, help us ensure things would run smoothly, and help us ensure we were engaging in best practices. In short, the audit was designed and executed in a way that we felt the team was there to make life better for us (work life, anyway).

The IACA team of three was always professional, nice, friendly, engaging, and respectful. They did not come across as suspicious of anything we were doing; contrary to the stereotypical portrayal, they did not come across as adversaries. They gave us adequate notice of meetings that needed to be scheduled with individuals or groups, they took no more time than they asked for, they were prepared for the meetings, and they stuck to the topics at hand. Throughout the audit, they provided written updates of status, including issues they were looking into, thereby keeping us apprised of progress and of matters they and we would need to further examine. At the end, they provided us with an extensive, detailed report. The report explained processes and practices through which we could enhance our efficiency and effectiveness, thereby better managing our operations. This was time well spent and it has already paid dividends.

I am a CPA and have been involved on both sides of audits for many years. The IACA team is among the very best with which I have had the pleasure to work.

~~ Contributed by Bill Dresnack
Senior Associate Dean, E. Philip Saunders
College of Business

What about *ethics* in the workplace?

To learn more about
RIT's Code of Conduct and the RIT Ethics Hotline,
check out http://finweb.rit.edu/svp/ethics/

~ Ask the Auditor ~

Submit a question to the IACA webpage http://finweb.rit.edu/iaca/forms/ask/ by September 9, 2011. If your question is chosen for publication in our newsletter, you will receive a prize valued at $15.

IACA TEAM:

Steven M. Morse '86, CPA
assistant vice president
475-7943

Patrick M. Didas '90, CPA, CFE, CCA
associate director
475-6826

Wendy J. Roy, CPA
senior internal auditor
475-7011

Nancy A. Nasca, CPA, CIA
senior internal auditor
475-5293

Elisa M. Cockburn, CPA
senior internal auditor
475-7849

Christine M. VanHemel
staff & audit assistant
475-7647

Victoria S. Foster
co-op student internal auditor assistant
475-4318

Pop Quiz Challenge

Take the Pop Quiz Challenge! Correctly answer the question below and you will be entered in a drawing to win a prize valued at $15. One lucky winner will be chosen randomly and notified by email.

Question: Which internal control term listed below is defined as: *The development of policies and the performance of procedures designed to ensure that the steps necessary to address risks which may prevent the organization from reaching its objectives are carried out.*

A. Control Environment

B. Risk Assessment

C. Control Activities

D. Information and Communication

E. Monitoring

Post your answer to our Quiz webpage at:
https://finweb.rit.edu/iaca/forms/quiz/

The winner's name and answer will be included in the Fall '11 Quaestor Quarterly Newsletter.

****

Congratulations to Jennifer Rivera from the Student Health Center for correctly answering the Winter issue's Pop Quiz question.

The question and the correct answer was: Only one of the following scenarios represents fraudulent activity while the rest are financial abuse. Select the fraudulent activity.

A. Providing a pizza delivery driver a 34% ($80) tip on a $240 order.

B. Unnecessarily spending down the department budget at the end of the fiscal year in order to "use it or lose it."

Correct

C. Rounding up hours recorded on a time sheet (i.e., actual hours worked are 8:05 – 4:55; but for time sheet purposes 8:00 – 5:00 is recorded).

D. Turning down the meals included in a conference registration fee and purchasing different meal choices for reimbursement.

R·I·T