digital
self
defense

Protect yourself and everyone else

RIT Information Security Advisory

Scam Watch!

RIT Public Safety has reported several scam attempts over the last quarter. We thought we would share them with you so that you'll recognize them and similar scams.

Why I'm Receiving This

We've received reports of the following scams:

- **Personal ads**—an RIT student reported that he responded to a Craigslist Personal Ad that he found "enticing." He exchanged pictures with the person in the ad who requested that he sign up for an account on saferaffair.com under the pretense that he wasn't some "crazy stalker." The website requested personal information and a credit card number "to verify your identity." When he looked up the person's email address he found that there were hundreds of complaints that the address belonged to a scammer.
- **Freelance photographer request**—an RIT student received a letter from a firm seeking to employ the student to shoot an upcoming out-of-town event. They offered the student $500/hour for his time and mailed the student a check for $2900 with instructions to cash the check, retain a portion of the funds, and forward the remaining share to the "store manager." This is a common scam where someone sends a counterfeit check and asks for a portion of the check to be wired to someone else.
- **Financial emergency overseas**—several RIT people received an urgent note from a known RIT student regarding a robbery he has suffered overseas. The note requested the recipient to wire funds ASAP so that the individual could buy a plane ticket home. The RIT student's Facebook account was compromised and used to send this message to his Facebook friends.

In addition to the scams listed above, RIT students have fallen victim to the following scams in the last couple of years:

- **Lottery Winner**—an RIT student was contacted by a Facebook Friend who informed him he had won a deaf lottery. The student was then contacted by an "administrator" through instant messaging. During the course of the scam, the student provided his bank account information and his account was hit for hundreds of dollars.
- **Housing listing**—an RIT student posted a "Roommate Wanted" notice. The student received a response from a prospective roommate. The prospective roommate sent the student a cashier's check and asked the student to refund the difference. Although the check

appeared legitimate, it was counterfeit.

- **Craigslist**—several RIT students listed items for sale and were contacted by "buyers" who sent the students cashier's checks and asked the students to refund the difference. Again, although the checks appeared legitimate, they were counterfeit.

These incidents are examples of common online scams. Typically, the recipients of the cashier's checks are able to deposit the checks into their bank accounts without a problem. A couple of weeks later, the Federal Reserve system notifies the banks that the checks were bad and the check recipients have "lost" the money they refunded to the fraudsters.

What RIT is Doing

- RIT Information Security and Public Safety work to detect these threats and report them to the RIT community as they occur.
- RIT provides anti-virus software to RIT faculty, staff, and students. Anti-virus software will provide some protection against malicious software.
- The RIT Information Security Office provides information on Safe Social Networking and other safe practices at http://security.rit.edu/dsd/bestpractices.html

What You can Do

If you are the recipient or victim of an online scam, contact RIT Public Safety at (585) 475-2853.

If you believe your password may have been compromised, contact the appropriate help desk immediately. Students should contact the ITS HelpDesk at (585) 475-4357 (phone), (585) 475-2810 (TTY).

If you suspect the presence of malicious content on an RIT web site, contact the Information Security Office. See http://security.rit.edu/cih.html for more information on how to report incidents of all types.

We've included links below to safe social networking practices. Here are a few tips:

- **Don't Post Personal Information Online!**
  It's the easiest way to keep your information private. Don't post your full birth date, your address, phone numbers, etc. Don't hesitate to ask friends to remove embarrassing or sensitive information about you from their posts either. *Be especially careful what information you reveal through Facebook Applications*. You may find that you've revealed all sorts of information about yourself--information that could help an identity thief impersonate you.
- **Use Built-In Privacy Settings**
  Most social networking sites offer various ways in which you can restrict public access to your profile, such as only allowing your "friends" to view your profile. Of course, this only works if you only allow a few people to see your postings--if you have 10,000 "friends" your privacy won't be very well protected. Your best bet is to disable all the extra options, and re-

enable only the ones you know you'll use.

- **Be wary of others**
  Recent research by Sophos found that 41% of Facebook users were willing to befriend a plastic green frog named Freddi Staur (an anagram of ID Fraudster), subsequently revealing their personal information. Most sites do not have a rigorous process to verify the identity of members so always be cautious when dealing with unfamiliar people online.
- **Search for yourself**
  Find out what information other people have easy access to. Put your name into Google (make sure to use quotes around your name). Try searching for your nicknames, phone numbers, and addresses as well--you might be surprised at what you find.

For More Information

FBI New e-scams and Warnings http://www.fbi.gov/cyberinvest/escams.htm

Fake Check Scams http://www.fraud.org/tips/internet/fakecheck.htm

Craigslist Scams http://www.craigslist.org/about/scams

Deaf Lottery Scam http://www.nad.org/node/437

Lottery Scams http://travel.state.gov/travel/cis_pa_tw/cis/cis_2475.html

Roommate Scams http://ezinearticles.com/?Beware-of-Roommate-Scams&id=1499613

FTC OnGuard Online http://www.onguardonline.gov/

11 Tips for Social Networking Safety
http://www.microsoft.com/protect/parents/social/socialnet.aspx

Ben Woelk

Information Security Office
Rochester Institute of Technology
Ross 10-A204
151 Lomb Memorial Drive
Rochester, NY 14623
585-475-4122
fbwis@rit.edu
http://security.rit.edu/dsd/bestpractices.html
Become a fan of RIT Information Security at
http://rit.facebook.com/profile.php?id=6017464645
Follow us on Twitter: http://twitter.com/RIT_InfoSec