UC Monthly Safety Spotlight, October 2011

Crime Prevention and Personal Security

Careless Chris Learns that Even Invisible Property Needs Protecting …an Imaginary Scenario

Fictitious employee Careless Chris learned a hard lesson a year ago when her UC laptop was stolen from a conference room.* After that profoundly embarrassing incident, she resolved to take scrupulous care of her new computer and other University-owned assets.

Chris worked with staff researchers, graduate students and visiting faculty. After her lost laptop was replaced, she resumed her work creating graphs, reports and presentations for the research team. She occasionally took work home, using a USB drive to transfer data to her home computer and then back to her laptop at work.

Chris's latest project was creating a new database that would streamline the process of storing, retrieving and displaying data. Her plan was to surprise her supervisor with the results and be praised for her initiative and creativity. Chris collected staff credentials, office locations and contact information, from the Principal Investigator to the graduate students. She gathered test results to sort by value and date.

One Thursday afternoon, Chris decided to print some large-format documents at an off-campus quick-print shop to test the quality. Since she couldn't find a USB drive issued by her department, she decided to use a drive that was in the bottom of her bag. She didn't exactly remember where it came from but everyone in her family used it, including her teen-aged son and his friends (for video game short-cuts), her husband and others. Just before leaving the office, Chris plugged the USB drive into the department computer and copied the data she needed. Remembering the danger of laptop theft, she carefully secured her computer before turning out the lights and locking the door.

Careless Chris didn't realize it, but locking the door wouldn't do much to prevent crime on this particular afternoon. The instant she plugged in her well-used USB drive, the malicious code it contained found her neatly organized folders. The names, contact numbers, countries of origin of her department's staff, research data and more were soon flowing to a hacker's website, and the virus was doing its best to spread throughout the system.

The following morning, Chris was preparing to present her new database project at the staff meeting, including the large-format graphics. "They are just going to love this new process," she said to herself, satisfied with all her hard work.

Her musings were interrupted by some disturbing news, however. One of the post-grads was alarmed to find information about her student visa on a social networking site. A lab assistant's private email account was suddenly overwhelmed with spam emails. The Principal Investigator was shocked when a science editor called to interview him about what should have been highly confidential research.

Continued

Safety Spotlight is a UC System-wide publication of the Environment, Health and Safety Leadership Council, UC Office of the President

UC Monthly Safety Spotlight, October 2011

Crime Prevention and Personal Security

After a flurry of confusion, remedial action by the IT staff and some diligent investigative work, the problem was tracked down to Chris's work station and the prime suspect: her personal USB drive. Chris was mortified to once again be the agent of loss and disruption. By failing to follow data security guidelines, she had endangered the security of her co-workers' personal files as well as important university research. "Not again!" she cried. "What a catastrophe! What could I possibly have done to prevent this?"

First of all, Chris shouldn't have been taking confidential information out of the office unless specifically approved by her supervisor. Likewise, she should not have stored personal information about her co-workers on any kind of drive (USB, DVD, home computer) without prior authorization. Normally, only specific department leaders and the Human Resources department should have access to these kinds of files. Chris should not have used any media at work that wasn't authorized by her department. Opportunities for malicious code to find its way onto a storage device, either by intent or by accident, are dramatically increased when it is shared by many people.

Finally, Chris should have followed her department's standard operating procedures for printing or publishing confidential information. By plugging a USB drive packed with department files into the print shop's server, she again exposed confidential data to unauthorized use.

Chris still has a lot to learn about security, whether it applies to tangible or invisible assets.

*Read "The Case of the Purloined Laptop" originally published in *UC Davis Monthly Safety Spotlight,* August 2010

UC Monthly Safety Spotlight, October 2011

Crime Prevention and Personal Security

The Case of the Purloined Laptop…an Imaginary Scenario
Originally published in UC Davis Monthly Safety Spotlight, August 2010

Fictitious employee Careless Chris loved her campus job. She enjoyed being on the forefront of educational research and working with graduate students and visiting faculty. As the department's lead admin, Chris was responsible for keeping track of schedules, meetings and special programs, as well as budget and human resources information. She helped process data for her learned colleagues, created graphs and reports, and specialized in feature-enhanced PowerPoint presentations.

Chris had great PC skills and treasured her trusted laptop with the enhanced memory and speed that made it possible for her to work with peak efficiency. This particular week, she and her co-workers were excited about an international conference scheduled two weeks away. Chris worked intensively with project leaders and concentrated on creating a sophisticated document packed with graphics and data for the presenters.

Chris considered herself very diligent in safeguarding her laptop. She protected it from extremes of temperature. She never left the laptop in her car if she took work home or to another location. She had created a foolproof log-in passphrase, and she backed up important files every Monday morning. She felt confident that by taking these precautions, she was not vulnerable to theft. Overall, she felt her laptop was safe and secure while on campus.

A few days before the international meeting, Chris and her colleagues met in a campus conference room first thing in the morning to practice the presentation. Chris's laptop took center stage on the podium as the presenters stepped through their talks. At midmorning, the group moved to an adjoining room for a coffee break and further discussion. Ten minutes later, Chris returned to the conference room and was horrified to see an empty space on the podium where her laptop used to be. At first, she rushed around searching and asking everyone in sight if they knew anything about the laptop. Before long, Chris was forced to accept the fact that the laptop had probably been stolen. She called campus Police and made an appointment to file a report.

Chris was devastated. She knew she'd have to work extra hard to re-create the presentation in time, and she felt very keenly the worry and frustration of her colleagues when they learned of the theft. However the consequences went far beyond the international meeting presentation. The costs added up quickly: the computer itself and its hardware enhancements and software packages; the labor involved in setting up a new computer and retrieving or recreating lost files. Confidential personnel and budget data and unpublished research information were compromised. Chris's mistakes included leaving her laptop unprotected in a public place, not backing up data often enough, and not adequately securing the department's confidential information.

After learning a lesson the hard way, Chris has added a new capability to her skill set. She is now spearheading a new departmental data security policy to help ensure that her group's hardware, software and data are protected. Whether on campus or off, she now takes more effective steps to secure valuable property.

Safety Spotlight is a UC System-wide publication of the Environment, Health and Safety Leadership Council, UC Office of the President

UC Monthly Safety Spotlight, October 2011

Crime Prevention and Personal Security

Invest your Attention on Your Personal Safety

Though it's easy to let your thoughts drift as you move through your day-to-day routine, the cost of this distraction can be a purse or backpack snatch or worse. The next time you're walking, cycling or jogging, make a conscious effort to examine your surroundings carefully. "Don't walk about with both ears plugged while you listen to music," advises Chief Spicuzza; "Trust us, you won't hear anyone coming up from behind." Use all five senses—including your sixth sense—and stay alert for possible threats. Try using this mental checklist:

- Are there nearby areas that could conceal a criminal?
- Where is the nearest open building entrance if you need to ask for help?
- Are you weighed down by excessive bags and packages?
- Are your shoes suitable for running if that becomes necessary?
- Is your cell phone easy accessible, and is the emergency number programmed in?
- Do you know how to describe your location to the dispatcher?
- Do you really need to talk or text right now, or can you postpone the distraction and pay attention to your surroundings instead?
- Police agencies also encourage you to follow these simple tips:
- Use lit paths and well-traveled areas when you go out at night.
- Don't jog or walk alone. Travel with a group or at least in pairs.
- Take advantage of escort services whenever they are available.
- Don't leave valuables in plain sight in your vehicle. Even if you try to conceal your possessions, thieves may still break in.
- Keep careful control over laptops and other electronics when you're in the library, meeting rooms, cafes or other public areas on campus.
- Keep your office, laboratory or workshop doors locked if you're working after hours.
- Don't prop doors open. If they are meant to be closed and locked, leave them that way.
- Lock your purse, backpack and other valuables in a drawer or cabinet if you step away from your workspace.

Take Advantage of Campus Resources

Your UC police department and other emergency response professionals are there to help you. Time spent exploring their websites for advisories, program and educational opportunities and other information is time well spent. Follow up by attending crime prevention, self-defense and emergency response courses. "The most important advice I have for everyone in our campus communities is to stay vigilant and stay involved," says Chief Spicuzza; "When you combine individuals who take responsibility for their own safety with professionally trained and equipped officers, you have a very powerful, effective, crime-deterring partnership."

Safety Spotlight is a UC System-wide publication of the Environment, Health and Safety Leadership Council, UC Office of the President

UC Monthly Safety Spotlight, October 2011

Crime Prevention and Personal Security

Be Your Own Security Force

As the days get shorter and activity picks up on UC campuses, the need for crime prevention is more important than ever. Tough economic times trigger property crimes, and crimes against people are another unfortunate fact of life. And though law enforcement professionals are on the job, prevention is much more effective when individuals take an active role in protecting themselves.

Keeping yourself and your possessions secure in the fast-moving campus environment is a joint effort shared by you and your local UC police department. “Police officers are dedicated to their mission to protect you,” says UC Davis Police Chief Annette Spicuzza; “But they can’t be everywhere all the time. It’s up to each of us to take steps to ensure our own safety, both on and off campus.”

Reset Perspective from Passive to Active

It’s natural for people to put routine activities on auto-pilot and overlook basic precautions. This passive attitude is just what law-breakers are looking for as they scan for criminal opportunities. They are more likely to avoid someone who is aware and on guard, protecting their space and ready to react to the unexpected. Start with a reality check. Recognize that it *can* happen to you and use your imagination to identify the potential for danger at all points of your daily activities. Take advantage of crime prevention programs and training offered by your UC police agency. Work together with your family and co-workers to sustain your proactive mindset and crime-resistant behaviors.

It Takes a Department

The whole is greater than the sum of its parts when department members work together to safeguard people, possessions and vital university resources. A group effort can generate momentum, raise awareness and make it easier to track success. Positive steps toward crime prevention in the workplace:
Contact your UC police agency regarding training and education, crime prevention presentations.

- Ask about specific coaching to improve security in your department.
- Get to know staff members from other departments in your work area so you know who is authorized to be there.
- To protect departmental resources, everyone on staff should follow the policy for file back-up and data security. Update and communicate the policy often to keep up with advances in technology.
- Train staff on how to report suspicious or threatening behavior, and how to spot the signs of potential workplace violence.
- Update and communicate contact numbers and procedures for quickly reaching your facility’s police force.
- Develop or update your department’s emergency response plan.
- Work with your campus emergency response staff to set up periodic emergency response exercises.

Continued

Safety Spotlight is a UC System-wide publication of the Environment, Health and Safety Leadership Council, UC Office of the President