Message from the CIO

Welcome back for a new school year! Recently, various media groups have covered a number of stories about risks associated with “blogging” and other personal Web space tools. These tools have become very popular among K-12 and college populations, so we are dedicating an entire IT Bulletin issue to the topic. We have outlined some best practices and guidelines, as well as an analysis of the threat. Here’s to another fall of practicing safe computing!

-Sam Segran
Associate Vice President for IT and Chief Information Officer

What are Personal Web Spaces and Blogging?

Personal Web spaces are a forum for communicating and posting ideas, photographs, videos, and other multimedia. Blogging is an online dynamic collection of one’s thoughts, opinions, selected links, and personal information. Personal Web space services are used to communicate with “real-world” friends, as well as “cyber” friends.

Social networking Web sites, such as MySpace and FaceBook, are popular with junior high, high school, and college communities. MySpace has become the Internet's second most popular blog site, as they have successfully marketed to these target groups. Users can post and exchange their information, photographs, documents, and videos. Each student can customize their site and include a wide range of personal information. These personal Web spaces have also provided information to predators, potential employers, educators, attorneys, and law enforcement officials.

Before using a personal Web space service, you should read and understand the privacy policies and feature options. Know how to protect your information by limiting the personal information you post and by using available security features from the service.

Feature Highlight: “Circle” of Friends Feature

One of the riskier features of online personal Web spaces is also the least commonly discussed feature. All personal Web spaces are equipped with a “contacts” feature that allows participants to build lists of friends. Once a list is created, then that group can access the information posted on the individual’s personal Web space. One way that people interact and create communication groups is to share contact lists, a feature typically referred to as the “Friend-of-Friend” or “Circle” feature. When individuals share these lists, it exponentially increases the number of people that you don’t know who can view your information.

The Friend-of-Friend feature creates “circles” of friends, giving users a false sense of security that they know everyone who is viewing their information. Unfortunately, a predator posting as an online student can gain access to one person’s friend list and have a large “circle” of potential victims (including circles of underage groups). A 50-year-old sexual predator could easily pose as a 12-year-old child online.

We strongly advise against granting access to your personal information to the contact lists of your online friends and acquaintances. Only those individuals that you have a personal, face-to-face relationship should be granted access to your personal Web space. The safest way to manage the distribution of your information is to disable the “Circle of Friends” feature and only post general information on your site. Remember that any concept of information privacy and security in these spaces is an illusion, not reality.

The Threat:

Personal Web space users that post and communicate personal information risk becoming victims of identity theft, stalking, or self-incrimination. In fact, some employers review personal Web spaces during the interview and employee evaluation phases. Some security risks associated with online profiles include:

- Online predators (including predators looking for underage users)
- Unintended distribution of personal user information, including pictures
- Loss of distribution control of personal information via the Friend-of-Friend feature
- Cyberbullying
- Identity theft
- Spam mail harvesters
- Stalking/harassment
- Suspect links that could lead to infection by malware
- Phishing attacks
- Exposure to incriminating photos (e.g. sexual, alcohol, drug, or other illegal behavior)
- False sense of security
- Some Web sites may not be secure (e.g. password not encrypted)
- Information can be viewed by unknown users (those with ill intentions as well as potential employers or university officials)
- Feeling of anonymity
- False identity of users with ill intentions

If a University official becomes aware of student, faculty, or staff illegal activity, they are required to take appropriate action. Information contained in a personal Web space can be viewed as evidence of illegal or inappropriate behavior. For instance, a student may jeopardize and limit career options if employers find lewd or inappropriate content on a personal Web space. Recent information from the media and education sector suggests that a student who lacks online discretion could damage their university enrollment and future career.

The Lubbock Avalanche Journal published the following Associated Press (AP) articles in the last year:

“High school teacher fighting for job after nude pictures come to light”
http://lubbockonline.com/stories/061706/tra_061706001.shtml

“Prospective employers can use search engines to look up online profiles”

“Officers suspended in MySpace case”
Recommended Practices:

Be as anonymous as possible.
Avoid postings that could enable a stranger to locate you. That includes your last name, the name of your school, sports teams, the town you live in, and where you hang out. Never, under any circumstances, post your phone number or address (including email addresses that display your full name). "Real" friends already have that information and won't need to obtain it from your blog.

Protect your information.
Check to see if your service has a "friends" list that allows you to control who can visit your profile or blog. If so, allow only people you know and trust. If you don't use privacy features, anyone can see your info, including people with ill intentions. (This could include friends or other people on your list with a grudge.)

Carefully monitor your contact list.
Be aware of who can view your personal information. The Internet allows for easy access and searching. Read about privacy and security features and utilize them.

Scrutinize third party information sharing.
Some blog services may give your personal information (including your IP address) to other advertising companies in order to pay for the free service you are receiving. You should investigate the privacy policies of any service you use to ensure you are not being placed on undesirable lists or that your personal information is being unknowingly shared.

Avoid in-person meetings.
Don't get together with someone you "meet" in a profile or blog unless you are certain of their actual identity. Although it's still not risk-free, if you do meet the person, arrange the meeting in a public place and bring some friends along.

Be aware: potential employers search.
Internet career site CollegeRecruiter.com estimates that 5 percent of employers currently research applicants on popular sites like Flickr, MySpace, Friendster, and Facebook. However, recent media coverage suggests that more employers will be searching these sites as part of candidate selection process. Employers have reported rejecting otherwise qualified applicants because of material they found online.

Think before posting photos.
What's uploaded to the net is public and can be downloaded by anyone and passed around or posted online. Avoid posting photos that allow people to identify you (street signs, license plates, school logo clothing, etc.), especially images that are sexually suggestive or display illegal activity (e.g. drinking under age, drug use, etc.). Before uploading a photo, think about how you'd feel if it were seen by a parent/grandparent, college admissions counselor, or future employer. Once it's on the Web, it is fair game.