who is watching me?

As social networking services become more popular, more people use them to gather information for malicious purposes. Here are some people who could be watching you:

Identity Thieves: Phone numbers, addresses, names and other personal information can be harvested easily from social networking sites and used for identity theft. Phishing has also become popular on social networking sites.

Cyber Stalkers and Other Predators: Are your friends interested in seeing your class schedule online? So could cyberstalkers. Knowing your schedule can make it very easy for someone to victimize you, whether they break into your home or attack you while you're out. If you're using FourSquare or Facebook places to share your location, they may be able to determine exactly where you are so they can strike.

Employers: Before you apply for a job, do a quick search for your name online. That's exactly what recruiters and employers are doing. What you post online may put you in a negative light to prospective or current employers. Always be aware of the image you project online.

KEEPING UB SECURE
Information Security Office

you're a target

If you're online, you are a target for scammers. Organized crime is increasingly targeting people on social networking sites through the use of a friend's compromised account.

Before posting anything online, ask yourself, "Would I be comfortable if this were posted on a billboard?" Never assume that what you post online will remain private. Always think about how someone might use the information you share.

stay informed

Visit the UBIT website to read the security standards, access security tools and software, or find out more ways to protect yourself.

UB INFORMATION SECURITY OFFICE
www.buffalo.edu/ubit/security
sec-office@buffalo.edu
(716) 645-7798

University at Buffalo
Information Technology

DIGITAL SELF DEFENSE:

safer social networking

Protecting Your Privacy Online

KEEPING UB SECURE
Information Security Office

introduction

It's never been easier to connect with one another online. Sites like LinkedIn, Facebook and Google+ all provide endless opportunities to meet new people, and share information and ideas.

Publishing private information on the Internet exposes you to a number of risks. This guide describes the risks you face by sharing information on these sites, and provides some tips for safe social networking and blogging.

getting started

When registering for social networks, you first create a profile that typically includes a digital photo, a description of yourself, some likes and dislikes and other personal characteristics. If you've created a public profile, anyone can search for other people with similar interests using the information you've provided.

Many popular social media sites are general social networking sites: however, some have a specific purpose. For instance, LinkedIn is a professional network. Keep the purpose of the community in mind and make a conscious descision about what information you're willing to share.

why does it matter what information I provide?

What are some of the things that you might post on blogs and social networking sites?

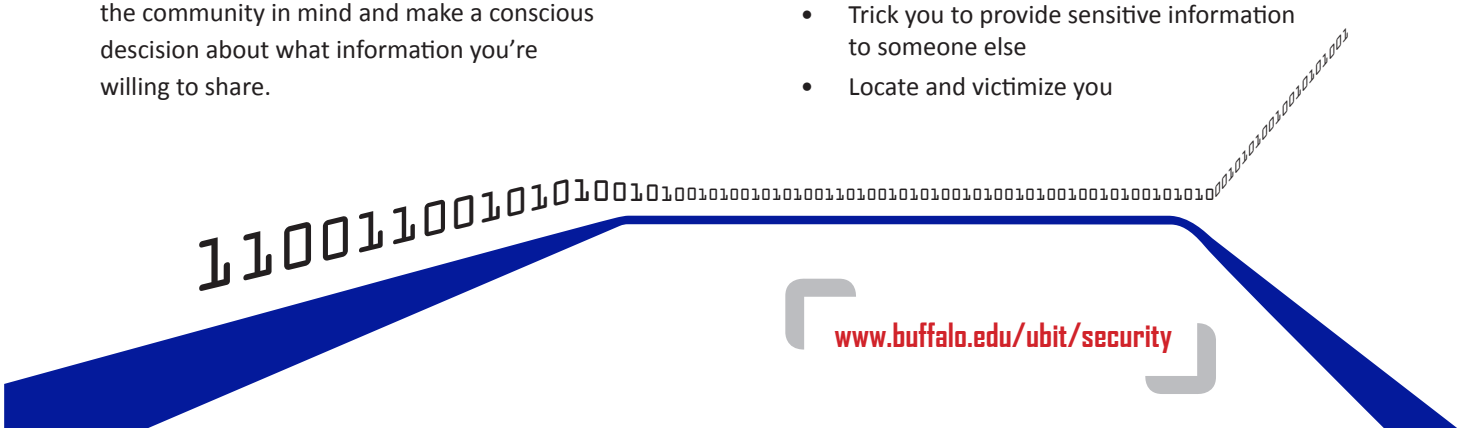
- Your class schedule for the quarter, along with your new cell phone number
- A complaint about what your boss did yesterday at work
- Information about what you or your friends are doing
- A story about how much you drank at a party last weekend
- A note detailing your upcoming vacation

Who would want to see any of those things, except the people you know, right?

Although it may seem harmless, the information you post in public space can be used in many ways you might not expect.

The information you post online can be used to:

- Monitor what you do and where you go
- Impersonate you to gain access to your financial information
- Trick you to provide sensitive information to someone else
- Locate and victimize you



www.buffalo.edu/ubit/security

protecting your information

Keeping your information out of the wrong hands can be fairly easy. Here are some tips to make sure your private information stays private:

- The simplest way to keep your information private is to not post any private or personal information online. Avoid posting anything that isn't required, especially information that could be used in identity theft. Don't hesitate to ask friends to remove embarrassing or sensitive information about you from their pages.

- Restrict who has access to what you post online. Set your account so that only people you've chosen can see what you've posted by creating a private profile. Use this feature in conjunction with other privacy settings.

- Disable unused features and applications. Many of these websites come loaded with extra features and applications to enhance the experience. Your best bet is to disable everything and re-enable only the features you plan on using.

- Choose your friends carefully. Most sites do not verify a person's identity at registration, so always be cautious when dealing with unfamiliar people.