

## Identity Theft

Identity theft is a rapidly growing threat, and it thrives on poor security practices. Your best defense is to build good security habits and encourage everyone you know to do the same. If you believe you may be the victim of identity theft, contact your local community law enforcement to file a report.

*"Identity theft is a serious crime. It occurs when your personal information (name, Social Security number, date of birth, credit card number, or bank account number) is stolen and used without your knowledge to commit fraud or other crimes. Identity theft can cost you time and money. It can destroy your credit and ruin your good name."*— Federal Trade Commission

## Using a public computer

You should think twice about entering your UserID and password on any unfamiliar computer. What assurance do you have that it is protected by good security practices? A public computer, such as a kiosk in a hotel lobby, is particularly dangerous. It might be operated by an unscrupulous business that deliberately installs malicious software to steal valuable personal information. If you must enter your UserID and password on a computer that might not be secure, change it the next time you are on a trusted computer.

## Using your SBU Credentials for a non-SBU account

Using your SBU UserID and password for other services, such as online banking, shopping, or even discussion forums, increases the chances that it may be stolen, because these services may not transmit the password securely. If you have no choice, because the web site automatically uses your email address for the account name, be extra careful to choose a password that has no similarity to your SBU password.



# Information & Technology Services

## Tips to safeguard your privacy and keep confidential information secure.

Protect personal information. The identity saved could be your own.

Your Novell and WebAdvisor UserID and password is your online identity at SBU. It provides access to your personal information and is the key to using a variety of campus services.

For many of us, it also provides access to other people's university data. Part of being a good network citizen is protecting other people's data. Keeping your UserIDs and passwords safe is one way you can help protect everyone's data on campus.

If someone steals your UserID and password, they can use your information to:

- Send out spam using the SBU mail system, usually via WebMail.
- Gain access to any services that you access using your UserID and password.

Since your UserID and password grants access to your personal university information, when it's stolen you are also at risk of identity theft.



SAFEGUARD YOUR PRIVACY AND KEEP CONFIDENTIAL INFORMATION SECURE  
Protect personal information. The identity saved could be your own.  
[www.SBUniv.edu/ITS/CyberSecurityAwareness/](http://www.SBUniv.edu/ITS/CyberSecurityAwareness/)

## Market Research

Companies whose business is to understand the needs and wants of consumers use a variety of market research techniques to do so. Your privacy can be at risk when you participate in surveys, online communities, focus groups, and other types of market research. To participate, you typically enter into an explicit agreement with a research firm, sometimes in exchange for some sort of reward. Reputable market research firms will be upfront about exactly what information they will gather and what they will do with it, and will provide you with a privacy statement.

For some types of market research, the firm needs special software to be installed on your computer to better track your activities. Do not install such software on an SBU computer.

If you are considering participating in this kind of research using a computer you personally own, ask yourself if you really want to give the market research firm and its customers potential access to everything you do on your computer. You may be surrendering control over your computer and may not have any way of knowing what information the research firm is gathering about you.

Be particularly wary of a questionable practice used by some market research firms in which they ask you to install software that may appear fairly harmless, and use the end-user license agreement (EULA)—the lengthy legal statement that you agree to before you can install the software—as the method for informing you about their actual intentions.

If you read the fine print in the EULA, you will probably find that it grants fairly broad access to your computer and your activities. You might also be surprised at the latitude in what can be done with the information collected. Because of this practice, people often refer to market research software as “spyware.”

## How to Create a Strong Password

Make all of your passwords as long and complex as feasible. Your passwords should be easy for you to remember, and difficult for other people to guess.

When creating a password:

Use at least 8 characters, including at least three of the following four character types:

- Uppercase letters
- Lowercase letters
- Numbers
- Symbols found on your keyboard, such as blank spaces, or ! \* - ( ) : | / ?

Do not include:

- Personal information, such as your UserID, names or nicknames of people, pets, or places, or your address, birthday, or hobbies
- Repeated characters, such as AAA or 555
- Alphabetic sequences, such as abc or CBA
- Numeric sequences, such as 123 or 321
- Common keyboard sequences, such as *qwerty* or *password*
- Simple substitutions such as zero for the letter o.

“I have students who need access to my computer so I give them my UserID and password so they can work in my absence.”

Sharing your UserID and password is a violation of university policy. Remember that your UserID and password protects your email as well as many university resources. As an SBU employee, you are responsible for any action taken by a student while logged with your credentials.

If you have a need to share emails with others, speak with the network administrator about a shared email address.