



### Cyber Ethics

---

---

#### What is Cyber Ethics?

Cyber ethics refers to the code of responsible behavior on the Internet. Just as we are taught to act responsibly in everyday life, with lessons such as “Don’t take what doesn’t belong to you,” and “Do not harm others,” -- we must act responsibly in the cyber world as well.

---

#### What are Responsible Behaviors on the Internet?

Responsible behavior on the Internet in many ways aligns with acceptable behavior in everyday life, but the consequences can be significantly different. For example, verbal gossiping is generally limited to the immediate audience (those within earshot) and may well be forgotten the next day. However, gossiping on the Internet can reach a far wider audience. The “words” are not forgotten the next day, but may live on the Internet for days, months or years and cause tremendous harm.

Some people try to hide behind a false sense of anonymity on the Internet, believing that it does not matter if they behave badly online because no one knows who they are or how to identify them. That is not always true. Computers, browsers, and Internet service providers may keep logs of their activities which can be used to identify illegal or inappropriate behavior.

The basic rule is do not do something in cyber space that you would consider wrong or illegal in everyday life.

When determining responsible behaviors, consider the following:

- Do not use rude or offensive language.
- Don’t be a bully on the Internet. Do not call people names, lie about them, send embarrassing pictures of them, or do anything else to try to hurt them.
- Do not copy information from the Internet and claim it as yours. That is called plagiarism.
- Adhere to copyright restrictions when downloading material including software, games, movies, or music from the Internet.
- Do not break into someone else’s computer.
- Do not use someone else’s password.
- Do not attempt to infect, or in any way, try to make someone else’s computer unusable.

We were taught the rules of “right and wrong” growing up. We just need to apply the same rules to cyber space.



## *Using Instant Messaging and Chat Rooms Safely*

Cyber Security Tip produced by US-Cert

**Instant messaging (IM)** - Commonly used for recreation, instant messaging is also becoming more widely used within corporations for communication between employees. IM, regardless of the specific software you choose, provides an interface for individuals to communicate one-on-one.

**Chat rooms** - Whether public or private, chat rooms are forums for particular groups of people to interact. Many chat rooms are based upon a shared characteristic; for example, there are chat rooms for people of particular age groups or interests. Although most IM clients support "chats" among multiple users, IM is traditionally one-to-one while chats are traditionally many-to-many.

**Bots** - A "chat robot," or "bot," is software that can interact with users through chat mechanisms, whether in IM or chat rooms. In some cases, users may be able to obtain current weather reports, stock status, or movie listings. In these instances, users are often aware that they are not interacting with an actual human. However, some users may be fooled by more sophisticated bots into thinking the responses they are receiving are from another person.

How can you use these tools safely?

- Evaluate your security settings - Check the default settings in your software and adjust them if they are too permissive. Make sure to disable automatic downloads. Some chat software offers the ability to limit interactions to only certain users, and you may want to take advantage of these restrictions.
- Be conscious of what information you reveal - Be wary of revealing personal information unless you know who you are really talking to. You should also be careful about discussing anything you or your employer might consider sensitive business information over public IM or chat services (even if you are talking to someone you know in a one-to-one conversation).
- Try to verify the identity of the person you are talking to, if it matters - In some forums and situations, the identity of the "person" you are talking to may not matter. However, if you need to have a degree of trust in that person, either because you are sharing certain types of information or being asked to take some action like following a link or running a program, make sure the "person" you are talking to is actually that person.
- Don't believe everything you read - The information or advice you receive in a chat room or by IM may be false or, worse, malicious. Try to verify the information or instructions from outside sources before taking any action.

*reproduced with permission*

## *LAST WORDS*

The free online security awareness site (<https://www.act-online.net>) offers a course on Cyber Ethics. Please take time to register and begin the security awareness training. For those completing the training, please forward a copy of the certificate to Human Resources so your personnel file will be updated.



Please use the following information when creating an account:

Training Coordinator Name: **SFASU ITSecurity**

Training Coordinator E-mail: **itsecurity@sfasu.edu**

Training Coordinator Code: **002151**

Company/Agency/Organization: **SFASU-Dept/College Name**

Many members of the SFA Community are creating a presence in social networking sites. The University currently does not have a policy on social media. In the meantime, the [University Web Site policy \(D-45\)](#) should be reviewed prior to creating an offsite presence since the content is not stored on University-owned web servers. Do not neglect your department's SFASU.EDU webpage in favor of social media sites.

Powered by:

Brought to you by:

