You’ve probably learned a long list of important safety and privacy lessons already: Look both ways before crossing the street; buckle up; hide your diary where your nosy brother can’t find it; don’t talk to strangers.

The Federal Trade Commission, the nation’s consumer protection agency, is urging everyone to add one more lesson to the list: Don’t post information about yourself online that you don’t want the whole world to know.

The Internet is the world’s biggest information exchange: many more people could see your information than you intend, including your parents, your teachers, your employer, the police and strangers, some of whom could be dangerous. Social networking sites have added a new factor to the “friends of friends” equation. By providing information about yourself and using blogs, chat rooms, email, or instant messaging, you can communicate within a limited community or with the world at large. But while the sites can increase your circle of friends, they also can increase your exposure to people who have less-than-friendly intentions. You’ve heard the stories about people who were stalked by someone they met online, had their identity stolen, or had their computer hacked. The FTC suggests these tips for socializing safely online:

• Think about how different sites work before deciding to join a site. Some sites will allow only a defined community of users to access posted content; others allow anyone and everyone to view postings. Think about keeping some control over the information you post.

• Consider restricting access to your page to a select group of people, for example, your friends from school, your club, your team, your community groups, or your family.

• Keep your information to yourself. Don’t post your full name, Social Security number, address, phone number, or bank and credit card account numbers and don’t post other people’s information, either. Be cautious about posting information that could be used to identify you or locate you offline. This could include the name of your school, sports team, clubs, and where you work or hang out.

• Make sure your screen name doesn’t say too much about you. Don’t use your name, your age, or your hometown. Even if you think your screen name makes you anonymous, it doesn’t take a genius to combine clues to figure out who you are and where you can be found.

• Post only information that you are comfortable with others seeing and knowing about you. Many people can see your page, including your parents, your teachers, the police, or the job you might want to apply for in the next couple of years. Remember that once you post information online, you can’t take it back. Even if you delete the information from a site, older versions exist on other people’s computers.

• Consider not posting your photo. It can be altered and broadcast in ways you may not be happy about. If you do post one, ask yourself whether it’s one your mom would display in the living room. Flirting with strangers online could have serious consequences. Because some people lie about who they really are, you never really know who you’re dealing with. Be wary if a new online friend wants to meet you in person. Before you decide to meet someone, do your research: Ask whether any of your friends know the person, and see what background you can dig up through online search engines.

• If you decide to meet them, be smart about it: Meet in a public place, during the day, with friends you trust. Tell a friend, parent or other responsible adult where you’re going, and when you expect to be back.

If you feel threatened by someone or uncomfortable because of something online, report it to the police and the social networking site. You could end up preventing someone else from becoming a victim. Find out more about cyber security and tips for securing your information on social networking sites at:
http://www.us-cert.gov
Each year, hundreds of students and parents fall victim to scams involving college loans.

- **Do your research.** Before handing over a check or credit card, check out the company. Does it have a website? A working phone number? When you call to ask questions, do you get answers? A Web search on the company's name can also turn up complaints others have made about it, although some scam artists change company names frequently.

- **Use a credit card.** If you are going to buy the services of a company, pay with your credit card. Many cards offer protection for fraudulent activity, so if the company turns out to be a fraud, the credit card company may reimburse your purchase. (Most card companies put limits on how long customers have to report such activity.)

- **Don’t "pay" for money.** If a check for a grant delivered in the mail costs money to cash, it is most likely a scam. In fact, many unsolicited checks that arrive in the mail are scams—be wary of them.

- **Beware common pickup lines.** “This scholarship is guaranteed or your money back,” “You can’t get this information anywhere else,” and "We’ll do all the work," are a few of the lines the Federal Trade Commission warns against.

- **Rely on trusted sources.** College financial aid offices are paid to help students and parents with the loan process make use of them. If you need extra help, ask them for suggestions.

---

**Tips on Avoiding College Loan Scams**

As electronics become more sophisticated and expensive, the possibility of your electronic device being stolen or snatched has increased. According to the NYPD, the growing trend in NYC and in major cities is snatching of electronic devices from person(s) not paying attention to their surrounding while on the streets, subways or buses. Here are some tips to keep in mind:

- **Keep electronic devices out of sight** while walking on the streets, or in public transportation. The idea is to eliminate the temptation of having these items stolen.

- **Change earpieces to another color;** the white headsets are a dead giveaway that they are attached to an I-pod, and attract unwanted attention.

- **If you’re using your cell phone in plain view, talk in a secure location.** Be AWARE of your surroundings. If you are in danger, feel threatened or being followed, look for an open store, a doorman building or a security booth where you can call the Police (911).

---

**Be Street Smart While Using Electronics**

- The vast majority of crime on a college campus or any institution can be prevented with minimal effort. Removing the opportunity to commit an easy theft will usually prevent the theft from ever occurring. According to the Institute of Campus Crime Prevention Programs, theft of unattended property is the number one reported incident on college campuses. A brief trip to the bathroom, lab, room next door or to get quick cup of coffee, a quick jog in the gym, can result in your property being taken.

- Take an active role in helping us take a “Bite Out of Crime.” Secure your office, lab or dorm room when not in use. Secure all pocket books, hand bags, wallets, small electronics including laptops in a secured file cabinet or locker. Use wallet & property lockers at the gym while working out. While at the library, in a classroom, etc. ask a friend to keep an eye on your property while you step away, and you do the same for them.

If you see suspicious activity, notice something out of place, or observe a crime in progress, call Public Safety Right-Away: 212-854-5555 @Morningside Campus or 212-305-7979 at the Medical Center Campus.

Enroll in CU Public Safety’s Operation ID (property engraved with a Unique ID Number) & NYPD Blue Light (same as Operation ID except invisible ink used) programs. Both programs are FREE and EFFECTIVE. For more information please call CU Crime Prevention 212-854-8513.