

DON'T POST OR SEND ANYTHING YOU WOULD BE EMBARRASSED FOR OTHERS TO SEE

Think about what your family, friends, future employers, or college admission decision-makers might think if they see it. How would you feel if that statement or picture was forever tied to your name and your identity? Does it really represent who you are? Remember, your keyboard may have a "delete" button, but once online it is often impossible to remove. Even if something is sent with the intention of privacy, they rarely remain that way.

DON'T COMPROMISE YOUR IDENTITY

Identity thieves are constantly looking for new ways to obtain your personal information, usually for the purpose of benefiting financially at your expense. Never post your address, date of birth, phone number, or other personal contact information anywhere on social media. Even with restrictions, access can be gained through fraudulent means such as by phishing, hacking, or malware.

DO BE CONSIDERATE OF OTHERS WHEN POSTING AND INTERACTING

If you message someone and they do not respond, or if someone messages you and asks that you not post about them, please respect their requests. Also don't post pictures of others without their permission. And if someone asks you to remove a picture, post, or to untag them, do so immediately. It's what you would want if you asked someone the same thing.

DON'T HANG OUT WITH THE WRONG CROWD ONLINE

Resist accepting every friend and follower request that comes your way. Giving strangers access to your personal information opens you up to all sorts of potential problems. Be selective with who you allow to enter into your world! Go through your friends and followers lists regularly, deleting those you do not fully know or trust.

DO PROPERLY SET UP THE PRIVACY SETTINGS AND PREFERENCES WITHIN THE SOCIAL MEDIA APPS, SITES, AND SOFTWARE YOU USE

Do not feel obligated to respond to messages and friend/follower requests that are annoying or unwanted. Use the privacy settings available to allow access to only those you trust. Turn off location-sharing, and the ability to check-in to places. If you need to let your friends know where you are, just text them using your phone rather than sharing it with your entire social network.

DO SECURE YOUR PROFILE

Use complex passwords that consist of alphanumeric and special characters. Avoid using recovery questions which have easy-to-guess or common answers. Never reveal your passwords to friends or family, or leave them written down somewhere. Avoid accessing your online profile from devices which are unsecure (like at a library computer).

DON'T TELL THE WORLD WHERE YOU ARE AT ALL TIMES

Criminals use social media to target victims by reading posts that clue them in as to where you are (and when you're not at home). Checking in while on vacation or posting an update such as "At the beach for the day" may be a fun way of letting your friends know what you are up to, but it also lets those with bad intentions know when your home is empty and vulnerable.

DO REGULARLY SEARCH FOR YOURSELF ONLINE, JUST TO SEE WHAT IS OUT THERE

Start with Google, but also use site-specific search engines on social networking sites, as well as sites that index personal information about Internet users. Some examples are: peekyou.com, zabasearch.com, pipl.com, yoname.com, and spokeo.com. If you do find personal information about yourself, investigate how you can have it deleted. Many sites provide some type of "opt-out" form which allows you to request its removal.

DO BE CAREFUL ABOUT OVERSHARING

Posting something as simple as a picture of you wearing your school apparel can give a person access to numerous other areas of your life. For example, that person likely knows where you now go to school, potentially what afterschool programs you are involved in, and your daily schedule built around those programs. Seemingly innocent posts may contain information that will allow an individual to learn much more about you.

DO NOT MEET ONLINE STRANGERS IN PERSON

It is unwise and potentially very dangerous to meet individuals in person that you only know from online interactions. However, if you choose to do so, do so smartly. For example, always let someone else know where you are going and who you are meeting. Additionally, always meet in a public place you are familiar with and never drive with or leave with the individual. Lastly, maintain communication during the interaction with a trusted adult.