

Be Cyber Safe (and Smart)

Think twice — or maybe even three times — before you post that.

Josh is 16 and just starting to think about college. He hopes to get a job this year to add to his college fund. When Josh met with his high school guidance counselor to talk about classes he'd need for college, he was amazed to hear that the first thing he should do is take a look at his Facebook account.

"Hiring personnel and colleges are now taking a look at social networking sites," his guidance counselor told him. "They want to see what kinds of things are posted about the person they might hire or might admit to their school." In fact, estimates are that approximately one-fourth of colleges look at potential students' Facebook profiles.

When Josh did a search on himself by typing his own name into a search engine, he was shocked to see what he found. One of his Facebook friends had posted a picture of Josh on his own page — a picture Josh had never seen — that showed him acting silly at a party and making strange faces. Anyone looking at it could think that Josh had been drinking.

And on his own FB page, Josh had some bad language that he didn't

want college recruiters seeing. On YouTube, there was a video of Josh and some kids pulling a stupid prank on their town square that was illegal.

KEEPING CLEAN

Here are some pointers for keeping your online presence clean:

REMEMBER THAT NOTHING REALLY EVER GOES AWAY. Think twice (or three times) about what you post (and what you do that might get posted). "Even 10 years later, it's still floating around out there," says Michael Ferjak, senior criminal investigator for the Iowa Internet Crimes Against Children Task Force in Des Moines, Iowa. "It doesn't matter whether it's Facebook, Snapchat, Instagram, Twitter or anything else — it's still a matter of keeping your head in the game when you're online."

CONTINUED>>>

For lots of cybersafety tips, visit boyslife.org/links/nsteens



ISTOCK BY GETTY IMAGES (3)

THINK ABOUT HOW MANY “FRIENDS” YOU NEED. Every time you add a friend on a social network site, you’re giving him or her access to all your private info.

“Do you really need 750 friends?” Ferjak asks. “You may keep your page clean, but your friends could be posting things about you on their pages.”

REALIZE THAT IT’S NOT PRIVATE. A lot of people think that only their friends and family can see their page, but that isn’t true. Check your privacy settings, know that your friends can copy and repost what is on your page to other places, and don’t share your passwords or give friends access to your accounts.

STAYING SAFE

It’s important to be smart online — and it’s also important to be safe.

Even if you’re careful not to post photos that show where you go to school or what town you live in, stalkers and predators can pick up that information using EXIF (exchangeable image file) data.

What’s EXIF data? Details that can be revealed through bits of information embedded in images taken with smartphones and some digital cameras and then shared on public websites. This data often includes the times, dates and geographical coordinates (latitude and longitude) where images are taken.

When photos using that kind of data are posted, they can tell a lot about a person’s daily activities. Once this info is posted online, you lose control of it. How much do you really want to share?

If you’re posting photos from a mobile phone, the Federal Bureau of Investigation suggests checking the “options” or “settings” on your phone (and any apps you’ve downloaded) to see if they are sharing location information. For many phones, sharing the information is the default setting, and you’ll have to change that if you don’t want your info shared.

For many phones, you’ll have to go to Settings > General > Location Services and then check “Do not share” or something similar. Also,

when taking photos, videos or selfies, make sure your background and appearance aren’t giving you away. Street signs, store names, T-shirts with school names on them — they can all give away details about who and where you are.

BEING NICE

You’re being smart and safe online — also make sure that you’re being nice. Cyberbullying is not only unkind, it can also be illegal.

How do you deal with it? Here are some tips from www.connectsafely.org:

If You’re the Cyberbully

GET OUT OF A GROUP MENTALITY. Sometimes people do things in a group that

**“SEXTING”
IS SENDING PICTURES OR
MESSAGES THAT HAVE SEXUAL
CONTENT IN THEM.**

Many teen guys who have sent or posted sexual content say they have sent it to a girlfriend. But most don’t know about the consequences for this behavior.

Sexting can be classified as child pornography, even if both the sender and receiver are under 18.

“If it ends up being saved, that can be considered possession, and that’s a felony in almost every state,” Ferjak says.

And Snapchat isn’t foolproof. You might think because a photo lasts only a few seconds it can’t cause problems. But someone might take a picture with a phone of the photo, and then there’s a permanent record of it that can be forwarded to other people. Your image could be passed around without your permission, and you could be bullied or judged by friends and classmates.

XXX

they wouldn’t do alone. Look at your group of friends. Are your friends bullying someone? Are you part of that? Can you help stop it?

PUT YOURSELF IN THE OTHER PERSON’S SHOES. How would you feel if this were being said about you or done to you?

REALIZE THERE ARE CONSEQUENCES.

Nothing is anonymous. Things can be tracked back to you. Almost every state has civil laws for cyberbullying, which means you and your family can be sued if you’re the bully — sometimes for large amounts of money.

If You’re Being Cyberbullied

DON’T RESPOND. Usually the bully is trying to get a reaction from you. If you don’t respond, he or she will move on. Although it’s hard to do, experts say to leave your online world for a while. Don’t log onto websites or blogs that are talking about you. Turn off your cellphone. Check your privacy settings and block the bully.

USE THE REPORTING TOOLS. Often sites have a place to report abuse. If you forward to them what you’re receiving, they might shut down the bully’s posts.

PRESERVE THE EVIDENCE. Don’t delete what you’ve received until an adult has decided what to do with it.

DON’T RETALIATE. It’s hard not to fight back, but it’s better not to make it worse and start a new cycle of bullying.

TALK TO A TRUSTED ADULT. Afraid to talk to someone about this because you’ll seem weak or you think your parents will take your computer away? Do it anyway. Sometimes just talking it out can help, and they’re more likely to trust you if you’re honest about your online life.

ASK YOUR SCHOOL TO EDUCATE. They can find teaching resources for all ages at www.NetSmartz.org. Also, many highway patrol or state cybercrime offices provide educational programs for students and their parents.

BE A FRIEND. Often someone who is being bullied can’t think clearly enough to report it. Be a friend and report it for them. ✦

If you’re being cyberbullied, don’t respond.

CYBER CHIP
Earn the BSA’s Cyber Chip, which shows you understand and agree to certain rules of cybersafety. Get the details at boyslife.org or from your unit leader, local council or Scout shop.

