Protect Your Privacy Online

By Kathiann M. Kowalski

Keep personal information private—for your own good!

High school sophomore Karra H. never expected to see herself on a Web site featuring scantily clad teens. Yet there she was, wearing a bikini while holding a suggestive cheerleading pose.

The site's anonymous owner got most of the photos from teens' social media pages. While Nancy McBride at the National Center for Missing & Exploited Children feels the actions of the site's creator were wrong, she warns teens against posting revealing images in the first place. "Once it's out there, it's out there forever," says McBride. "Somebody else can go out there and grab it." In other words, protecting privacy starts with you.

Watch Out for Strangers—And 'Friends'

In Karra's case, the unknown Web site operator didn't contact Karra or use online information to track her down in real life. Strangers rarely physically assault teens they find or connect with online, but it has happened.

Jochen Luebke/Newscom

When some female friends told 17-year-old Eric M. in Utah that they had chatted online with unknown adults, he urged them to stop. "There are child molesters, and there are a lot of crazies out on the Internet," says Eric. "If you don't know someone, don't talk to them."

More often, teens hurt one another—or themselves. Cyberbullying can be both nasty and illegal. One 19-year-old New Jersey college student faced

criminal charges after he tweeted about watching a roommate's romantic date via Webcam. Other teens use cell phone cameras and social media sites to share photos of their own private moments or illegal activities, such as underage drinking. Even if charges don't result, embarrassment can follow.

"One of the biggest mistakes that teens make is believing that the information that they post is private and just amongst their friends," explains Michelle Boykins at the National Crime Prevention Council. Anyone can copy and resend material. There's even less control over "friends of friends."

Identity Theft Happens

Teens are also targets for identity theft—the use of someone's personal information for fraud or crime. Last year about 8 percent of reported identity theft cases in the U.S. involved teen victims, says attorney Steven Toporoff at the Federal Trade Commission. That's roughly 18,000 cases. Adults in their 20s make up the biggest group of victims.

"Neglecting potential identity theft could really come back to bite you," stresses Toporoff. Many teens discover identity theft only later, when they apply for college loans or auto loans. By then, cleaning up credit reports can take hundreds of hours. Meanwhile, lenders delay extending credit.

"Facebook has become a gold mine and a giveaway for identity thieves," notes Neal O'Farrell at the Identity Theft Council in California. Some users post their full dates of birth, addresses, or phone numbers. Others disclose their places of birth, pet's names, favorite bands, or similar information. That data can help criminals recover someone's password for various accounts. "Identity thieves now have very sophisticated programs that scrape these pages of this information, join the dots, and then clone the identity," says O'Farrell.

Even teens who don't give away information can be vulnerable. Earlier this year, for example, criminals broke into servers for the Sony and Sega corporations, two leading game makers. The security breaches revealed data about millions of people.

Other criminals develop false identities with teens' and young children's Social Security numbers. When one study reviewed a database with information about 42,000 people age 18 and younger, 10 percent of those kids' Social Security numbers had already been used for loans or to open credit accounts. In most of those cases, some sort of identity theft had happened.

"Run a credit check on yourself," suggests O'Farrell. (The government requires the three companies that control individuals' credit information in the United States to provide you with a free report once a year.) If you don't have a credit card or loan yet, finding a report on yourself could signal a problem.

Review your social media page too. Delete anything that could help strangers impersonate or find you. "Unless it's someone I know, I don't freely give out any contact information," says 16-year-old Matt K. in New York. It's just as important that you remove anything that's inappropriate.

"You can't get away with any behavior you want online," stresses McBride. Don't post anything you wouldn't want parents, colleges, or potential employers to see. After all, says McBride, "this is a public forum."

Take These Steps Now

- Don't strike up online relationships or give your contact info to strangers.
- Never meet someone offline without a parent.
- Disable location tagging on your phone's settings for photos and messages.
- Trim your social media profile to the basics.
- Delete phone info from social media profiles. Review your security settings regularly because sites sometimes change their defaults.
- Change passwords every 90 to 120 days. And use different passwords for different devices and sites.
- When you get credit or debit cards, review statements and report inconsistencies right away.
- Use secure web sites for any online purchases.
- Even if you don't have a credit card, check to see whether you have a credit report at www.annual creditreport.com. (Beware of similar-sounding sites selling products.) Correct any problems.
- Above all, use good judgment. Keep your private life private.

Don’t Let Geotagging Target You

Maurizio Gambarini/Newscom

Many mobile devices now include geotagging. The technology embeds specific location information into uploaded images or other material. For instance, if you have photos online showing the location of your home and then you make it known online that you’re on vacation and your home is empty, thieves could take advantage. To keep your mobile phone photos from telling where you are, disable the feature in the device’s settings.

Name: _____ Date: _____

1. What percentage of reported identity theft cases in the United States involve teen victims?

A 18,000
B 8%
C 18%
D 10%

2. The author tries to persuade readers that protecting your privacy online is important. Which persuasive writing tactics does the author use to make his case?

A statistics and facts
B personal anecdotes
C direct quotations from experts in the field
D all of the above

3. Which word would the author most likely use to describe the approach someone should take when posting information online?

A nervous
B bold
C cautious
D carefree

4. Read the following sentence: "'Neglecting potential identity theft could really come back to bite you,' stresses Toporoff."

In this sentence the word **stresses** means

A worries
B emphasizes
C strains
D says

5. What would another good title be for this passage?

A Going Online? Beware of Thieves and Bullies
B Proper Etiquette for Facebook Usage
C Cyberbullying: Trends, Problems, and Solutions
D The Downsides and Challenges of the Internet

6. What is one example of how teens use the internet and social media for cyberbullying?

_____

_____

_____

7. What information could an identity thief take from a kid's Facebook page today that would still be useful to the thief twenty years from now?

_____

_____

_____

8. The question below is an incomplete sentence. Choose the word that best completes the sentence.

The author suggests you "trim your social media profile to the basics" _____ identity thieves can't steal your identity.

A because
B but
C whenever
D so

9. Answer the following questions based on the sentence below.

Geotagging can target you, wherever you are, when you upload photos or information to your mobile device.

What? <u>geotagging</u>

What? _____

When? _____

Where? _____

10. Read the vocabulary word and definition below and complete questions 10a, 10b, and 11.

Vocabulary Word: vulnerable (vul · ner · a · ble): susceptible of being hurt, emotionally or physically.

10a. Read the sentences below and underline the word **vulnerable**.

1. The elderly are particularly vulnerable to breaking a bone if they fall.
2. The plants are vulnerable to frost and can die because of the cold, so she brought them inside during the months from November to March to protect them.
3. If you post a lot of personal information online, you are making yourself more vulnerable to having your identity stolen.
4. He made himself vulnerable to his friends by sharing a lot of personal stories and sharing his emotions with them.
5. When the guard decided to take a nap when he was supposed to be guarding the castle, the fort was vulnerable to attack.

10b. Which object(s) would you use to make sure your belongings were not vulnerable to theft?

11. How can you make yourself less vulnerable to someone stealing your identity?

_____

_____

_____

_____