ICT CyberSecurity Essentials

Lesson 1: Protecting Your Identity

LESSON SKILLS

After completing this lesson, you will be able to:

- Define "privacy," and relate it to the term "digital footprint."
- Explain the risks associated with giving out personal information.
- Describe the possible consequences of posting personal messages online.
- Suggest ways in which people can behave positively in cyberspace.

KEY TERMS

blocking	online profile	risk
digital footprint	privacy	social network
dossier	privacy settings	stranger
online predators		

Points to Ponder

These Points to Ponder are designed to help you focus on key elements in this lesson. They are also suitable for use to spark discussions or individual research.

- Define the term "privacy," and "Internet privacy."
- List all of the information you are required to share when opening an online account such as Facebook. This includes your first and last name, a cell number or e-mail, and your birthday, so Facebook knows you are 13 or older.
    - Now consider the information you can share on their Facebook profile—there's a lot of it!
- Define the term “Digital footprint.”
    - Think about this: "Suppose you lost your mobile device today and it had no password protection. What information on your device would you be most worried about?" Please think about account any passwords that are saved in your apps, especially ones that link to social media or financial information, e.g. Google Play Store or in-app purchases.
- Define dossier.
    - How aware are you of the tracks you leave behind? View the video "Digital Dossier" (Adobe Flash video, 4 mins). This video is an excellent explanation of the digital footprint.
- Create a T-chart with the headings "Personal Information" and "Never Post Online."
    - Identify the types of information that you would consider to be personal. List examples of information that you should never post online.

Overview

This lesson brings awareness to you about online privacy and ways to be responsible digital citizens. It focuses on the risks involved with social networking and ways to protect personal identity. You will examine the possible dangers of posting personal information on the Internet. You will also learn ways to identify risky situations and ways to guard their privacy.

Note: *Content in this lesson was developed mainly for middle school students. Some people may consider it inappropriate or too intense for elementary school students. We recommend that elementary and middle school teachers who want to integrate this topic into their instruction should preview in advance all online resources cited in the lesson, and should exercise their judgment in determining the suitability of this content for the students in their classes.*

Protect Your Identity and Your Privacy

Objectives

5.1.1: Describe risks associated with social networking sites (e.g., Facebook, Myspace, Twitter), and identify ways to reduce these risks.

5.1.2: Define "privacy," and relate it to the term "digital footprint."

5.1.3: Practice cybersafety techniques to protect your personal information when using Internet searches, e-mail, chat rooms and social network Web sites.

While the Internet offers you a wide variety of opportunities, it also has its **risks**. These risks can be anything from cyberbullying to actual physical harm, if the wrong people get your information.

Privacy

What are the things you like to do online? You may believe you are totally anonymous when playing games, watching YouTube, reading books on your e-reader, etc. **Privacy**, according to Dictionary.com is, "the state of being free from unwanted or undue intrusion or disturbance in one's private life or affairs; freedom to be let alone: Tourists must respect the tribe's privacy" (Dictionary.com, 2016). How does this apply to you? How does the meaning change between the real world and the online world? How much privacy do you have online when doing each of the things you mention?

Privacy is affected when someone knows your name or address. What if someone reads your e-mail? What if someone follows you around all day? These examples represent a loss of privacy. People online, often **strangers**, may try to obtain information about you.

Link to Learn More

- Girls – Think U Know - YouTube video, 3 mins

You can accidentally open yourself up to danger without meaning to; giving out personal information is often done in dribs and drabs, and there are people who will add up the little things to be able to figure out where you are and how to find you. For example, imagine you're in a chat room and there's someone there who's pretending to be a kid but is really an **online predator**: someone who intentionally targets people for harm using online chat rooms or social media. You're smart and you don't give out your phone

number, your school, or even your last name: you think you're being really careful. But you mention that you play soccer for a county team, and you tell them which county you're in. No biggie, right? There are tons of people in the county. You post a picture of yourself in your jersey—again, no biggie, because they don't know your name and finding one person in a whole county can't be easy. But now the predator knows your team name and colors, and which county you're in. All he has to do is look up the team Web site and find out which team is yours and when they're playing, then show up at a game. Bingo. He's found you, from a picture and the name of your county alone, and only has to follow your parents' car home after the game to know where you live. Always, always assume that any stranger on the Internet has bad intentions and will cause harm if given the chance; that may not be the case, but just as you don't trust random strangers in public with your home address or a key to your house, don't trust random strangers online with information that can provide a key to your privacy. On social media, such as Facebook, you're safest to lock your account down so that only people on your friends list can see what you post and be very, very picky whom you friend.

Link to Learn More

- Digital Dossier (Adobe Flash video, 4 mins).
- Social Smarts (Graphic Novel, PDF)

Digital Footprint

Your **digital footprint** means that when you update your status, check-in to a location or post a photo, these things are being saved and tracked, both by the companies that provide the services and, probably, by your browser in files called "cookies". That's how browsers remember your favorites and your previous searches, and can fill in fields for you. Ask yourself which breaches of privacy would worry you. Which information do you not mind sharing with the world? What kind of information needs to be kept secret?

A **dossier** is a detailed report, usually about a person. A digital footprint is like a dossier: everything you do online, everything you post, everything you share, is saved somewhere on a server and can, theoretically or in truth, be accessed, even years later. Colleges and potential employers look at your social media footprint when they're considering whether to you admit you. That stupid picture of yourself when you were fifteen holding your dad's can of beer can be used against you five, ten, fifteen or more years later.

- What are some Web sites where you might go? What kind of footprint would you leave there? (i.e., if someone at a college admissions office or your potential boss saw it, what would they think?)
- What kind of things do you post? They don't go away. Even the stuff you send on Snapchat is saved on their servers and can be retrieved.

Top Tips for Internet Safety

- Treat your password like your toothbrush: don’t share it with anyone and change it often.
- Always remember to log off when you have finished with an online service.
- Use your own digital footprints to remember your favorite Web sites, like the history button and your bookmarks.
- Remember that most of the Web sites you visit will make a note of your visit, and may also track the Web sites you visit before and after their Web site!

Logging My Daily Schedule

In this activity, you will create a seven-day log detailing your daily schedule using the MyDailySchedule spreadsheet file, which should be provided by your teacher as either an Excel spreadsheet or a shared Google Sheets file.

1. Open the file MyDailySchedule, and save it as "*[YourName]*DailySchedule."
2. At the bottom of the sheet, you will see tabs with the names of the week (and one "Example" tab).
3. Click on the "Example" tab and review the sample of how you will complete the remaining sheets.
4. For each day of the week, complete the fields by logging every activity you complete from the time you wake up until you go to sleep.
5. After you have entered your activities for all seven days:
    a. Categorize your daily activities by name and the amount of time you have spent within that category. For example, playing video games would be marked as 1.5 hours for the first day.
    b. Complete Step 5a for all of the days of the week to determine the weekly categories and amount of time spent per category each week.
6. Create a graph showing how much time you spent on each activity. You can do this within the sheet or by adding a new tab at the bottom.

Reflection: Sometimes we do not realize how much time we really spend online until we see it written down and counted (as we did in this activity).

Case Study: Safety and Revealing Too Much

Directions

Form teams of two to three students or work with a few friends. Read the following case study scenario. Then complete the assignment that follows with your team. Be prepared to share your results with the class.

Scenario

Jody is a high-school sophomore who happens to be a star player on the girls' varsity basketball team. She has a Facebook account that her parents know about, and she frequently posts pictures of her basketball team and their big wins on her main page. The pictures normally show the girls in their team uniforms with subtitles that indicate the game dates and times.

One day before school, Jody receives a creepy message from an unknown person asking for details about when and where the next game will be. At first Jody ignores the stranger, but the person becomes more determined and keeps sending messages, now asking personal questions about Jody and her teammates. Jodi blocks the stranger from her Facebook page and tells her parents what is happening.

When her parents check her profile page, they become more concerned. The pictures and updates Jody has posted reveal a lot of personal information, including what school she goes to, when the girls practice, and where they are playing upcoming games. Jody didn't mean to reveal personal information, and in fact she was careful about what she did and didn't post.

What can an interested stranger do with a small amount of information?

Assignment

Help Jody and her teammates stay safe. Use your knowledge of cybersafety techniques and the WWW Decision Tool technique to answer the following questions.

1. Create a list of checkpoints to evaluate Jody's good and bad choices.
2. Using various search engines, explore websites that discuss this topic.
3. Using a word processor, summarize the information and write a one-page paper about the recommended steps that Jody should take to stay safe online.
4. Include in your research paper a bibliography citing the information you used from Internet sources.
5. Save the file in your documents folder.