

# Chapter 4

## Protecting What's Yours: Your Identity



### Overview

Do you know the differences between private and personal information and which type is almost never safe to share online? In this chapter, you will learn about identity thieves, the type of information they steal, and how they accomplish identity theft. Listed tips for staying safe online, including how to create a strong password, will help you avoid identity theft. A discussion of what to do if your identity is compromised rounds out the chapter.



### Key Terms

- Identity theft
- Identity thieves
- Private information
- Personal information
- Passwords

# Fact!



## Did You Know?

In 2012, about 16.6 million people—about 7% of U.S. citizens age 16 or older—were victims of identity theft.

*Source: Bureau of Justice Statistics*

**When thieves send out emails that ask for private information, it is known as phishing.**



## What Is Identity Theft?

**Identity theft** is when private information, such as your name or Social Security number, is stolen and used without permission, usually to commit financial fraud. **Identity thieves** often use cyberspace to find and steal identities, because a great deal of information is available on the Web. Identity thieves gather available information from social media accounts and other public sites, and they find ways to trick people into revealing even more information.

## How Identity Theft Is Accomplished

Identity thieves can be very clever. **Listed below are three ways thieves use the Internet to steal private information:**

### 1 Phone Calls

Thieves may contact us by phone, pretending to work for legitimate companies or institutions that we trust. Since our trust in them has already been established, it does not seem suspicious that they are asking for private information such as account passwords, Social Security numbers, or home addresses. Identity thieves may also pretend to be a friend or acquaintance in order to obtain private data.

### 2 Phishing

When thieves send out emails that ask for private information, it is known as phishing. (The term comes from the image of a person casting a fishing line.) The emails may state that you have won a prize and that in order to claim your winnings, you must provide specific private information. Other email phishing scams include thieves posing as a service provider or a credible company. The emails say there is a problem with your account and that in order to resolve it, you must give them some private data. The emails may also ask you to click on a link contained in the body of the email. Once you do, malicious viruses can be downloaded to your computer. The viruses can steal information stored on your computer and record keystrokes you make while typing in banking or credit card logins and passwords.

### 3 Public Computers

If a person uses a public computer and leaves without signing out of private accounts, anyone using the computer next will have full access to that person's private information.





## Stolen Information

What do thieves do with the information they steal? **While not every thief uses stolen information in the same way, many use the stolen data in the ways listed below:**

- To **gain access** to your bank accounts
- To **take out a loan** in your name
- To **open credit card accounts** in your name
- To **open utility accounts** in your name
- To **seek medical assistance** using your name
- To hijack, or take over, your email account to **send unsolicited messages**

## What's Private and What's Personal?

The words *private* and *personal* have similar meanings, but in cyberspace, the difference between them is very important. It's not always easy to comprehend what information is private and should never be shared online and what information is personal but is acceptable to share online. **Review the characteristics of private versus personal information and think about what information you reveal on the Internet:**

### 1 Private Information

**Private information** is information that could identify who you are. **Private information, such as the items shown below, should never be shared online:**

- Full name
- Social Security number
- Birth date
- Address
- Phone number
- Account passwords
- Credit card numbers
- Bank account numbers
- Any private information belonging to parents or guardians

**Be alert:**  
**In cyberspace, there is a big difference between private and personal information.**



## 2 Personal Information

**Personal information** doesn't necessarily identify who you are, even though the information is personal to you. It's acceptable to share some personal information online as long as you have a parent's or guardian's permission to do so. **Personal information includes the examples shown below:**

- Favorite sports
- Favorite music
- Opinions on movies
- Advice on a topic
- Favorite book

## When Is It Safe to Share Private Information?

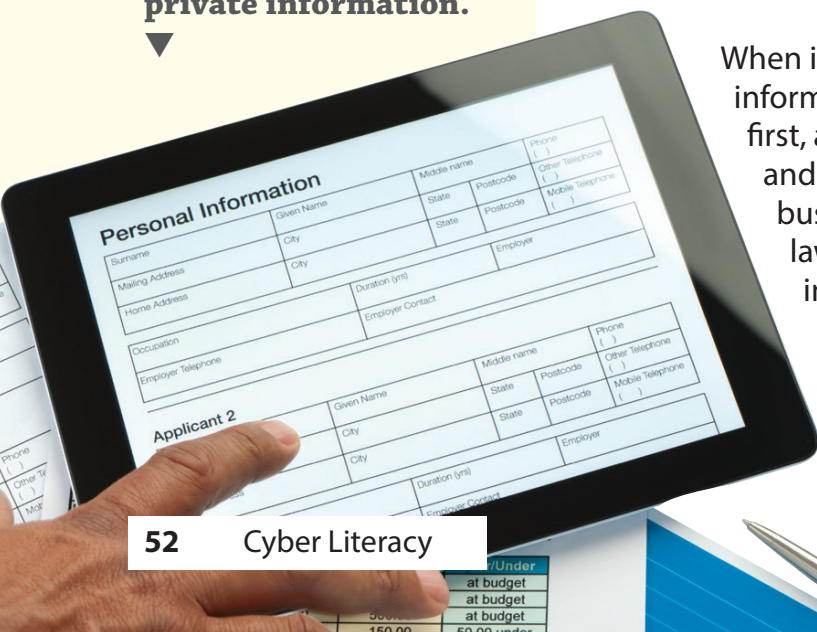
Most of the time, it is never safe to share private information. But as you get older, there are some situations in which you may be required to provide private details about yourself. Always check with a parent or guardian first before sharing private information.

**Shown below are a few examples of situations in which you may be required to provide private information (such as your Social Security number):**

- Applying for a **driver's license**
- Filling out paperwork for a **new job**
- Preparing **tax information**
- Applying for a **bank loan**
- Opening a new **bank account**

**When you apply for an after-school job, it is safe to provide private information.**

When in doubt about giving out private or personal information, always check with a parent or guardian first, and then ask why the information is needed and how it will be used. If a government agency or business asks for your private data, it is required by law to disclose if it is optional for you to share your information, what the data will be used for, and what law requires you to share.












## Stay Safe by Staying Alert

Protecting your identity online is very important, because the nature of the Internet has made it easier for thieves to steal private information and passwords. **There are some things you can do to make sure you are protected online, most of which require a heightened sense of observation and staying alert while using the Internet:**

### Identity Protection Tips

-  Create strong passwords.
-  Never give your passwords to other people, including your friends.
-  Do not share private information about yourself.
-  Be careful of what information you share on social networking sites (even if you think you're interacting only with friends).
-  Monitor your online accounts frequently, because consumers are often the first to notice instances of identity theft.
-  Tell a trusted adult if you observe any questionable activities on your accounts.
-  Always log out of your private accounts when you are finished using them.

#### Remember:

**Identity theft is when private information is stolen and used without permission, usually to commit financial fraud.**



#### Stay safe:

**Create strong passwords and do not share them with anyone, including your friends.**





**Use the following websites to help you generate strong passwords:**

- <https://identitysafe.norton.com/password-generator>
- <http://www.random.org/>
- <http://strongpasswordgenerator.com/>



## How to Create a Strong Password

**Passwords** are like locks that keep our private information safe. emails, social networks, and some gaming websites all use passwords to help protect our private data. Without a strong password, private information can be easy for thieves to steal.

**A few tips for creating a strong password are listed below:**

### 1 Don't use any self-identifying facts.

Never use your full name, birth date, or address.

### 2 Avoid using obvious facts about yourself.

Never use information that would be easy to guess (such as your nickname or your pet's name).

### 3 Make passwords of at least eight characters.

However, follow the instructions on a website for password length. Some websites may require passwords longer than eight characters.

### 4 Include a combination of numbers, symbols, and letters.

This will make your passwords as unique as possible. Some websites require this combination of characters. Websites may also tell you whether a password is weak or strong. If a website indicates that your password is weak, add characters until it is strong. Be sure to read the recommendations on a website for creating a strong password whenever setting up a new online account.

### 5 Change your passwords every few months.

### 6 Create passwords that you will remember.

If you think you will have trouble remembering them, write them down and keep them in a safe place.

### 7 Don't enter your passwords into your phone.

Someone might steal your phone, or you might lose it.

### 8 Don't type your passwords in a public place.

People might look over your shoulder as you type in your passwords. Additionally, if you are in a place that offers free Internet access, such as a coffee shop, people using the same wireless connection might be able to see your passwords as you type them into a website.





## What to Do If Your Identity Is Compromised

There are many tools in place to help consumers deal with identity theft, but the first step is to tell your parents or guardians. If you are worried that private information about yourself may be available publicly, it's important to report it right away so that your identity can be protected. Many times, if a case of identity theft is reported immediately, it is easier to undo the damage. But if identity theft goes undetected, thieves can use stolen information for a long time, creating long-lasting problems.

A parent or guardian will help you determine the best course of action if your identity has been compromised. **Listed below are a few general steps to follow if your private information has been exposed publicly:**

### 1 Report it.

Tell a parent or trusted adult. He or she may want to report identity theft to the police or place an alert on any compromised accounts. He or she may also call the major credit reporting agencies to report the identity theft and ask for unauthorized purchases to be removed from your credit report.

### 2 Close it.

If an account has been exposed to identity theft, close it to avoid any further damage.

### 3 Watch it.

If you are opening a new account or leaving a compromised account open, be sure to watch it carefully for any questionable activity.



Report identity theft immediately to minimize the potential damages.

## Fact!



### Did You Know?

In 2012, most victims of identity fraud were unaware of the fraud until a financial institution contacted them about an account that showed suspicious activity. Two-thirds of identity-theft victims were unable to determine how their private information was stolen.

**Source:** Bureau of Justice Statistics

# Chapter 4 Assessment

## What Do You Think?

Write a reflection of three to five paragraphs about a time when you or someone you know shared too much private information, perhaps by giving a friend a Facebook or email password. Your paragraphs should answer the following questions:

- 1 Why is it not safe to share your passwords, even with people whom you know?
- 2 What can you do if you have shared private information?

## Challenge: What Would You Do?

Read each of the situations below and determine what you would do. Write one paragraph for each situation. Use what you have learned in the chapter to justify your answers.

- 1 You have to create a new email password, but you're afraid you'll forget the password you create.  
**What would you do? Why?**
- 2 While you are registering for an online gaming website, it requests your Social Security number.  
**What would you do? Why?**
- 3 Your boyfriend/girlfriend asks you for your Facebook password.  
**What would you do? Why?**
- 4 An online friend asks for your home address.  
**What would you do? Why?**





## Extension Activities

### Activity 1 Short Answer

Use what you have learned in this chapter to write responses to the prompts below.

- 1 Define the term *identity theft*.
- 2 Describe the difference between private and personal information.
- 3 Identify five pieces of information that should never be shared publicly.
- 4 List three ways to create a strong password.
- 5 Explain how identity thieves gain access to private information.

### Activity 2 Identification Card

Examine the student identification card below and, using what you have learned in this chapter, identify and list what data could be stolen and used by an identity thief.

#### Student Identification Card

Niceville Public Schools

2015/2016



**Scott Smith**

Date of Birth: 12/20/99

Address: 333 Pleasantville Drive  
Niceville, MI 12345

Phone #: 555-123-4567

Student ID #: 2225554466

*continued*



## Extension Activities

### Activity 3 Multiple Choice

Read the questions below. Use what you have learned in this chapter to help you choose the correct answer.

- 1 What is phishing?
  - A. When your email password has been stolen
  - B. When you create a strong email password
  - C. When thieves ask for private information
- 2 Which of the following is NOT considered private information?
  - A. Social Security number
  - B. Opinions
  - C. Home address
- 3 What should you do first if you think your identity has been compromised?
  - A. Keep an eye on the situation.
  - B. Tell a parent and trusted adult.
  - C. Tell a friend.
- 4 Which of the following statements is true of a strong password?
  - A. It should be at least eight characters long and use a combination of symbols, numbers, and letters.
  - B. It should be shared with friends.
  - C. It should include personal information so that you can remember it.
- 5 When might you be asked to share private information, such as your Social Security number?
  - A. When signing up for an online gaming subscription
  - B. When joining an online chat room
  - C. When opening a new bank account



## Hands-On

### Create an Identity Theft Tip Sheet

Think about what you learned in this chapter and what you know about identity theft. Make notes of your knowledge. Make sure to include what you know about the following elements:

- A definition of identity theft
- How to create a strong password
- The difference between private and personal information
- How to avoid identity theft
- Facts about identity theft that you learned in this chapter

Then, using poster board and colored pencils or a computer presentation program, create a tip sheet similar to the one provided in **Figure 4.1** on the next page.

*continued*





# Hands-On

Figure 4.1

Identity Theft Tip Sheet	
Avoiding Identity Theft: How to Keep Your Information Safe and Secure	
<b>What Is Identity Theft?</b>	<b>Password Tips</b> 1. 2. 3. 4. 5. 6. 7. 8.
<b>How to Avoid Identity Theft</b>  <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____	
<b>Identity Theft Facts</b>	<b>Private vs. Personal Information</b>