

10 WAYS TO be Smart Online

Lesley Ito

Series Editor: Andy Boon



POCKET READERS

10 WAYS TO - Series Overview

The 10 WAYS TO series provides advice, skills, and strategies to the readers for successfully negotiating different aspects of life. Each book suggests 10 clear, useful ways to the reader. The reader is encouraged to critically reflect on the reading material and their own lives in order to make any changes that would benefit them. The series includes the following.

- 10 ways to achieve work-life balance
- 10 ways to be more productive
- 10 ways to manage money
- 10 ways to be successful in love
- 10 ways to be assertive
- 10 ways to be smart online
- 10 ways to be environmentally friendly
- 10 ways to be healthy
- 10 ways to work in a team
- 10 ways to organize a trip

More titles will appear in the series at a later date.

10 WAYS TO be Smart Online

Introduction	... 4
1. Don't choose a weak password	... 6
2. Don't believe spam emails	... 8
3. Don't believe phishing scams	...10
4. Watch out if your friends get hacked	... 12
5. Don't become online friends with people you don't know	... 14
6. Be a smart online shopper	... 16
7. Don't believe fake news	... 18
8. Protect your computer and the information on it	... 20
9. Don't give out your private information	... 22
10. Watch what you post on social media	... 24
Summary	... 26
Reflection Questions	... 28
Vocabulary in Context	... 29
Vocabulary List	... 36

Introduction

The Internet has changed our lives in so many ways. Before the Internet, we could only buy things by going to stores. We usually only talked to people who lived near us. We used the telephone to talk to people far away. We read the morning newspaper to get the news.

Now, we can go online using our smartphones and computers. We can buy things online. We can chat to people from all over the world. We can read the news online. We can do these things at any time of the day. Going online is great!

However, there is also a lot of danger online. Some people may want to

scam us. They want to **steal** our information. They want to steal our money. **Hackers** may try to give our computer a virus. They may get **access** to our email or social media. Some people post **fake** or incorrect news to try to spread wrong information. We have to be careful. We have to **protect** ourselves. We have to be smart to stay safe online.

Now, stop and think for a moment. Do you worry about your information online? Do you worry about shopping online or visiting websites? Do you worry about becoming friends with people on social media? Do you worry about reading and sharing fake news **articles**? Let's look at ten ways that you can be safer online:

1. Don't choose a *weak* password

A weak password is one that is easy for hackers to guess. If hackers **guess** your password, they can access your email or social media account. They can steal your information. The weakest passwords are: 123456, 12345678, Password, qwerty, letmein, hello, iloveyou, and welcome.

The strongest passwords use UPPER CASE LETTERS, lower case letters, numbers, and other characters (For example - “#, \$, or %”). They are also long. So, choose a strong password. Don't use numbers from your birthday, address, or telephone number. It is also a good idea to use the first letters of each word in a sentence instead of a word. For example: !TaTwTbSo10! is a

strong password. It uses the first letter of each word in this sentence: *There are ten ways to be safe online.* Some letters are upper case. Some letters are lower case. There are numbers. The numbers are not from a birthday, address, or telephone number. There are special characters at the beginning and end of the password - two exclamation points! This is a password that can keep you safe from hackers.

2. Don't believe *spam* emails

Spam emails are sent to many people at one time. In the email, the writer does not greet you by name. Maybe, they try to sell you something. Or, maybe, they say they want to give you lots and lots of money.

It's easy to know when you get a spam email. First, a spam email is from someone that you do not know. Then, look for spelling mistakes. Spam emails often have many words that aren't spelled correctly. Finally, spam emails say things that are too good to be true. For example, why would someone you don't know want to send you lots and lots of money? Why would someone you have never met want to do business with you?

How can you protect yourself from spam emails? Don't click on any *links* in the email. Don't open any *attachments* in the email. Clicking on these links or opening these attachments may give your computer a virus. The best way to protect yourself from a spam mail is just to *delete* it.

Reflection Questions

1. Can you remember the 10 ways to be safe online? Test yourself. If you forget any, go back, and read them again.
2. Do you do any of the 10 ways to be safe online in your life? If so, which ones do you do?
3. How could you use any of the 10 ways to be safe online in your life?
4. What do you think you will do differently in your life after reading this book?
5. Can you think of other ways to be safe online?

Vocabulary in Context

1. Scam

- Some people may want to **scam** us. They want to steal our information.
- I was told I won some money, but it wasn't true. It was a **scam**.
- **Scammers** tell you something that isn't true, so they can take your money.

2. Steal

- Scammers want to **steal** our information. They want to take it without asking.
- The girl wants to take the clothes from the store without paying. She wants to **steal** the clothes.
- He took the woman's bag and ran away. He **stole** the bag.

3. Hackers

- **Hackers** may try to give our computer a virus.
- I think my computer has a virus. I think it was **hacked**.
- The boy tried to get into the company's computer system. He didn't have a password, so he **hacked** into the system.

Vocabulary List

Scam:	(Verb and Noun) Telling a lie to try to steal information or money; a scheme where a person is told a lie to try to steal their information or money. A scammer (Noun) is a person who tries to scam others.
Steal:	(Verb) to take something that is not yours.
Hacker(s):	(Noun) a person who tries to get into a person's computer remotely by stealing the password or breaking into the security system. Hack (Verb) is the action of breaking into a computer.
Access:	(Noun & Verb) the ability to enter a place; the action of entering a place.
Fake:	(Adjective) not real; not true.
Protect:	(Verb) to keep something safe. Protection (noun) is a thing that protects something.
Articles:	(Noun) a piece of writing in a newspaper, magazine, or online news source.
Weak:	(Adjective) not strong.
Guess:	(Verb) to say what you think the answer is, even if you don't know.
Spam:	(Noun) bad or junk emails that are sent to many people at one time.