

# Unit 5 Law

## Part 1 Overview of the unit

### Teaching objectives

Upon completion of this unit, the T is expected to enable Ss to:

OBJECTIVES	
<ul style="list-style-type: none"><li>recognize the common types of cybercrimes</li><li>understand how to protect yourself from common cybercrimes</li><li>understand the significance of cybersecurity and China's role in global digital governance</li></ul>	Knowledge
<p><b>Listening skill</b></p> <ul style="list-style-type: none"><li>understand supporting evidence</li><li>recognize citations</li></ul> <p><b>Critical thinking skill</b></p> <ul style="list-style-type: none"><li>evaluate source reliability</li></ul> <p><b>Speaking skill</b></p> <ul style="list-style-type: none"><li>disagree politely</li></ul>	Skills
<ul style="list-style-type: none"><li>debate the appropriacy of a punishment in a cybercrime case study</li></ul>	Unit task

## A suggested teaching plan

Periods 1 & 2	Before class	Check Ss' online study ( <b>Warming up, Academic listening</b> )	
	In class	Introduce the topic; deal with the video in <b>Warming up</b> based on Ss' online performance	20 mins
		Go through <b>Academic listening 1</b> based on Ss' online performance	30 mins
		Go through <b>Academic listening 2</b> based on Ss' online performance	30 mins
		Deal with <b>Getting the skill</b> in <b>Critical thinking</b>	20 mins
	After class	Ask Ss to do the oral practice of <b>Academic listening</b> Ask Ss to preview <b>A cross-cultural view</b> and <b>Academic communication</b>	
Periods 3 & 4	Before class	Check Ss' online study ( <b>A cross-cultural view, Academic communication</b> )	
	In class	Deal with <b>A cross-cultural view</b>	30 mins
		Introduce the objectives of <b>Academic communication</b> ; analyze the speaking model	15 mins
		Go through the speaking skill based on Ss' online performance	5 mins
		Raise a thorough discussion and help Ss finish the mini-project in <b>Skill enhancement</b>	20 mins
		Guide Ss to finish the speaking task step by step	30 mins
	After class	Ask Ss to upload the recordings of their presentations and complete self-evaluation	

## Part 2 A detailed teaching guide

### Warming up



#### Cybercrime

With advancements in Internet technology, cybercrime is rising. Experts say that modern criminals can steal more with a keyboard than they can with a gun. Internet technology has not only given traditional crimes such as fraud a new form, but also brought cybercrimes like hacking. Let's look at these cybercrimes together.

Fraud is a crime that tricks victims out of money or property. Internet fraud is similar. Criminals use the Internet to cheat others to get money or property.

Besides fraud, there's ransomware. Holding someone or something for ransom means refusing to release it until money is paid. Ransomware works in the same way. Criminals will use ransomware to threaten to publish the victim's data, or to block their access to their own data, until a huge ransom is paid.

To hack means to cut or chop. In cyberworld, hacking involves illegally breaking into a computer system or network. Usually hackers do it either to make a profit, or to gather secret or important information to use or sell.

Phishing comes from the analogy to "fishing." Phishing is the crime of tricking people into giving sensitive information. By faking official websites or by sending emails and text messages, criminals try to get usernames, passwords and financial information.

Though cybercrime has a short history, it is now a major security threat. Cybercrime prevention needs our joint effort and every Internet user's awareness of risks.

### Words and expressions

cybercrime *n.* 网络犯罪

fraud *n.* 欺诈, 诈骗

ransom *n.* 赎金

ransomware *n.* 勒索软件

cyberworld *n.* 网络世界

phishing *n.* 网络钓鱼

analogy *n.* 类似处, 相似处





### Teaching suggestions

- 1 Introduce the unit topic by showing the pictures of Task 1 & 2 on Pages 76-77. Explain difficult terms based on Ss' online performance in Task 1.
- 2 Play the video and pause at the parts where most students make most mistakes according to the Ucampus statistics in Task 2.
- 3 Ss work in groups to discuss the questions in Task 3. Then ask 2-3 Ss to share their answers.

## Reference answers

### Task 1

			
<b>hacking</b>	<b>Internet fraud</b>	<b>phishing</b>	<b>ransomware</b>

### Task 2

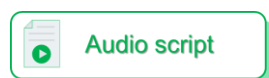
<b>hacking</b>	<b>Internet fraud</b>	<b>phishing</b>	<b>ransomware</b>
Criminals illegally break into a computer system or network for various purposes.	Criminals make use of the Internet to defraud people of money or property.	Criminals pretend to be a real organization, such as a bank, and trick victims into giving their sensitive information.	Criminals threaten to publish the victim's data or block their access to it unless a ransom is paid.

### Task 3

1. I think hacking is the most dangerous because everyone could be the victim even if they do nothing to incur the risk. If my computer got hacked, I would probably have no other choice but to reinstall my operating system, and I might lose my important documents forever.
2. Yes, I think so. In a traditional way, it's difficult for criminals to run away with a large sum of cash, which could be too heavy to transport. But cyber criminals may transfer a huge amount of money from your account to someone else's account by just a few clicks without leaving a trace.

## Academic listening

### Listening 1 Ask an expert



#### *Ask an expert*

**HOST:** Greetings listeners, and welcome to *Ask an expert*, the weekly show in which we interview experts from a variety of fields. Today's topic is cybercrime, and our expert is Robert Braun, professor of law at Pennbrook University. Professor Braun, welcome to our show.

**BRAUN:** Thank you.

**HOST:** Let's start with a simple definition. What is cybercrime, and how common is it?

**BRAUN:** Well, it means any illegal activity committed with a computer. Now that covers a broad range of criminal activities, including crimes against people, such as stealing someone's identity or online bullying, crimes against property, such as illegal movie downloads, and crimes against governments, mainly spying.

**HOST:** That is a broad range, indeed. Well now, let's get specific and look more closely at some of the cybercrimes you mentioned. I suppose many of our listeners have heard the term "malware." Could you explain what that means?

**BRAUN:** Sure. “Malware” isn’t a crime. It’s a general term that means any kind of software that’s used to commit crimes, for instance stealing private information, spying on users, or displaying unwanted advertising. The victims can be individuals, corporations, or governments. To give just one example, in its December 30, 2015 issue the respected magazine *Business Insider* reported that in 2014 hackers used malware to break into a computer system at the White House, the home of the President of the United States! In another famous case, about 15 million customers had their personal information stolen when criminals hacked into the website for the finance company Experian.

**HOST:** Yes, I remember that. All right, I’d like to continue now and discuss the topic of computer piracy. What is that?

**BRAUN:** It means illegally downloading movies, books, or music from the Internet, without paying for the content.

**HOST:** Why is that illegal?

**BRAUN:** Let me explain. We have a concept called “intellectual property.” According to the Macmillan Dictionary, “intellectual property” is something that someone has created or invented and that no one else is legally allowed to make, copy, or sell. In other words, it’s against the law to download intellectual property without paying for it.

**HOST:** What’s the punishment for illegally downloading a movie?

**BRAUN:** People who are caught downloading movies illegally can face up to a year in jail and a fine of \$100,000. That’s just for personal use. If you turn around and sell those illegally downloaded movies, the crime is much more serious. You could go to jail for five years and face a penalty of \$250,000.

**HOST:** That seems pretty severe.

**BRAUN:** It’s a serious crime. It’s expensive to make movies, and if companies can’t make money, they’ll stop doing it.

**HOST:** I’m speaking with law professor Robert Braun. Let’s take a break, and then we’ll talk some more.

### **Words and expressions**

bully v. 欺侮，恐吓

### **Proper names**

Robert Braun 罗伯特·布朗（人名）

Experian 益博睿（一家信息服务公司）

Macmillan Dictionary 麦克米伦词典

## Before you listen

### Task 1 Match the words with their definitions.

1. spy D	A. (n.) a specific part, feature, or quality of something
2. aspect A	B. (n.) behavior that threatens or hurts someone smaller or weaker
3. severe H	C. (n.) the information or ideas in a book, magazine, movie, website, etc.
4. case F	D. (v.) to find out the information about a person, country, organization, etc. secretly
5. victim G	E. (n.) an idea, design, or invention that cannot legally be copied or sold
6. bullying B	F. (n.) a matter or situation related to the law, and usually argued in court
7. intellectual property E	G. (n.) someone who has been harmed, injured, or killed because of a crime or accident
8. content C	H. (adj.) very strict or extreme

### Task 2

#### Step 1 Complete the sentences with the following words and expressions. Change the form if necessary.

aspect	bullying	case	content
intellectual property	victim	spy	severe

1. Spying on people's affairs is not an acceptable way to get to know them.
2. To safeguard personal information is one of the most important aspects of cyber law.
3. Anyone who is caught trying to break into government computers should face a(n) severe punishment.
4. A good lawyer will win every case.
5. If you're the victim of identity theft, it will be inconvenient for you in many ways.
6. The best thing to do about online bullying is to ignore it, and hope it stops.
7. The Internet makes it too easy to steal other people's intellectual property.
8. There need to be stricter controls on what content can be shared online.

#### Step 2 Think about the sentences, and choose the one(s) you agree with.

1. Spying on people's affairs is not an acceptable way to get to know them.
2. To safeguard personal information is one of the most important aspects of cyber law.
3. Anyone who is caught trying to break into government computers should face a severe punishment.
4. A good lawyer will win every case.
5. If you're the victim of identity theft, your bank should pay back any money that was stolen from you.
6. The best thing to do about online bullying is to ignore it, and hope it stops.
7. The Internet makes it too easy to steal other people's intellectual property.
8. There need to be stricter controls on what content can be shared online.

## Answers

Open-ended.

### Task 3 Answer the following questions.

1. Have you ever met with cybercrime?
2. Do you agree that the people who download movies illegally should be punished? How do you think they should be punished?

### Reference answers:

1. My computer was hacked by a “WannaCry” virus several years ago and all my documents were lost.
2. I totally agree. I think the punishment for downloading movies illegally should be similar to that for theft, i.e. fines or even imprisonment. Because in my understanding, it’s like taking something that doesn’t belong to you without permission. So it is a kind of theft in nature.

## Global listening

### Task 1 Listen to a radio show called *Ask an expert* and rearrange the topics in the order they are mentioned.

- |          |  |
|----------|--|
| <u>5</u> | Examples of crimes that used malware   |
| <u>2</u> | Definition of malware                  |
| <u>1</u> | Punishment for illegal movie downloads |
| <u>4</u> | Definition of computer piracy          |
| <u>6</u> | Definition of cybercrime               |
| <u>3</u> | Definition of intellectual property    |

## Close listening

### Task 1 Listen to *Ask an expert* again and choose the best answer to each question you hear.

1. Question 1
  - A. An editor who works for the Macmillan Dictionary.
  - B. An editor from the respected magazine *Business Insider*.
  - C. A law professor at Pennbrook University.
  - D. An expert from the finance company Experian.
2. Question 2
  - A. Unwanted advertising was displayed on a respected magazine.
  - B. A finance company was broken into.
  - C. A government computer system was hacked.
  - D. Fifteen million customers’ personal information was stolen.
3. Question 3
  - A. It destroys the film industry.
  - B. It endangers digital security.
  - C. It causes social discrimination.
  - D. It violates the intellectual property.

4. Question 4
- A. Up to a year in jail and a fine of \$100,000.
  - B. Up to a year in jail and a fine of \$250,000.
  - C. Five years in jail and a penalty of up to \$150,000.
  - D. Five years in jail and a penalty of \$250,000.

**Questions:**

- 1. Who is the guest expert of the weekly show?
- 2. What case did *Business Insider* report in 2015?
- 3. Why is computer piracy illegal?
- 4. What is the punishment for selling illegally downloaded movies?

**Task 2 Answer the following questions according to what you have heard.**

- 1. What does “malware” mean? Is it a crime?
- 2. Why is illegally downloading a movie a serious crime?

**Reference answers:**

- 1. Malware is a general term that means any kind of software that’s used to commit crimes, for instance stealing private information, spying on users, or displaying unwanted advertising. It’s not a crime itself, but it can be the tool for crimes.
- 2. Because it’s expensive to make movies, and illegal downloading will cause movie companies to make less money and perhaps to stop making movies.

**Task 3 Work in pairs to discuss the following questions.**

Do you think the punishment for downloading movies illegally is appropriate, too severe, or not severe enough? Why?

**Reference answers:**

I think it’s too severe. In my opinion, if people illegally download a movie but do not distribute it or sell it, they should pay the market price plus a small fine, which is a lot smaller than \$100,000. Putting them in jail for one year not only increases the cost of the judicial system, but also deprives the people of their freedom. As for people who sell the illegally downloaded movies, I think the punishment should depend on how much damage the behavior has caused.



## Academic listening skill

### Task 1 Read the following paragraph to learn about the listening skill of understanding supporting evidence.

Understanding supporting evidence is an important skill in academic listening. There are three common types of evidence: 1) definition, which tells the meaning of a concept; 2) example, which provides the information of a representative; 3) explanation, which clarifies the message in different ways.

The following are some common signals for them:

<b>Definition</b>	<i>This / It is defined as ...</i>	<i>This / That / It means ...</i>	<i>X is ...</i>
	<i>X, which means ...</i>	<i>X, meaning ...</i>	
<b>Example</b>	<i>For example, ...</i>	<i>For instance, ...</i>	<i>... such as ...</i>
	<i>To give an / another example, ...</i>	<i>An example of this is ...</i>	<i>In another case ...</i>
<b>Explanation</b>	<i>In other words, ...</i>	<i>That is to say ...</i>	<i>Specifically, ...</i>
	<i>Let me explain ...</i>		

### Task 2 Listen to Ask an expert again and fill in each blank of the notes with no more than two words.

#### Cybercrime

**Cybercrime** = any 1) illegal activity committed with a computer.

e.g. stealing someone's 2) identity, online bullying, illegal movie downloads, spying

**Malware** = any kind of 3) software used for crime.

e.g. stealing 4) private information, spying on users, displaying unwanted advertising

#### Famous cases:

Hackers used malware to break into a White House computer system in 2014.

Experian's website was hacked, with 5) 15 / fifteen million customers' personal information stolen.

**Piracy** = illegally downloading content without 6) paying for it.

- This content = **intellectual property**, something that sb. has created or invented / no one else is legally allowed to make, 7) copy, or sell.

- Punishment for downloading a movie illegally:

a. 1 year in jail + \$100,000 fine (personal use)

b. 5 years in jail + \$250,000 penalty (downloading + selling)

## Teaching suggestions

### Close listening

- 1 Ask Ss to read the two questions in Task 2. Then play the recording. Ask Ss to take notes while listening.
- 2 Ask Ss to work in pairs. Ss take turns to answer the questions. Check Ss' answers and replay the parts where they make most mistakes.
- 3 Ask Ss to read the questions in Task 3 and discuss them in pairs.
- 4 After the discussion, T invites 1 or 2 Ss to share their answers with the whole class. T gives comments on the Ss' answers.

### Extension activity

- 1 Ask Ss to work in groups to share their experiences of being victims of cybercrimes and to discuss how they can protect themselves in similar situations.
- 2 After the discussion, T invites 1 or 2 Ss to share their answers with the whole class. Make comments on S's answers.

### Academic listening skill

- 1 Log on Ucampus and present the task. Ask Ss to read the notes first and try to recall different types of supporting evidence.
- 2 Then play the audio for Ss to check their answers.

### Extension activity

- 1 Play the audio and ask Ss to find examples of the three types of supporting evidence.
- 2 Ask 2-3 Ss to share their answers with the class. Each S gives only one example and should not repeat others' answers. T comments on their answers.

Ss' answers may be:

#### Definition

1)

-Let's start with a simple definition. What is cybercrime, and how common is it?

-Well, it means any illegal activity committed with a computer. Now that covers a broad range of criminal activities, including crimes against people, such as stealing someone's identity or online bullying, crimes against property, such as illegal movie downloads, and crimes against governments, mainly spying.

2) "Malware" isn't a crime. It's a general term that means any kind of software that's used to commit crimes, for instance stealing private information, spying on users, or displaying unwanted advertising. The victims can be individuals, corporations, or governments.

3)

-I'd like to continue now and discuss the topic of computer piracy. What is that?

-It means illegally downloading movies, books, or music from the Internet, without paying for the content.

### Example

1) To give just one example, in its December 30, 2015 issue the respected magazine *Business Insider* reported that in 2014 hackers used malware to break into a computer system at the White House, the home of the President of the United States!

2) In another famous case, about 15 million customers had their personal information stolen when criminals hacked into the website for the finance company Experian.

### Explanation

1)

-Why is that illegal?

-Let me explain. We have a concept called "intellectual property." According to the Macmillan Dictionary, "intellectual property" is something that someone has created or invented and that no one else is legally allowed to make, copy, or sell. In other words, it's against the law to download intellectual property without paying for it.

2) It's a serious crime. It's expensive to make movies, and if companies can't make money, they'll stop doing it.



### Oral practice

**Task 1** The following sentences will help you understand cybercrime. Translate the Chinese in brackets into English using the words and expressions you've just learned, and then record each sentence.

1. Now that covers a broad range of criminal activities (犯罪活动), including crimes against people, such as stealing someone's identity or online bullying (网络欺凌), crimes against property, such as illegal movie downloads, and crimes against governments, mainly spying.
2. All right, I'd like to continue now and discuss the topic of computer piracy (盗版).
3. According to the Macmillan Dictionary, "intellectual property (知识产权)" is something that someone has created or invented (发明) and that no one else is legally allowed to make, copy, or sell.
4. People who are caught downloading movies illegally can face up to a year in jail (入狱) and a fine of \$100,000. That's just for personal use (个人用途).

**Task 2** You will hear four clips of the conversation. Each clip will be played only ONCE. After you hear a tone, please repeat the exact words the second speaker has said. You may take some notes while you listen.

1.

**HOST:** Let's start with a simple definition. What is cybercrime, and how common is it?

**BRAUN:** Well, it means any illegal activity committed with a computer. Now that covers a broad range of criminal activities.

2.

**HOST:** Well now, let's get specific and look more closely at some of the cybercrimes you mentioned. I suppose many of our listeners have heard the term "malware." Could you explain what that means?

**BRAUN:** Sure. "Malware" isn't a crime. It's a general term that means any kind of software that's used to commit crimes.

3.

**HOST:** All right, I'd like to continue now and discuss the topic of computer piracy. What is that?

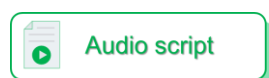
**BRAUN:** It means illegally downloading movies, books, or music from the Internet, without paying for the content.

4.

**HOST:** That seems pretty severe.

**BRAUN:** It's a serious crime. It's expensive to make movies, and if companies can't make money, they'll stop doing it.

## Listening 2 Protect yourself online



### *Protect yourself online*

Good afternoon everyone and welcome to today's session on cybersecurity. Our goal in this session is to make sure you and your data are protected against people who would like to harm you or your electronic devices. Our main focus will be a discussion on identity theft, and how to prevent it. This is an important topic for college students because the government agency that's responsible for consumer protection, people between the ages of 18 and 24 are the most likely targets of identity theft.

All right, now to begin, what is identity theft? The government defines it like this on its website, and I quote: "Identity theft is a crime where a thief steals your personal information, such as your full name or your social security number, to commit fraud." In addition, the well-known consumer protection organization Consumer Reports explained in a 2016 article that identity theft can be either low- or high-tech. Low-tech theft can happen when a thief looks over your shoulder while you're typing in your personal identification number at an ATM. This is called "shoulder surfing." High-tech ID theft happens when a thief hacks into your computer or your phone. Then, for example, they can steal your social security number and use it to acquire credit cards or even a passport. Or they can steal your credit card numbers and use them to purchase things online. And you may not even know you've been a victim of ID theft until you start getting credit card bills for things you know you didn't buy.

I'm not trying to worry you, and of course the bank will compensate you for any money that is stolen from your account. However, it can be a horrible experience to try to recover your identification once it's been stolen. So, now let's talk about steps you can take to protect yourself and make sure your identity is secure.

Step 1: Protect your numbers! Never share your personal or financial information with anyone. Don't carry your social security card in your wallet, and never give your credit card to anyone else to use.

OK, Step 2, be aware of phishing requests. Phishing, spelled p-h-i-s-h-i-n-g, is when you get an email or text that looks like it's from a company you know, such as your bank or credit card company, asking you to provide your account number or credit card information. These are fake emails sent by criminals whose motive is to try to trick you into giving them your personal details. Remember, an honest company will never ask you to give out that type of information. If you think there is something odd about an email or text, don't reply, and don't click on any links within the message either because they could contain malware.

Now, Step 3. Create strong passwords and update them regularly, both on your computer and on your phone. And avoid common passwords like your birth date or your school name. Most people are not very careful about this. The password manager company called Keeper reported on its website that almost one-fifth of people use the same password! Can you guess what it is? "123456"! Using a password that is so easy to guess will expose you to cyber-attack, so if that's your password, I advise you to change it immediately. Use a combination of numbers and letters, and try to use uppercase and lowercase letters if possible.

Next, Step 4. Be careful about what you share on social media sites. A lot of students practically live on social media sites and a lot of them give away too much information too easily. Krystal Merton, the Security Manager at Pennbrook University, explains that criminals can follow your social media posts and use them to extract information that will help them answer the security questions on your online accounts, such as your birthplace or your mother's maiden name. This is supported by Conrad Stewart, director of student services at the Mayweather Institute in New York. Stewart says, "Criminals exploit students that over-share and over-trust on social media sites." So be careful what you share, and check your privacy settings to make sure only the people you choose are allowed to see what you post on social media.

Finally, Step 5. Protect your computer by installing anti-virus software. This prevents hackers from breaking into your computer or phone and stealing your information. The university provides this kind of software free to all its students and staff, so if you need help installing it just call or bring your device in to the campus computer center.

All right, before we go any further I want to remind you that identity theft is a criminal offense. It is illegal in most countries around the world. The punishment for identity theft includes both jail time and fines. The trouble is that a lot of thieves are very clever, and it is getting harder and harder to catch them.

That's why it's so important to follow the security measures I've been talking about. And if you think you have been a victim of identity theft, be sure to contact the university computer center immediately.

### **Words and expressions**

social security number (美国) 社会保障号码

extract v. 套出 (信息); 索取 (钱财)

maiden name n. (女子的) 娘家姓

### **Proper names**

Consumer Reports 美国消费者报告 (美国非营利组织)

Keeper 一款密码管理程序

Krystal Merton 克丽丝特尔·默顿（人名）

Conrad Stewart 康拉德·斯图尔特（人名）



### Before you listen

#### Task 1 Match the words with their definitions.

1. acquire (v.) D	A. an action intended to achieve or deal with something
2. hack (v.) B	B. to illegally break into a computer system in order to steal information
3. high-tech (adj.) F	C. safe from attack, harm, or damage
4. measure (n.) A	D. to get something
5. motive (n.) E	E. the reason you do something
6. privacy (n.) H	F. using high technology
7. recover (v.) G	G. to get something back that has been lost or stolen
8. secure (adj.) C	H. the state of being free from public attention

#### Task 2 Complete the sentences with the words in the box. Change the form if necessary.

acquire	hack	high-tech	measure
motive	recover	privacy	secure

1. It is illegal to hack into other people's computers?
2. What measure / measures can you take to protect your personal information online?
3. What can you do to maintain your privacy on social media sites?
4. Why is a(n) secure Internet connection important when one browses online?
5. What is the main motive of people who illegally download and share movies for free?
6. Should we make it harder for technology companies to acquire personal information?
7. What steps would you need to take to recover your identity after an identity theft?
8. Which high-tech devices do you think would improve your education?

#### Task 3 Answer the following questions.

1. What can you do to maintain your privacy on social media sites?
2. What steps would you need to take to recover your identity after an identity theft?

### Reference answers:

1. Based on my knowledge and experience, the following measures can be taken:
  - Use anti-virus software and keep it updated;
  - Use strong passwords;
  - Never share personal information like home address, ID number, contact information or date of birth;
  - Be alert to unusual requests from strangers.
2. The steps I would need to take may include:
  - Report to the website;
  - Submit evidence to reclaim my identity;
  - Report to the police if the above steps don't work.

### Global listening

**Task 1 Listen to *Protect yourself online* and put the steps in the order they are mentioned.**

- 2 Be aware of phishing requests.
- 5 Protect your computer by installing anti-virus software.
- 4 Be careful about what you share on social media sites.
- 3 Create strong passwords and update them regularly.
- 1 Never share your personal or financial information with anyone.

### Close listening

**Task 1 Listen to *Protect yourself online* again and choose the best answer to each question you hear.**

1. Question 1
  - A. How to keep you and your data safe.
  - B. How the Consumer Reports helps college students.
  - C. How to protect yourself on social media.
  - D. How to set strong passwords.
2. Question 2
  - A. It is inevitable.
  - B. It is easy to find out.
  - C. It is a type of fraud.
  - D. It is a low-tech crime.
3. Question 3
  - A. Write your passwords down on paper and lock it up.
  - B. Never share your personal or financial information with anyone.
  - C. Ask a friend to keep your credit cards for you.
  - D. Always carry your social security card with you.
4. Question 4
  - A. richmondhigh
  - B. 20121225
  - C. Trustno1
  - D. MYPASSWORD

5. Question 5
- A. Delete the account with the stolen ID.
  - B. Reinstall the current software or app.
  - C. Call the police immediately.
  - D. Contact the university computer center.

**Questions:**

1. According to the speaker, what is this session supposed to explain?
2. What is true about identity theft?
3. What should you do to protect your personal information?
4. Which of the following is a strong password?
5. What is the speaker's suggestion for a student who has been a victim of identity theft?

**Task 2 Answer the following questions according to what you have heard.**

1. According to the 2016 Consumer Reports article, what's the difference between low-tech ID theft and high-tech ID theft?
2. According to Krystal Merton, how can criminals exploit your information through social media sites?

**Reference answers:**

1. Low-tech ID theft can happen when a thief looks over your shoulder while you're typing in your personal identification number at an ATM. High-tech ID theft happens when a thief hacks into your computer or your phone. For example, they can steal your social security number and use it to acquire credit cards or even a passport. Or they can steal your credit card numbers and use them to purchase things online. And you may not even know you've been a victim of ID theft until you start getting credit card bills for things you know you didn't buy.
2. Krystal Merton explains that criminals can follow your social media posts and use them to extract information that will help them answer the security questions on your online accounts, such as your birthplace or your mother's maiden name.

**Academic listening skill**

**Min-lecture**

Watch the mini-lecture and learn about the skill of recognizing citations.



You can watch the video on Ucampus.

**Task 1 Listen to the first half of *Protect yourself online* and complete each of the quotations with no more than two words.**

1. According to the agency that's responsible for consumer protection, people between the ages of 18 and 24 are the most likely targets of identity theft.
2. The government defines it like this on its website, and I quote: "Identity theft is a crime where a thief steals your personal information, such as your full name or your social security number, to commit fraud."
3. In addition, the well-known consumer protection organization Consumer Reports explained in a 2016 article that identity theft can be either low- or high-tech.



### Scripts:

#### Part of *Protect yourself online*

Good afternoon everyone and welcome to today's session on cybersecurity. Our goal in this session is to make sure you and your data are protected against people who would like to harm you or your electronic devices. Our main focus will be a discussion on identity theft, and how to prevent it. This is an important topic for college students because the government agency that's responsible for consumer protection, people between the ages of 18 and 24 are the most likely targets of identity theft.

All right, now to begin, what is identity theft? The government defines it like this on its website, and I quote: "Identity theft is a crime where a thief steals your personal information, such as your full name or your social security number, to commit fraud." In addition, the well-known consumer protection organization Consumer Reports explained in a 2016 article that identity theft can be either low- or high-tech. Low-tech theft can happen when a thief looks over your shoulder while you're typing in your personal identification number at an ATM. This is called "shoulder surfing." High-tech ID theft happens when a thief hacks into your computer or your phone. Then, for example, they can steal your social security number and use it to acquire credit cards or even a passport. Or they can steal your credit card numbers and use them to purchase things online. And you may not even know you've been a victim of ID theft until you start getting credit card bills for things you know you didn't buy.

I'm not trying to worry you, and of course the bank will compensate you for any money that is stolen from your account. However, it can be a horrible experience to try to recover your identification once it's been stolen. So, now let's talk about steps you can take to protect yourself and make sure your identity is secure.

#### Task 2 Listen to the second half of *Protect yourself online*. Match the cited information (1–3) with their sources (A–C).

A. Krystal Merton   B. Conrad Stewart   C. Keeper

- C   1. Almost one-fifth of people use the same password "123456."
- A   2. Criminals can extract information from your social media accounts to help them answer the security questions on your online accounts.
- B   3. Criminals take advantage of students who share, or trust more than they should on social media sites.

### Scripts:

#### Part of *Protect yourself online*

Step 1: Protect your numbers! Never share your personal or financial information with anyone. Don't carry your social security card in your wallet, and never give your credit card to anyone else to use.

OK, Step 2, be aware of phishing requests. Phishing, spelled p-h-i-s-h-i-n-g, is when you get an email or text that looks like it's from a company you know, such as your bank or credit card company, asking you to provide your account number or credit card information. These are fake emails sent by criminals whose motive is to try to trick you into giving them your personal details. Remember, an honest company will never ask you to give out that type of information. If you think there is something odd about an email or text, don't reply, and don't click on any links within the message either because they could contain malware.

Now, Step 3. Create strong passwords and update them regularly, both on your computer and on your phone. And avoid common passwords like your birth date or your school name. Most people are not very careful about this. The password manager company called Keeper reported on its website that almost one-fifth of people use the same password! Can you guess what it is? “123456”! Using a password that is so easy to guess will expose you to cyber-attack, so if that’s your password, I advise you to change it immediately. Use a combination of numbers and letters, and try to use uppercase and lowercase letters if possible.

Next, Step 4. Be careful about what you share on social media sites. A lot of students practically live on social media sites and a lot of them give away too much information too easily. Krystal Merton, the Security Manager at Pennbrook University, explains that criminals can follow your social media posts and use them to extract information that will help them answer the security questions on your online accounts, such as your birthplace or your mother’s maiden name. This is supported by Conrad Stewart, director of student services at the Mayweather Institute in New York. Stewart says, “Criminals exploit students that over-share and over-trust on social media sites.” So be careful what you share, and check your privacy settings to make sure only the people you choose are allowed to see what you post on social media.

Finally, Step 5. Protect your computer by installing anti-virus software. This prevents hackers from breaking into your computer or phone and stealing your information. The university provides this kind of software free to all its students and staff, so if you need help installing it just call or bring your device in to the campus computer center.

All right, before we go any further I want to remind you that identity theft is a criminal offense. It is illegal in most countries around the world. The punishment for identity theft includes both jail time and fines. The trouble is that a lot of thieves are very clever, and it is getting harder and harder to catch them.

That’s why it’s so important to follow the security measures I’ve been talking about. And if you think you have been a victim of identity theft, be sure to contact the university computer center immediately.



## Teaching suggestions

### Close listening

- 1 Ask Ss to read the two questions in Task 2. Then play the audio. Ask Ss to take notes while listening.
- 2 Ask Ss to work in pairs. Ss take turns to answer the questions.
- 3 After the discussion, T invites 1 or 2 Ss to share their answers with the whole class. T gives comments on the Ss’ answers.

### Academic listening skill

- 1 Ask Ss to tell the types of quotations according to what they have learned in the mini-lecture about recognizing citations.
- 2 Ask Ss to classify the following examples into A) direct quotation, B) indirect quotation, and C) no quotation:

- 1) According to the Collins dictionary, “plagiarism is the practice of using or copying someone else’s idea or work and pretending that you thought of it or created it.”
- 2) In 2014, U.S. Senator John Walsh was forced to withdraw from an election when it was discovered that he plagiarized his final paper while earning his master’s degree at the United States Army War College.
- 3) Lorenza Shabe believes that an accusation of plagiarism can severely damage your reputation and it could result in the loss of research funding and even your position, so it has both short- and long-term consequences for your research career.

**Answers:**

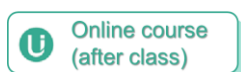
1) A; 2) C; 3) B

- 3 Ask Ss to explain why speakers cite information to support their arguments based on what they learned in the mini-lecture.

Ss’ answers may be:

Speakers cite information to make their arguments more convincing, arouse the audience’s empathy and to increase the rationality of their reasoning process.

- 4 T invites 1 or 2 Ss to share their answers with the whole class. Finally, T gives comments on the Ss’ answers.



**Oral practice**

**Task 1** The following sentences will help you talk about identity protection. Translate the Chinese in brackets into English using the words and expressions you’ve just learned, and then record each sentence.

1. This is an important topic for college students because, according to the government agency that’s responsible for consumer protection (消费者保护), people between the ages of 18 and 24 are the most likely targets of identity theft (身份盗窃).
2. These are fake emails sent by criminals whose motive (动机) is to try to trick (欺骗) you into giving them your personal details.
3. Create strong passwords and update (更新) them regularly, both on your computer and on your phone. And avoid (避免) common passwords like your birth date or your school name.
4. Using a password that is so easy to guess will expose (使……暴露于) you to cyber-attack, so if that’s your password, I advise you to change it immediately. Use a combination (组合) of numbers and letters, and try to use uppercase and lowercase letters if possible.

**Task 2** Read the following paragraph and record it. Pay special attention to the underlined words or phrases that indicate quotations.

All right, now to begin, what is identity theft? The government defines it like this on its website, and I quote: “Identity theft is a crime where a thief steals your personal information, such as your full name or your social security number, to commit fraud.” In addition, the well-known consumer protection organization Consumer Reports explained in a 2016 article that identity theft can be either low- or high-tech. Low-tech theft can happen when a thief looks over your shoulder while you’re typing in your personal identification number at an ATM. This is called “shoulder surfing.” High-tech ID theft happens when a thief hacks into your computer or your phone.

## Critical thinking

### Getting the skill



#### Teaching suggestions

- 1 Ask Ss to work in pairs to answer the questions in Task 1. Ask volunteers to share their answers with the class.
- 2 Check Ss' answers in Task 2. Encourage them to explain why some sources are reliable while others are not.
- 3 Ss work in groups to discuss the questions in Task 3. This exercise is to check Ss' understanding and application of the critical thinking skill of evaluating source reliability.
- 4 T invites 1 or 2 Ss to share their answers with the whole class. Finally, T gives comments on the Ss' answers.

#### Reference answers

##### Task 1

Reliable sources mean sources that provide information you can trust. For example, if certain information on biology is provided by a biologist, then this source of information may be considered reliable.

The reliability of a source may be evaluated in these aspects:

- 1) Authority. The author should be an expert and provide the information by following the professional standard in their own field. If the information comes from an organization, the organization should be reputable.
- 2) Date of publication. The information shouldn't be outdated.
- 3) Objectivity. The information shouldn't be biased or provided for a particular purpose.

##### Task 2

Open-ended.

##### Task 3

1. The sources included are: common sense, personal blogs, university publications, a legal document, and a well-known newspaper. I think university publications and the legal documents are reliable sources, while the rest could be subjective and unverifiable.
2. Common sense or personal blogs are anecdotal and are based on personal accounts rather than facts or research. These types of sources are not necessarily true or reliable. They should be used together with fact-based evidence.

The citation of the columnist could be reliable if the names of the columnist and the newspaper are provided. In this way, readers or listeners can judge their credibility based on their reputation and expertise.

3. Reliable sources like the legal document or university publications can strengthen the arguments, while subjective evidence does not help to strengthen the arguments.

## A cross-cultural view



### Cybersecurity

**Host:** Hello, everyone! We're here today to talk to Dr. Zhang Hua, an expert in cybersecurity. Welcome, Dr. Zhang.

*(Applause)*

**Zhang:** Thank you.

**Host:** Thank you for coming, Dr. Zhang. Would you like to give a few opening remarks? Then we'll move on to some questions.

**Zhang:** OK. Today our talk is about cybersecurity. The emergence of digital technologies has reshaped our life, but it also leads to new security risks. If you have specific questions concerning this issue, feel free to ask.

**Student A:** Hi, Dr. Zhang. My email box has been hacked, and some of my friends had their social media accounts stolen or their game accounts hacked. Are we just unlucky or is this becoming a common problem?

**Zhang:** It's indeed a common and serious problem. Not just individuals like you are affected, large organizations also face security threats. In the first half of 2020, the China National Vulnerability Database of Information Security collected 11,073 system security vulnerabilities. That's an increase of 89% over the same period in 2019. Serious data breach incidents occur frequently. Facing these threats, our country has been comprehensively improving its ability to safeguard cybersecurity, especially for critical infrastructure like banks, energy companies and telecommunications firms. Moreover, the government has introduced the Cybersecurity Law of the People's Republic of China to criminalize activities such as computer hacking.

**Student B:** Hi, Dr. Zhang. I think what worries people is not only the theft of digital accounts, but also the abuse of big data, such as personalized pricing based on personal information. Are there any regulations for it?

**Zhang:** We do have laws protecting personal information. According to Chapter VI, Article 1038 of the Civil Code of the People's Republic of China, information processors are forbidden to disclose or tamper with the personal information that they collect and store. They may not illegally provide such information to others without consent.

**Student C:** That's good to know. But I heard some cybercrimes were carried out through overseas servers, therefore harder to trace.

**Zhang:** You are right. Cybercrime is rampant worldwide. Cyber-attacks and data fraud or theft now rank among the top five global risks, according to The Global Risks Report 2019 published by the World Economic Forum. That is why we need effective global digital governance in today's closely-connected world, in order to safeguard national security, public interests and the rights of all countries.

**Student D:** What role does China play in global digital governance these days?

**Zhang:** An important role. China proposed the Global Initiative on Data Security in September 2020. It is committed to an open, fair and non-discriminatory business environment, and opposes using information technology in ways that damage critical information infrastructure. Stealing important data from other countries, or illegally collecting personal information would be prevented. This initiative reflects China's determination and sincerity to work with all countries to safeguard global digital security.

**Host:** Thank you, Dr. Zhang. It's hopeful to see that the global community has realized the importance of this

issue, and has taken collaborative action. Please join me in thanking Dr. Zhang for sharing his knowledge with us.

(Applause)

### Words and expressions

cybersecurity *n.* 网络安全

vulnerability *n.* [计算机]漏洞

breach *n.* 泄密

criminalize *v.* 立法禁止, 使不合法

disclose *v.* 透露, 揭露, 泄露

tamper *v.* 擅自改动

server *n.* (计算机网络中的) 服务器

rampant *adj.* (犯罪、疾病等) 猖獗的, 泛滥的

governance *n.* 统治, 管理

### Proper names

China National Vulnerability Database of Information Security 中国国家信息安全漏洞库

Civil Code of the People's Republic of China 《中华人民共和国民法典》

The Global Risks Report 2019 《2019 年全球风险报告》

World Economic Forum 世界经济论坛

Global Initiative on Data Security 《全球数据安全倡议》



### Teaching suggestions

- 1 Check Ss' answers in Task 1. Play the video for the class. Pause the video where Ss made most mistakes and guide them to give the correct answers.
- 2 Ask Ss to work in groups to discuss the questions in Task 2. When they are ready, ask volunteers to share their ideas with the class.
- 3 Ask Ss to work in groups to finish Task 3 by following the steps in the exercise. Pay particular attention to Step 2. If Ss have difficulties in finding information, T can provide some material from *China Daily* or CGTN for their reference. T invites 1 or 2 Ss to share their answers with the whole class and gives comments on the Ss' answers.

### Reference answers

#### Task 1

1. False
2. False
3. False
4. True
5. True

## Task 2

1. In the first half of 2020, the China National Vulnerability Database of Information Security collected 11,073 system security vulnerabilities, an increase of 89% over the same period in 2019.
2. China has been comprehensively improving its ability to safeguard cybersecurity and has established a security system for critical information infrastructure, implemented the Cybersecurity Law, and put forward regulations on the collection and use of personal information.
3. The initiative reflects China's determination and sincerity to work with all countries to safeguard global digital security.

## Task 3

### Evaluation and reasons:

I would probably choose to quote statements 1, 2, and 4, because they all have well-accepted sources of information, such as China National Vulnerability Database of Information Security, The Civil Code of the People's Republic of China and the World Economic Forum. What's more, all the information is released in recent years. Statement 3 is just based on personal observation and is not very reliable or authoritative.

### Revision of Statement 3:

Big companies can abuse the big data of their customers. For example, China Daily reported nowadays the case of some mobile apps for abusing personal information without users' consent, which violates their privacy.

## Academic communication



## Speaking model

**Read the conversation about a cybercrime case, and then answer the following questions.**

**Professor:** Morning, class! Could someone review the case for me? What was it about?

**Luis:** OK, so this student who failed several courses hacked into the university database, and changed three of his grades from Fs to As. However, he made a mistake, and university staff were able to connect the break-in to his account. He was arrested, and sentenced to 200 hours of community service. He was also kicked out of the university.

**Professor:** Thank you, Luis. So, what do you think about the punishment? Anyone?

**Felicity:** I think the sentence was much too light. At his trial, he admitted knowing it was wrong to hack into the database. He even said, and I quote, "It was easier to change my grades than to go to class and work hard." I think he should have been sentenced to at least six months in jail, plus a fine.

**Professor:** OK. So Felicity said the sentence was much too light because this student knowingly committed the crime. Who agrees or disagrees with Felicity?

**Al:** I understand what Felicity is saying, but I disagree with her about the sentence. He was only 18 years old. It was his first semester, and he was having a lot of trouble adjusting to college. Plus, he was under a lot of pressure from his parents to do well. I know, that's not an excuse for hacking, but it shows the kind of stress he was under. I strongly believe jail is the wrong punishment for this type of crime. Community service seems about right. He could spend that time teaching kids and senior citizens how to use computers – legally!

**Professor:** All right, thank you, Al. So Al believes this student was under stress and a lighter sentence could have ended up in better results. Anyone wants to disagree?

**Luis:** Yes, I believe what Al said is reasonable in a sense, but I personally think this kind of behavior might deserve heavier punishment so that others who have a similar attempt could be deterred in the future.

1. What crime did the student commit? What reason(s) did he give?
2. What punishment did the student receive?
3. What is Felicity's opinion on the punishment? What reason(s) does she give?
4. Why does Al say "I understand what Felicity is saying ..." before disagreeing?

**Reference answers:**

1. He hacked into his university's database and changed three of his grades from Fs to As. He said it was easier to do this than to go to class and work hard.
2. He had to do 200 hours of community service and was expelled from the university.
3. She thinks the sentence was much too light because he knew it was wrong to hack into the database.
4. He wants to make his disagreement sound more polite.

## Speaking skill



You can watch the video on Ucampus.

### Mini-lecture

Watch the mini-lecture and learn about the skills of disagreeing politely in a discussion.

### Oral practice

**Task 1** The following sentences will help you talk about crime punishment. Translate the Chinese in brackets into English using the words you've just learned, and then record each sentence.

1. Could someone review (回顾) the case for me? What was it about?
2. He was arrested (逮捕), and sentenced (判决) to 200 hours of community service.
3. I think the sentence was much too light. At his trial (审判), he admitted (承认) knowing it was wrong to hack into the database.
4. I think he should have been sentenced to at least six months in jail (监狱), plus a fine (罚款).
5. I strongly believe jail is the wrong punishment (惩罚) for this type of crime (犯罪).

**Task 2** You will hear two clips of the conversation. Each clip will be played only ONCE. After you hear a tone, please repeat the exact words the second speaker has said. You may take some notes while you listen.

1.

**Professor:** OK. So Felicity said the sentence was much too light because this student knowingly committed the crime. Who agrees or disagrees with Felicity?

**Al:** I understand what Felicity is saying, but I disagree with her about the sentence.

2.

**Professor:** All right, thank you, Al. So Al believes this student was under stress and a lighter sentence could have ended up in better results. Anyone wants to disagree?

**Luis:** Yes, I believe what Al said is reasonable in a sense, but I personally think this kind of behavior might deserve heavier punishment.



**Task 3** Now it's your time to role-play the discussion. Firstly, choose the way you want to do the task. You can click on **Scripts** to role-play it, or you can do a more challenging task by clicking on **Hints** to role-play it according to the hints in Chinese. Then choose the role you want to play.

**Professor:** Morning, class! Could someone review the case for me? What was it about?

(提问, 问是否有人愿意复述案情。)

**Luis:** OK, so this student who failed several courses hacked into the university database, and changed three of his grades from Fs to As. However, he made a mistake, and university staff were able to connect the break-in to his account. He was arrested, and sentenced to 200 hours of community service. He was also kicked out of the university.

(简要复述该学生的犯罪事实, 因几门课考试不及格而入侵大学的数据库, 并将三门课的成绩从 F 改为 A。但是他在入侵过程中出了差错, 使得学校能够追踪到他的账号。他被逮捕, 并被判处做 200 小时的社区服务。并且他被学校开除了。)

**Professor:** Thank you, Luis. So, what do you think about the punishment? Anyone?

(继续追问他人对量刑的看法。)

**Felicity:** I think the sentence was much too light. At his trial, he admitted knowing it was wrong to hack into the database. He even said, and I quote, "It was easier to change my grades than to go to class, and work hard." I think he should have been sentenced to at least six months in jail, plus a fine.

(提出量刑太轻, 因为他明知故犯。引用该生原话, 说他认为改成绩比上课和用功学习更轻松。认为应该判处至少六个月监禁, 附带罚款。)

**Professor:** OK. So Felicity said the sentence was much too light because this student knowingly committed the crime. Who agrees or disagrees with Felicity?

(转述、总结上一位讲话人的意见, 询问他人是否有其他意见。)

**Al:** I understand what Felicity is saying, but I disagree with her about the sentence. He was only 18 years old. It was his first semester, and he was having a lot of trouble adjusting to college. Plus, he was under a lot of pressure from his parents to do well. I know, that's not an excuse for hacking, but it shows the kind of stress he was under. I strongly believe jail is the wrong punishment for this type of crime. Community service seems about right. He could spend that time teaching kids and senior citizens how to use computers – legally!

(表示理解前一位讲话人的观点, 但不赞同。指出该生年仅 18 岁, 刚上大学还不适应, 且他面临来自父母的压力。虽然这不是入侵学校数据库的理由, 但能说明他承受的压力。强烈认为监禁不适用于此类犯罪, 社区服务则很适合, 他可以教孩子和老人使用电脑, 而且是以合法的方式使用。)

**Professor:** All right, thank you Al. So Al believes this student was under stress and a lighter sentence could have ended up in better results. Anyone wants to disagree?

(转述上一位讲话人的意见, 询问有无反对意见。)

**Luis:** Yes, I believe what Al said is reasonable in a sense, but I personally think this kind of behavior might deserve heavier punishment so that others who have a similar attempt could be deterred in the future.

(表示有一定道理, 但个人认为这种行为需要加重处罚才能起到威慑作用。)



## Teaching suggestions

### Speaking model

- 1 Introduce the objectives of Academic communication.
- 2 Ask Ss to work in pairs to discuss the questions.
- 3 When they are ready, ask volunteers to share their answers briefly with the class.

## Speaking skill

Comment on Ss' online performance.

### Alternative activity

- 1 Ask Ss to read the speaking model and find examples of disagreeing politely.

Ss' answers may be:

Acknowledge the other speaker's point of view, and make it clear that you understand it. Then state your own position:

- I understand what Felicity is saying, but I disagree with her about the sentence.
- Yes, I believe what Al said is reasonable in a sense, ...
- I know, that's not an excuse for hacking, but it shows the kind of stress he was under.

Acknowledge that your opinion is yours alone:

- I think the sentence was much too light.
- I think he should have been sentenced to ...
- ... but I personally think this kind of behavior might deserve heavier punishment ...

Use hedge words

- I personally think this kind of behaviour might deserve heavier punishment so that others who have a similar attempt could be deterred in the future.

- 2 Go through the answers with the class.
- 3 T invites 1 or 2 Ss to share answers with the whole class.
- 4 Comment on the Ss' answers.

### Skill enhancement

- 1 Ask Ss to read the instructions and work in pairs to present their ideas. Encourage Ss to use the speaking skill.
- 2 Walk around the class and help the Ss who have difficulty with the task.

### Extension activity

- 1 Ask Ss to discuss in pairs why the skill of disagreeing politely is important.
- 2 When they are ready, ask volunteers to share their answers briefly with the class.

Ss' answers may be:

Disagreeing politely lessens the aggressiveness and offensiveness and makes one's opinion more likely accepted emotionally.

- 3 Comment on the Ss' answers.

## Speaking task

### Brainstorm

- 1 Ask Ss to work in groups, read the case study and think about the questions.
- 2 Guide Ss to analyze the material and underline the specific parts for the "crime," "punishment" and "reason."
- 3 Walk around and help any students who are struggling to understand the case study.
- 4 When they are ready, invite 1 or 2 Ss to give their answers and comment on them.

### Plan

- 1 Allow plenty of time for this stage. Ask Ss to form two pairs in each group. Each pair takes a side. Remind Ss to notice that theoretically there might be two possibilities on the disagreeing side, for example, the punishment is too heavy or too light. But in this case, few people would think Sean Thomas deserves a more severe punishment than the current one (\$185,000 and three years in prison), so the disagreeing side would generally defend for him and think the punishment should be lighter.
- 2 Ask Ss to make a list of four or five supporting ideas. Guide Ss to consider the background of the event, the influence on individuals and the industry, the effect of the punishment on his education, justice to the society, etc.
- 3 Ask Ss to choose from the quotations on Page 91 or use their own sources of quotation if they have any. Remind the Ss that the quotations they use should well support their claims in logic.
- 4 Monitor carefully to ensure all groups are making good progress.

### Speak

- 1 Ask Ss to work within their groups to conduct their debates. Remind Ss to record their debates.
- 2 Remind Ss to pay attention to not only the sentence structures but also the intonation and body gestures they use.

### Share

- 1 Ask each group's representative to report their debate results.
- 2 Comment on each group's performance.

### Reflect

- 1 Ask Ss to evaluate their performance by answering the listed question.

**2** Ask Ss to upload their recording online after class.

- ✧ With weaker classes, lead Ss to analyze the case in step 1 and ask Ss to decide which side in step 2 they want to take. Guide Ss to read the quotations on Page 91 and choose the ones that can best support their standpoints. Then invite 2-3 Ss from each side to present their arguments by using the quotations.

## Unit review



### Vocabulary

- ☐ I can use the words and expressions about cybersecurity.

### Listening

- ☐ I can listen for supporting evidence.  
☐ I can recognize citations.

### Speaking

- ☐ I can disagree politely.

### Critical thinking

- ☐ I can evaluate source reliability.