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）