APSS – Online classes

Activity 8

Description

Materials	Workbook. Module 3. 3.2 Language functions Giving Advice
Learning objectives	Using the correct kind of language for different communicative functions in English
Method and objectives	Answer Key / self- correcting + submission
Assesment	Self-assessment and teacher’s assessment

To - do

- To revise expressions for giving advice:
  - Complete the dialogue (p.60).
    - These exercises are self-correcting (I'll post the key).
    - Answers are open in most cases.
    - Just try one that makes sense in the conversation.
  - Read the list of expressions carefully (p.62)
  - Submit the folllowing task: Speaking Activity 3. Role Play (p.63).
    - In pairs
    - Helping users to protect their computer.
    - Choose a computer threat in the list.
    - Use the promts in a) to make up a short dialogue saying what the danger is and giving advice on how to prevent it.
    - Record the dialogue (no more than 2 minutes).

3. Giving advice and recommendations

[to-do item] Complete the dialogue (p.60).

The following dialogue deals with some advice on how users can protect their computer from viruses and other related problems. Read the situation described in the box and then look at the dialogue. Some parts are missing. Try to complete them with a partner. Then listen to the dialogue and check your answers.

> Mike and Dan are two university students in the computer lab. They’re trying to finish their course project. Dan starts to have problems with his file, which may have been infected by a computer virus, and Mike tries to help him. Dan doesn’t know much about computers and Mike is almost an “expert”.

D: How’s your project going?

M: I’m almost finished. Never thought it’d take so long. What about you?

D: I’ve still got some work to do. I hope I can hand it in by the deadline... Oops!

M: Oops? What’s going on?

D: I don’t know what’s happened with my file. I keep getting odd messages. And my work is in a very weird format.

M: Let me see…uh-uh.

D: What happened?

M: I think your file may be infected by a virus.

D: How is that possible?

M: Do you use an antivirus program?

D: I don’t need one. I never share files with anyone else. And I only connect to the college network. It’s very secure.

M: Well, most viruses enter through the network. Everyone uses it. And through email, of course. You should be very careful.

D: What should I do?

M: First of all, I think you should update your computer.

D: Update it?

M: Of course. It’ll be of no use if it can’t recognize the latest viruses. And new viruses appear every day.

D: I received some mails telling me I have a virus and must click a button to remove them.

M: Don’t trust them, please. They’re hoaxes!

D: Hoaxes?

M: A computer virus hoax is a message warning the recipients of a non-existent computer virus threat. It is usually a chain e-mail that tells the recipients to forward it to everyone they know. But it can get worse.

D: Worse?

M: ...some of them tell you to erase important files of your operating system or they can be Trojans.

D: Trojans?

M: Yeah. Trojan horses. Apparently harmless files that enter your computer, but in fact they can be viruses in a disguise. Very dangerous.

D: What should I do to avoid them?

M: Don’t trust any messages warning you about viruses. And don’t open any attachments from people you don’t know. Also be careful when downloading files from the Internet. Especially executable files, programs, from certain sources.

D: How do I know?

M: Maybe you could get a virus scanner.

D: A virus scanner?

M: A program that searches for viruses in your files. Some internet applications also do that. If they find a virus, you should then use an antivirus program to clean the file.

D: So if I have one virus scanner, my computer would less likely to be attacked?
M: That’s right. That’s why prevention is so important. You should have backup copies of your important data, keep your antivirus updated…
D: So that I don’t have to worry about opening files and messages.
M: Exactly, you should do some things to protect your computer.
D: Like?
M: An antivirus program, of course, and a copy of it on a disk. Backup copies of important files. And an external disk to reboot, that is restart, your computer, in case your operating system is damaged. At the computer center they’ll give you specific advice, follow it. You should be, I’d say, a bit paranoid about security.
D: Paranoid?
M: The more paranoid you are, the more secure your computer will be.

Word file: Asking for and giving advice

[to-do item] Read the list of expressions carefully (p.62)

There are other ways of asking for and giving advice, ranging from formal to informal:

Asking for advice

+ Formal

- was wondering if you could advise me on...? / about...?
- I was wondering if you could give me some advice on...? / about...?

- Can/Could you advise me on…?/ …about?
- Can/Could you give me some advice on…?/ …about?

- What would you do in my position? / if you were me?
- What do you reckon / think / believe I should do?

- What should I do?

+ Informal

Giving advice

+ Formal

- I was wondering if you’d ever thought of...
- I think your best course would be to do...
- I’d advise you to do...
- Might it be an idea to...
- You might (like to) try...
- You could consider...
- If I were you, I’d do...
- I suggest you do...
- Have you ever thought of...?
- Don’t you think it might be an idea to...?
- I think you ought to ... should ...
- I think you’d better....
- You’d better...
- Why don’t you ....?

+ Informal

Speaking Activity 3.

[to-do item] Submit the folllowing task: Speaking Activity 3. Role Play (p.63).

- *In pairs*
- *Helping users to protect their computer.*
- *Choose a computer threat in the list.*
- *Use the promts in a) to make up a short dialogue saying what the danger is and giving advice on how to prevent it.*
- *Record the dialogue (no more than 2 minutes).*

Helping users to protect their computer / to purchase an appropriate laptop.

a) Below is a list of common problems users may encounter if they are not careful. Do you know what they refer to? Get together with other partners and discuss them using the following prompts.
   a) Go through the different examples of risky uses of computers and make sure you understand what they mean.
   b) In what ways do they pose a threat to safe computing? What dangerous consequences may they have?
   c) How can users identify or prevent these problems? What advice can you give to other users?

COMPUTER SECURITY THREATS:

Phishing *“Phishing” or email messages requesting you personal information such as bank account number, etc.*	
What they mean	Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication. Typically carried out by email spoofing or instant messaging, it often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site.
Ways they pose a threat to safe computing?	Almost all types of phishing attacks can be broadly divided into two categories: • Tricking users: this involves directly tricking the user to pass on sensitive information via spoof sites • Installing Malware
Dangerous concequences they may have	Sensitive information such as personal details, bank account information, credit card details etc. can be stealed. This information is then used for a variety of purposes ranging from identity theft, fraudulently obtaining funds, crippling down computer systems through to securing trade secrets or even sensitive information pertaining to national security.
How can users can identify/ prevent these problems?	This requires a generous application of common sense and caution, and a solid awareness about come phishing patterns.
Advice you can give to other users	Tips on how to spot a phishing email: • Poor grammar, punctuation and just plain tacky language • Emails soliciting personal information • Alarming content • Urgent deadlines • Unrealistic financial rewards • Mismatched URLs • Mis-matched domain name

Careless use of passwords	
What they mean	Use an easy-to-guess password and use it in many different places.
Ways they pose a threat to safe computing?	Criminals can access your accounts very easily and they can steal the information you have in those accounts, apart from everything they offer.
Dangerous concequences they may have	Same as threats.
How can users can identify/ prevent these problems?	• Passwords may not contain the Account Name value • Have: • Uppercase letters • Lowercase letters • Base 10 digits (0 through 9) • Non-alphanumeric characters
Advice you can give to other users	Use different passwords for different accounts.

Opening non-reliable attachments	
What they mean	Open and/or execute files the origin of which is unclear.
Ways they pose a threat to safe computing?	Most computer viruses are spread via email attachments. This does not come as a surprise, since email became one of the most used means of communication in the last decades. It just takes seconds to make appointments, to send files or to communicate anything, whether it is personal or business related. But, it also only takes those few seconds to cause a lot of damage.
Dangerous concequences they may have	It can be a trojan.
How can users can identify/ prevent these problems?	If you consider these three main rules, you can feel much safer in your daily email communication. • Antivirus Program: An antivirus program, which updates regularly and automatically, recognizes some viruses and helps you detect problems. However, many malware just passes such programs, especially when the viruses or trojans are new and yet unknown to those programs. • Talk to the sender: To protect yourself if that program fails, you should always make sure that the attachment really came from the person or institution who seemingly sent it. • Knowledge: It is helpful to be aware of some facts about file types and their extensions; which ones are more dangerous than others?
Advice you can give to other users	Make sure you can trust the origin of the attachment

Spyware *Allowing spyware into your computer (by downloading programs, exchanging movies and music files, etc.)*	
What they mean	Spyware is a type of malware that aims to gather information about a person or organization, without their knowledge, and send such information to hack another entity without the consumer's consent. Furthermore, spyware asserts control over a device without the consumer's knowledge, sending confidential information to another entity with the consumer's consent, through cookies.
Ways they pose a thread to safe computing?	Spyware can cause you two main problems. First, and perhaps most importantly, it can steal personal information that can be used for identity theft. The second, and more common, problem is the damage spyware can do to your computer. Spyware can take up an enormous amount of your computer's resources, making it run slowly, lag in between applications or while online, frequent system crashes or freezes and even overheat your computer causing permanent damage.
Dangerous concequences they may have	Same as threats.
How can users can identify/ prevent these problems?	The best way to control spyware is by preventing it from getting on your computer in the first place, but not downloading programs and never clicking on email attachments isn't always an option. Sometimes, even a trusted website can become compromised and infect your computer — even if you've done nothing wrong. Many people are turning to internet security solutions with reliable antivirus detection capabilities and proactive protection.
Advice you can give to other users	Get a good and paid antivirus.

Pirated software	
What they mean	Copyright infringement is the use of works protected by copyright law without permission for a usage where such permission is required, thereby infringing certain exclusive rights granted to the copyright holder, such as the right to reproduce, distribute, display or perform the protected work, or to make derivative works.
Ways they pose a thread to safe computing?	The first risk that you run is infecting your PC. The second risk is the program not actually working.
Dangerous concequences they may have	Same as threats.
How can users can identify/ prevent these problems?	Just don’t pirate.

Pirated software	
Advice you can give to other users	Go for an alternative software: Find an alternative software that solves your needs for free! A competitor app may want to pick up users by offering premium features from your original choice of software for free.

Updates *Not having an updated antivirus program and a firewall*	
What they mean	Not having an updated antivirus program and a firewall.
Ways they pose a threat to safe computing?	Some new security patches will not be installed and your computer will be more exposed to possible attacks.
Dangerous concequences they may have	Same as threats.
How can users can identify/ prevent these problems?	Make constant updates.
Advice you can give to other users	Same as above.

Phishing script:

I: Hey Júlia! Long time no see.
J: Hello Isma. I couldn’t agree more. We haven't seen each other for many months.
I: So, how's it going? Anything new?
J: I don't have much to tell you. Oh wait, there’s some gossip I can tell you. Last week one of my colleagues suffered a phishing attack.
I: Phishing attack? What is it?
J: Phishing attacks typically consist of an email designed to pose as a trusted provider, a well-known institution, or even a trusted co-worker or manager. It invites you to click on a malicious link, log into a fake website, or download an incorrect attachment.
I: Wow! And what can happen if someone suffers one of these attacks?
J: Mostly, confidential information such as personal data or bank account information may be stolen. This information is then used for identity theft, fraudulently obtaining funds, and more.
I: And what should I do if I want to prevent me from suffering a phishing attack?
J: There are some properties that phishing emails have in common. If I were you, I’d be aware if: • If the email has poor grammar, punctuation and just plain tacky language • If it requests personal information • If it has alarming content • If it shows urgent deadlines • If it has unrealistic financial rewards • Or if the link ot domain name are mismatched
I: Now that I think about it, you may have received an email with these properties. From now on, I am going to pay more attention to avoid phishing attacks. Thank you very much for your advice Júlia!
J: Glad to help!