APSS – Online classes

Activity 4

Description

MATERIALS	Workbook. Module 2. **Listening 8** (video). Computer Security and Computer Crime
LEARNING OBJECTIVES	Applying listening strategies for comprehension. Comprehension and debate.
METHOD AND OBJECTIVES	Answer Key / self- correcting + submission
ASSESMENT	Self- assessment and teacher's assessment

Listening 8: Computer Security and Computer Crime

VIDEO: HTTP://WWW.ARCHIVE.ORG/MOVIES/THUMBNAILS.PHP?IDENTIFIER=PREVENTI2002
VIDEO: HTTP://WWW.ARCHIVE.ORG/DETAILS/SECURITY2001

Part 1 - Computer security

Activity 1

Read and answer the following question by discussing with your partners.

> *Computers have attracted the interest of some highly skilled people who have tried to use them to break into unauthorised systems, corrupt data, steal money and do all sorts of illegal activities. Computer crime is different but not less dangerous than other types of crimes. It has been along since computers started to be widely used in businesses and it grew considerably with the advent of the Internet. It is almost impossible to be completely safe.*

- Do you agree with the assumptions stated above?

Computer crime and abuse represents one of the undesirable, but ultimately inevitable, consequences of the IT and communications revolution.

- Give examples of security attacks and risks users face today.
  - Computer virus:
    - Computer viruses are pieces of software that are designed to be spread from one computer to another.
    - They're often sent as email attachments or downloaded from specific websites with the intent to infect your computer by using systems on the network.
    - Viruses are known to send spam, disable security settings, corrupt and steal data from your computer including personal information such as passwords, even going as far as to delete everything on the hard drive.

  - Phishing
    - Phishing is a method of a social engineering with the goal of obtaining sensitive data such as passwords, usernames, credit card numbers.
    - The attacks often come in the form of instant messages or phishing emails designed to appear legitimate.
    - The recipient of the email is then tricked into opening a malicious link, which leads to the installation of malware on the recipient's computer.
    - It can also obtain personal information by sending an email that appears to be sent from a bank, asking to verify the identity by giving away the private information.

- In the case of a security attack, who is responsible: the computer security expert, the hacker, the user?

I think that it is the *data owner* that faces liablity for losses resulting from a data breach, even if the security failures are the fault of the *data holder (cloud provider*). Why? Standard vendor agreement contracts exclude consequential damages and cap direct damages. In most cases, all damages flowing from a data breach of the data holder will be considered consequential damages and barred by a standard provision disclaiming all liability for consequential damages.

Part 2 - Computer crime

It can get worse if you reply a spam email. When you respond to a spam email and it links you to some online store, you may not realize it, but some tools called spyware are following you.
On online shopping, your movements can be tracked your movements from website to website. They are logging everything you are looking at.
Woman: "My identity was stolen by a stranger. This person was able to open an account in my name, a credit card account, without my knowing, and was able to charge large on this account." She called her credit card company suggested that she had spent so much time online that her information could be found on the internet. (tota info com, coses de la seva mare, social security number, etc.)
A hacker could take your personal and confidential information and use it to perform identity thaft (?), charge things to your credit card, steal passwords on your machine, do things under your name, etc.

Now do the following activities dealing with major risks user face.

Now, think about computer security from the point of view of the user.
- What are the major concerns users face?

One of the majors concerns of internet users is their personal information can be stolen.
- Comment on the main risks involved in using a computer (viruses, hacking, etc.).

In our opinion, the main risk of using a computer is the ignorance. Most users cannot protect their information from themselves, in other words, they give their information indiscriminately to anyone on the internet who asks for it, assuming that there is no risk in it.
You can get together with another partner and exchange views.

Activity 1

- Have you ever had any computer security problems (viruses, hacking, etc.)?

In one occasion, someone logged in my "Origin" account (game platform) and could play with my games, such as Sims 4. All I had to do to solve it was to change my password. It is no longer "`Passw0rd!`".

- Watch the following video extract about a woman who had a computer security problem.
  - What kind of problem did she have?

Her identity was stolen by a stranger. This person was able to open an account in her name, a credit card account, without her knowing, and was able to charge a large amount of money on that account.

  - What did she do?

She called her credit card company and they said that it could probably be because the had spent so much time on the internet, giving personal information that was later stolen.

  - What else do you think she could have done?

She could have protected her computer with an antivirus before doing anything online. Using this kind of software, you can protect your personal data so it cannot be accessed remotely. Currently, this is not how security works anymore.

Part 3 - An interview: computer security and the Internet

In this interview, an expert identifies some ways in which hackers can access other people's systems or steal sensitive data through the network. Can you answer the following questions?

1. The presenter describes computer security on the Internet as a "catch-22" situation. What is the relationship between accessibility and security on an internet site?

The more secure you make your website, the harder it is to use it for normal users, and the other way around

2. What's the interviewee's job? The presenter introduces him as a "lawful hacker". What does it mean?

He works for a company protecting it from hackers. He is what is called a white hat hacker, he knows what hackers do and protects his company's systems from thier attacks.

3. The interviewee shows the "mock" bank server he has created. What does he use it for?

He uses it to show how hackers can easily get confidential data from a bank system only by changing one part of the URL with an SQL statement.

4. What are the next two examples he gives of illegal actions?

One of the examples that he gave was to access to all of the accounts of the mock he created and steal personal information. Another example was to introduce a sploit.txt file into the server to show that, if it was a malicious file, it could damage the system.

5. Does he think that giving credit card details over the Internet is especially risky for consumers?

He said that the encryption could help in securing the credit card details, but, in the end, wether you buy things on the internet or in a local store, the information is stored into a database, that could be accessed by a hacker. Also, many bank companies give insurances to prevent these kind of thieveries. So, in his opinion, it is not a bad idea to buy on the internet.