**Lesson 8 Andreu Mut Portes L1G1**

* Today’s lesson activities will be done autonomously while I call you to do the speaking practice with me.
* Do the activities on this document and upload it on POLIFORMAT – TAREAS.
* Deadline: During today’s class time

**Practice 8 – Cyber security**

**1. Listen to this talk about the ethical challenges in cyber security and answer the questions.**

1. Why is our safety at risk?

Complexity is the enemy of security. The simpler an application is, the more secure it is. It happens the opposite thing.

1. What are the different types of hackers described?

White attackers: Break security to improve security. Have ethics to consider. They report something and if you don’t fix it, they reveal it.

Criminal ones: No ethics they want money and make chaos breaking rules and laws.

Activists: The want to protest. Have some ethics

Government: as what happened in the elections in USA

1. Why are cyber weapons useful for intelligence agencies?

Because they are effective, affordable and deniable

1. What is the ethics of the attacker? What is the example he gives?

“Stacks net” They put a data limit on the application. After June 2012 It won’t work again. From 2009 to 2012 it did all the damange.

1. What is the ethics of the defender? What does his job consist in?

The speaker is an example, he works on that, he breaks into networks but with permission so they can tell how they did it.

Record a **2-MINUTE FLIPGRID** in which you summarise the content of the recording (use the answers to the questions if you want) and give your opinion on whether hackers are a need or a threat. I’ll stop you after 2 minutes.

**2. Read the text and answer the questions.**

**Most Hackers Aren’t Criminals**

Professional hackers work to keep people safe by finding security vulnerabilities before criminals do.

<https://www.nytimes.com/2019/11/07/opinion/hackers-hacking.html>

When asked what his father did for a living, my son explained to his kindergarten teacher that “he steals things, but it’s O.K. because he gets paid to do it.”

He wasn’t wrong.

I’m a hacker, and I run a team of hackers. We spend our days discovering ways to break into anything that can connect to the internet — servers, automated teller machines, light bulbs — in an attempt to access information that was never meant to be seen. If we get to it before a criminal does, then we’ve done our job.

I’m proud of what I do for a living, just like doctors or lawyers are proud of the work they do. The Texas Department of Motor Vehicles, however, recently took a critical stance on my profession. When I purchased vanity plates for my car, the agency was quick to take them away, claiming that a license plate displaying “HACKING” endorsed illegal and criminal activity.

While this reaction really isn’t the fault of the well-intentioned municipal employee who took away my license plates, it’s a symptom of how a deeply rooted misrepresentation of my profession has created flawed perceptions and stereotypes.

The way that hackers are depicted in Hollywood and by the security industry itself has contributed to the word “hacker” becoming synonymous with “criminal.” Hackers are often portrayed as hooded figures in dark rooms who are engaged in illegal activity while jabbing at keyboards and are almost always male. In recent years, television shows like “Mr. Robot” and movies like “Ocean’s 8” have introduced female characters as hackers, but the male hacker stereotype unfortunately prevails.

The stereotypes don’t apply to most hackers in the security profession. Hackers aren’t social pariahs who operate in silos and work alone. I have been a hacker for over 30 years, and I do not wear hoodies. Some hackers even choose to suit up for the job. And — spoiler alert — women hack too. Offensive security culture is innately inclusive: This is a business in which companies hire hackers to outsmart them, to find an organization’s breaking point before criminals do. Testing a company’s security and coming up with creative ways to hack into it is something that requires diverse teams and diverse mind-sets.

Back in the 1950s, the modern use of the term “hacking” was coined within the walls of the Massachusetts Institute of Technology. For many years after, a hacker was defined as someone who was an expert at programming and problem-solving with computers, who could stretch the capabilities of what computers and computer programs were originally intended to do.

Hacking is an activity, and what separates any activity from a crime is, very often, permission. People are free to drive, but they do not have permission to drive 150 miles per hour — that’s reckless driving and it’s a criminal offense. Bankers can transfer their clients’ money, but if they do so without permission, that’s embezzlement. And you’ve never heard of someone being arrested simply for being a stockbroker, because no one is charged for choosing a career in finance — but they’d be arrested if they engaged in illegal activity like insider trading.

Thanks to security researchers’ hacking practices, this year [vulnerabilities](https://www.zdnet.com/article/new-dragonblood-vulnerabilities-found-in-wifi-wpa3-standard/) in a new version of the most common Wi-Fi encryption standard (WPA3) were found before criminals could use them to break into home and business networks. Conversely, just last month criminals found [an unknown vulnerability](https://arstechnica.com/information-technology/2019/10/attackers-exploit-0day-vulnerability-that-gives-full-control-of-android-phones/) in Google’s Android operating systems before security researchers did, giving the bad guys full control of more than a dozen phone models.

Hacking isn’t an inherently criminal activity. Someone who engages in the illegal use of hacking should not be called a “bad hacker” but a “cybercriminal,” “threat actor” or “cyberattacker." Hackers are people like me and my team at IBM — security professionals who are searching for vulnerabilities, hoping to find weak links in our computer systems before criminals can exploit them.

Those who commit computer crimes fall into two categories: “black hat” and “gray hat.” A black hat is someone who hacks with malicious intentions (espionage, data theft), seeking financial or personal gain by exploiting vulnerabilities. A gray hat is someone whose intentions may not be malicious but lacks the permission to hack into a system. Whether a particular criminal is a black hat or a gray hat is simply descriptive of the motivation behind what has already been established as illegal activity.

Somewhere along the way, the security industry also recruited ethics to help justify hacking behavior, giving us “the ethical hacker” and adding an artificial defensiveness to a profession that has existed since the 1950s. Unfortunately, even accredited security certifications use the adjective in their very title. And while we can’t and shouldn’t fault the general public for referring to us as ethical hackers, I ask you this: Does it sound right to introduce someone as an ethical stockbroker? How about an ethical engineer or ethical professor?

Hackers play a critical role in keeping companies and people safe. A hacker failing to do the job right is the equivalent to letting a company believe and function as if it’s wearing a bulletproof vest when in fact, it’s wearing cashmere. At IBM, one thing my team, X-Force Red, does is hack autonomous vehicles, planes and trains to make sure that every possible security vulnerability is found and corrected before each machine is shipped. Imagine what bad things could happen if security weaknesses aren’t identified and corrected before those vehicles are out the door.

The misrepresentation of the term “hacker” not only undermines the offensive security community but also distorts legislators’ understanding and perception of hackers overall. The Computer Fraud and Abuse Act, for example, relies heavily on the term and its misinterpretation. For society to have open and productive discussions about security research and penetration testing, we need to set the record straight on who and what hackers really are. Many government officials whom I’ve spoken with understand this. Others choose to take my license plate away.

**A. Answer these questions. Use your own words as much as possible**:

1. **What is the stereotype of a hacker**?

The one that gives Hollywood and TV Shows. A criminal how is engaged in illegal activities.

1. **Why isn’t hacking a crime according to the writer**?

Because if you have permission to break into a network, it is not something illegal. And they have permission.

1. **The writers gives some examples of how hacking can help a company or society in general. Explain at least 2 examples using your own words**:

Hackers found a vulnerability on the WiFi encryption standard (WPA3)

On the other hand, crackers found a vulnerability on Android OS before Hackers did so they have control on some phone models.

1. **Explain in your own words the differences between a black hat and a grey hat**:

Black hat are the criminals, bad ones which have malicious intentions.

A grey hat hasn’t got permission to hack a system but they don’t use to have malicious intentions.

1. **Why does the writer believe the term ‘ethical hacker’ is not correct**?

Because the word “hacker” implies that he is ethical. A hacker is someone who desn’t make illegal activities.

**Speaking Topic 8**

**PART 1. Discuss these questions in groups:**



* **In your opinion, are hackers a need or a threat? Why are they necessary? Why are they dangerous? Give reasons for your opinions.**
* **What’s the difference between hackers and crackers? Explain in English.**
* **Is cracking justifiable or not? Why?**
* **If you could hack any system, what system would you like to hack? Why?**
* **Is cyber espionage justifiable? Why not / In which cases?**
* **In your opinion, is it okay to record workers at work to protect a company’s safety?**
* **In your opinion, is it okay to spy on citizens to protect a country’s safety?**
* **Do you worry about your privacy? Why / why now?**
* **Do you take measures to protect your privacy? Why not / which ones?**

Record a **5-minute** summary in which you explain your opinions and most importantly the reasons for your opinions!