ITS444- E-Commerce
Karinna Rocha
Paul Nevill

1. What metaphor does Zertag use to describe the idea that online, there are “no safe neighborhoods?” What does she mean?

2. What does Zertag mean when she says that the Internet has a “huge attack surface”? How will the “Internet of Things” exacerbate this issue?

The metaphor of "no safe neighborhoods" expresses the idea that the internet is not a safe environment and that danger exists everywhere. This metaphor shows the reality that there is always a chance of danger, no matter where one is online. It also shows how simple it is for people with bad intentions, such as trolls, bots, and hackers to invade online areas. These people have the power to create a sense of fear and threat towards all the genuine users all over the world, harming people and organizations’ capacity for unrestricted expression and free discussion. Zertag brought this idea to the table when she discussed the analogy where the cyber environments are like neighborhoods, where people like to shop, do banking, and enjoy social media, but there are also people with bad intention that like to rob, steal identities, and do bad things. On the other hand, though, different than in real life, there is no protection against people that do immoral things. There is no governmental department that would protect users, even though we do have cyber security laws. The video explains that in the internet, the logistic of protection is reversed than the real life because on the internet it can be so easy to get hacked, but it can take a long time for users to realize that this incident happened. Even though the internet opens a lot of possibilities and doors to opportunities, it also brings a lot of dangers which makes us be more careful with what we do on the internet because we can suffer attacks at any time.

On my perspective when Zertag talks about the “huge attack surface” on the Ted talk, huge attack surface is a way to express that the internet has a large amount of interconnected network devices, platforms or even systems that allow us to communicate to each other, access

intonation of run business worldwide scale, meaning that there are many possibilities for attackers to have access to the networks that is in use, causing a lot of vulnerabilities around. When the speaker talks about the amount of the devices or the Internet of things, such as laptops, desktop, bluetooth, cell phones, tablets, cars, speakers devices, any type of device that has access to the internet can be attacked somehow from the hackers, it is good to remember that we are going into a time that even medical devices that connect to our body and sends data to the doctors also can be threat. Due to the Internet, attackers have access to a large variety of potential targets and attack methods. For instance, hackers can utilize social engineering strategies to enter networks or execute spam emails to fool people into disclosing private information. They can also utilize malware to attack systems, steal data, or launch more assaults, or they can exploit software flaws in well-known platforms like web browsers or email clients. So it is really good to protect ourselves over this type of people, by Strong security measures, such as firewalls, antivirus software, and encryption, as well as persistent education and awareness-raising about the dangers and threats of the internet are needed to achieve this.