Paul Neville

ITS 444

03/20/2023

Questions Chapter 5

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

In her book "Hacking the Future: Privacy, Identity, and Anonymity on the Web," Coleen M. Zertag uses the metaphor of a "digital jungle" to describe the idea that there are "no safe neighborhoods" online. By using this metaphor, she means that the internet is a dangerous and unpredictable environment, just like a jungle.

The video "No Safe Spaces Online" by the National Cyber Security Alliance (NCSA) further illustrates this idea. The video shows how online activities such as social media, online shopping, and banking can be vulnerable to cyber attacks. It also highlights the fact that individuals must take steps to protect themselves, just as they would in the physical world.

The video presents the metaphor of a house to explain how individuals can protect themselves online. Just as one secures their house by locking doors and windows, individuals can secure their online presence by using strong passwords, enabling two-factor authentication, and keeping software up to date. The video also emphasizes the importance of being cautious about sharing personal information online and avoiding clicking on suspicious links.

Both Zertag's metaphor of a digital jungle and the NCSA's metaphor of a house highlight the need for individuals to be vigilant and take precautions to protect themselves in the online world. The internet is a constantly evolving environment, and new threats are emerging all the time. Therefore, it's essential to stay informed about the latest risks and to update security measures regularly.

In conclusion, the metaphor of a digital jungle effectively conveys the idea that there are "no safe neighborhoods" online. This metaphor reminds individuals that the internet is a dangerous and unpredictable environment, and that they must take steps to protect themselves. The NCSA's metaphor of a house provides practical tips on how to secure one's online presence. By staying informed and taking the necessary precautions, individuals can navigate the online world with greater confidence and security.

Paul Neville

ITS 444

03/20/2023

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?

When Coleen M. Zertag says that the internet has a "huge attack surface," she means that there are countless entry points or vulnerabilities that can be exploited by cyber attackers. These vulnerabilities can exist in software, hardware, or even human behavior. For instance, a weak password or a click on a malicious link can provide an attacker with access to an individual's device or network.

The rise of the "Internet of Things" (IoT) exacerbates this issue by increasing the number of connected devices and expanding the attack surface. The IoT refers to the network of devices and sensors that are connected to the internet, including everything from smart home appliances to industrial control systems.

As more devices are connected to the internet, the potential attack surface grows exponentially. Each connected device represents a potential vulnerability that can be exploited by cyber attackers. For instance, an attacker could gain access to a smart home's security system or manipulate an industrial control system to cause physical damage.

Moreover, many IoT devices have weaker security measures compared to traditional computers and smartphones. This is because the focus has been more on functionality than security, and many IoT devices are not designed with security in mind. This means that attackers may be able to exploit vulnerabilities in these devices more easily, making them attractive targets.

In conclusion, Zertag's assertion that the internet has a "huge attack surface" refers to the many vulnerabilities that exist in the online world. The rise of the IoT exacerbates this issue by increasing the number of connected devices and expanding the attack surface. It is crucial for individuals and organizations to take steps to secure their devices and networks, such as using strong passwords, enabling two-factor authentication, and keeping software up to date. Additionally, manufacturers must prioritize security in the design and production of IoT devices to prevent future cyber attacks.