Trends in Internet Security and Cybersecurity

Yunus Teke, 2508638

1. **Cybersecurity risks of Remote/Distance working**

Due to the Coronavirus pandemic, people were forced to shift their workplaces. A high proportion of the workforce will continue to work remotely. This new remote-working environment brought unknown cybersecurity risks. Home offices are usually less protected than regular offices, which have more secure firewalls, routers, etc.

Many employees are using their personal devices without two-factor authentication, and they may have mobile app versions of instant messaging applications, such as Teams and Zoom. These blurred lines between personal and professional life increase the risk that sensitive information could fall into the wrong hands. Even if the employee is working from a distance, the employer is supposed to identify new security vulnerabilities beforehand and fix them.

1. **Internet of Things (IOT)**

The expanding Internet of Things (IoT) creates more opportunities for cybercrime. The Internet of Things refers to physical devices other than computers, phones, and servers, which connect to the internet and share data. Examples of IoT devices include wearable fitness trackers, smart refrigerators, smartwatches, and voice assistants like Amazon Echo and Google Home. So many additional devices change the dynamics and size of what is sometimes called the cyber-attack surface – that is, the number of potential entry points for malicious actors. Compared to laptops and smartphones, most IoT devices have fewer processing and storage capabilities. This can make it harder to employ firewalls, antivirus, and other security applications to safeguard them.

As a result, IoT attacks are amongst the discussed cyber-attack trends. You can read more about IoT security threats here.

1. **Rise of Automotive Hacking**

Modern vehicles come packed with automated software, creating the best connectivity for drivers in cruise control, engine timing, door lock, airbags, and advanced systems for driver assistance. These vehicles use Bluetooth and Wi-Fi technologies to communicate, thus opening them to several vulnerabilities or threats from hackers. Gaining control of the vehicle or using microphones for eavesdropping is expected to rise in 2022 with more automated vehicles. Self-driving or autonomous vehicles use an even further complex mechanism that requires strict cybersecurity measures. So, the company that produces the new tech automobiles must take precautions to hack beforehand not to risk the people who buy those vehicles.

1. **Cyber-security of Cryptocurrency market**

The decentralization of cryptocurrency is an excellent opportunity for cybercriminals. Cybercriminals can hack into cryptocurrency trading platforms and steal funds. Cryptocurrency is already the most preferred form of exchange in cases of ransomware attacks. Ransomware incidents usually have a common thread.

Cybercriminals can hide their true identities when asking for ransom in digital currencies. They can easily convert cryptocurrencies into traditional forms without ever being discovered when making an exchange. They can attack any business and ask for ransom in digital currencies as this form of cybercrime is untraceable, and no evidence leads back to the perpetrators. With cryptocurrencies spreading across the business world, cybercrime has become a real threat. More and more criminal actors are trying to use digital assets to keep their illicit activities under the radar. In addition to this, cryptocurrencies are an excellent way to launder funds. The only thing that protects people from attacks like these in the future is ensuring they have the proper cybersecurity in place.

**The Future of Computer Networks**

It is hard to imagine a future without the Internet. The web is getting better and better, in a way. The web, first known as Web 1.0, came out in the late 1980s and had relatively few participants. Web 2.0, defined as the interactive Internet, has been used for over 20 years. Web 3.0, the future of the Internet, which is eagerly awaited, has been on the agenda lately thanks to the cryptocurrency world.

After the spread of Web 2.0, many big brands and applications that we know began to be born. These are all brands we can think of, such as Google, Twitter, Facebook, YouTube, LinkedIn, which have developed thanks to Web 2.0.

Agents in Web 1.0 were servers. We needed servers to interact with someone. In Web 2.0, these servers were replaced by platforms, and we were able to communicate only by registering. Web 3.0 will allow for a decentralized connection without any intermediaries.

This Web 3.0 comes with new technologies, too, such as Metaverse. On a closer look, Web 3.0 and Metaverse are quite relevant entities. Web 3.0 will be an infrastructure for Metaverse. VR devices used for Metaverse can accelerate the transition to Web 3.0. This process can be easily achieved if an open-source system, a reliable infrastructure, and verifiable communication methods are provided. Both formations are the future of the internet world.

In my opinion, the future of networks is going to be revolutionary.

**References:**

* **https://fultonmay.com/what-is-cryptocurrency-and-how-does-it-affect-cyber-security/**
* **https://www.simplilearn.com/top-cybersecurity-trends-article**
* **https://www.kaspersky.com/resource-center/preemptive-safety/cyber-security-trends**