DEPARTMENT OF EDUCATION AND TRAINING OF HO CHI MINH CITY

FPT UNIVERSITY

FACULTY OF INFORMATION ASSURANCE

FPT Education

FPT UNIVERSITY

Discussion report

RISK MANAGEMENT IN INFORMATION SYSTEMS

Teacher: Mr. Pham Yen Thao

HO CHI MINH CITY, JULY 2023

Has the number of cyberattacks in Vietnam increased or decreased in recent 5 years? What are some common ways malware / virus spread? What do you think about this?

Cyberattacks pose an increasing threat to people and organizations all around the world. The same is true of Vietnam. Although there have been fewer cyberattacks in Vietnam recently, the threat still exists.

Vietnam had a 104% surge in cyberattacks in 2019 alone. However, in 2020, 2021, and 2022, there were fewer cyberattacks. In Vietnam, there were 33.8% fewer cyberattacks in 2022 than there were in 2021.

The cyberattacks that have occurred in Vietnam recently are shown in the following graph:

Year	Number of Cyber Attacks	% Change from Previous Year
2019	6,219	+104%
2020	5,168	-0.15%
2021	4,357	-17.3%
2022	2,91	-33.8%

The most common types of cyberattacks in Vietnam are phishing, defacement, and malware.

- Phishing: One of the most popular methods that viruses and malware are distributed in Vietnam is through phishing. Emails that appear to be from reputable sources, such banks or government organizations, are sent during phishing attempts. Links or attachments in phishing emails frequently download malware onto the victim's machine when they are clicked.
- Defacement: Defacement assaults are another typical way that viruses and malware propagate in Vietnam. Defacement assaults entail altering a website's look without the owner's consent. By incorporating malicious code into the website's source code, these assaults may be used to propagate malware.
- Malware: In Vietnam, malware is another popular means of virus and malware transmission. There are several ways to install malware on a computer, including via clicking on malicious link, opening an infected attachment, or downloading a file from an untrusted source.

The Vietnamese government has taken action to strengthen cyber security. The government started a drive to remove malware in 2019. Millions of PCs in Vietnam had malware that was wiped clean thanks to this operation. The federal government unveiled a national cybersecurity policy in 2022. The objectives of the government are set forth in this policy for enhancing cyber security in Vietnam.

Both businesses and people need to be aware of the cyber danger and take precautions to be safe. Businesses and people can take the following steps to safeguard themselves against cyberattacks:

- Using strong passwords and changing them regularly
- Keeping their software up to date
- Using a firewall and antivirus software
- Being careful about what links they click on and what attachments they open
- Being aware of phishing scams

In my opinion, Vietnam's government is doing appropriately to increase the nation's cyber security. To further inform people and companies about the cyber danger, more has to be done. Additionally, I think that the government need to collaborate with foreign parties in order to exchange knowledge and best practices regarding cyber security. Cyberattacks pose a significant danger to Vietnamese businesses and citizens. Businesses and people may contribute to lower the danger of being attacked by taking precautions to protect themselves.