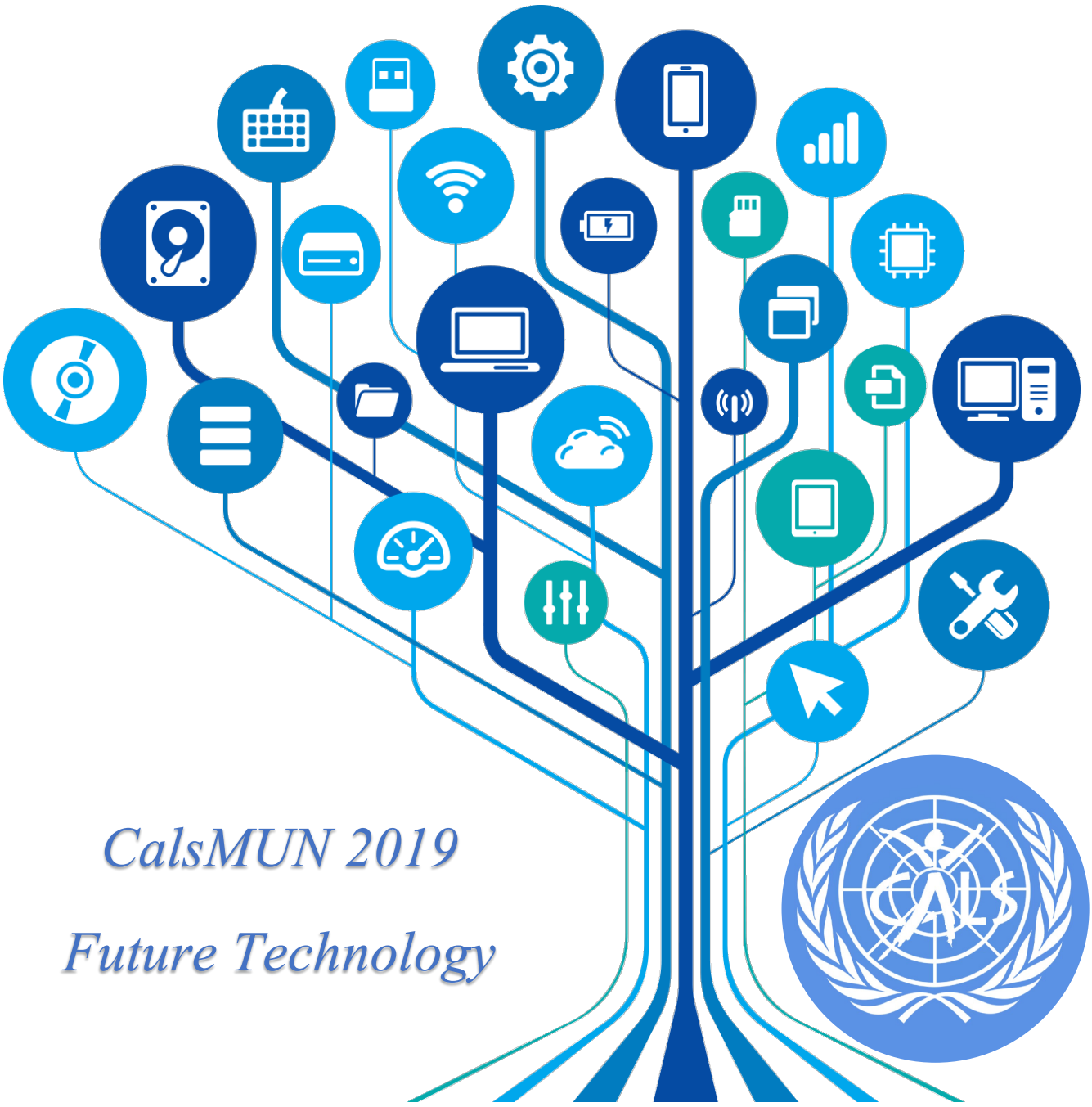


CalsMUN 2019

Future Technology

Research Report

Forum: Commission on Crime Prevention and Criminal Justice

Issue: Combatting cybercrime on a national and international level

Chairs: Friso van Gruijthuijsen and Zuzanna Borowska

Personal Introduction

Friso van Gruijthuijsen
Hi! My name is Friso van Gruijthuijsen, I am 17 years old and I am a student at the Stedelijk Gymnasium Leiden. I have done 9 MUNs so far, and this will be my first time chairing. I was the Secretary-General of LEMUN 2018. I will only be there on Sunday; Stuart Verkerk will replace me on Saturday. I have put a picture of me and Stuart below.

I look forward to the conference!

Left: Stuart, on the right: myself 😊

Introduction

Nowadays, the world is more connected than ever. We can speak to a relative who is living on the other side of the world, we can order a pizza in a few seconds, and we can watch a football match that is physically playing at the other side of the world. That can all be done with a device that is sitting inside our pocket.

But it has a downside. Cybercrime costs the world 600 billion US Dollars *a year*. The costs are expected to rise to 6 trillion dollars in 2022. Furthermore, if someone loses all of his or her digital files due to cybercrime, the psychological effects on that person can be devastating.

Thus, the damage is so high, that in case cybercrime was a problem that was easy to solve, we would already have done it. Combatting cybercrime is incredibly difficult. In this Research Report we will look at what cybercrime is, what it *not* is, and what we can do about it.

Cybercrime is an issue that often becomes so difficult that only the ones with a PhD in Computer Science can understand it. We aim to make this topic understandable for everyone, so we will do our best to avoid the technical details of cybercrime.

Key Terms

Cyber Crime
Criminal activities carried out by means of computers or the Internet.

Ransomware
A type of malicious software designed to block access to a computer system until a sum of money is paid.

Phishing Email
The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Malware
Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Trojan Horse
A program designed to breach the security of a computer system while ostensibly performing some innocuous function.

General Overview

Before we will explore how we can combat cybercrime, we will first have to define what we will discuss and what not. There are so many forms of cybercrime, that discussing them all would lead to confusion, which would mean we could not address the issues effectively. We don't have the time to discuss them all.

So, what will we discuss in this Research Report? We will mainly focus on the following forms of cybercrime:

- Ransomware
- Phishing
- Hacking in order to steal something
- DDoS attacks

We will first discuss what the forms of cybercrime are, how they work, and what the damage is. As the causes of ransomware, phishing, hacking and DDoS attacks mostly overlap, we will discuss those causes combined at the end of the General Overview.

There are topics that we will *not* discuss, however. You can think about the following subjects:

- Weaponization of Social Media (e.g.: Possible Russian interference in the 2016 American presidential election via the use of social media)
- Distribution of child pornography
- Grooming: making sexual advances to minors
- Cyberbullying: bullying a child or adult via social media

The Problem

Ransomware
A ransomware attack usually goes the following way:

1. A hacker decides to make, or buy, a piece of software that encrypts someone's files, which can only be unlocked by the hacker.
2. The hacker tries to install the software on the computer of a stranger. There are multiple ways to do that, but one of the most common methods is that the hacker sends an email to the victim with a suspicious link.
3. The victim tries to access his/her files via his/her computer, but he/she doesn't see the files. Instead, he/she sees a message that he/she has to pay XXX amount of money to the hacker before a certain date.

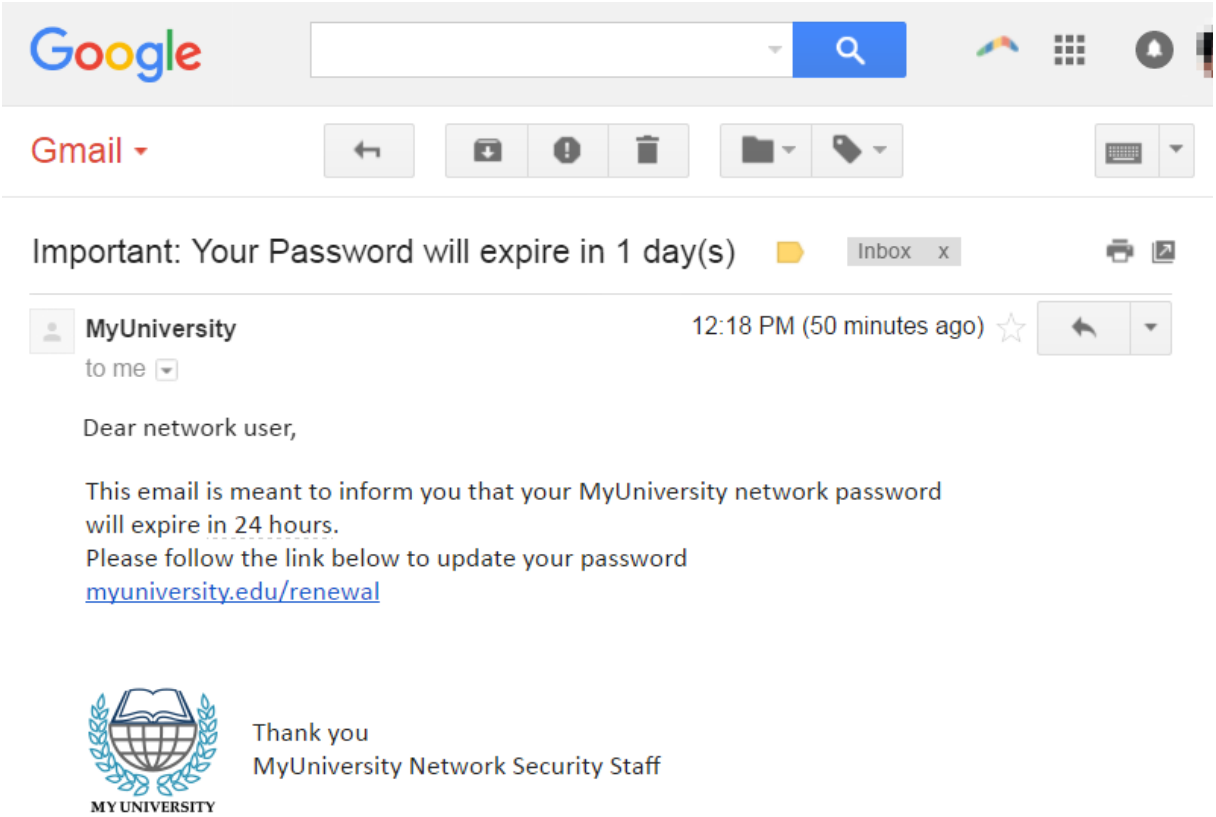
4. The victim panics. Now, a few things can happen. Or the victim finds a way to retrieve his files, or the victim loses his/her files, or the victim pays the hacker to get the files back.

WannaCry is a ransomware worm that spread rapidly through across a lot of computer networks in May of 2017. It affected major companies and organisations, such as Renault, Deutsche Bahn, and Portugal Telecom. It is one of the clearest examples of ransomware.

According to Cybersecurity Ventures, ransomware costs the world more than 8 billion US dollars. Furthermore, in 2019, a ransomware attack will hit a company every 14 seconds. It is clear that ransomware attacks are a problem that needs to be addressed.

Phishing

"Phishing" is the act of trying to persuade someone to give his/her username and password. It can happen both in the normal and in the digital world. If someone from Microsoft in India has ever called you to ask you for your password, you have been the target of a phishing attack. Another example is that someone sends you an email where he/she asks you to give your password. Below you see a clear example of a phishing attack.



It is difficult to assess what the global costs of phishing attacks are. According to McAfee, 97% per cent of consumers are unable to correctly identify phishing emails.

Hacking

There are lots of discussion about what hacking really is, but what it comes down to, is that someone tries to steal digital files. In order to access those files, the hacker tries to find a security breach in the computer system of the victim. That victim can be an individual, organization, or country. As the security breaches vary from system to system, hacking attacks vary in method, size and impact.

The objective of hacking attacks varies as well. Sometimes, countries hack in order to obtain sensitive, secret information from other countries. In other cases, individuals were hacked by people trying to blackmail them.

Sometimes, a hacker finds a security breach in a website, but he doesn't feel the need to exploit it. In that case, he can sell the breach on the "dark web". The dark web is a special part of the internet which normal internet browsers will not visit.

To give you an idea about what a hacking attack looks like, we have put an example below, which we found at www.wired.com.

Under Armour is an American company that manufactures footwear, sports, and casual apparel. Hackers breached Under Armour's MyFitnessPal app in late February, compromising usernames, email addresses, and passwords from the app's roughly 150 million users. The company discovered the intrusion on March 25 and disclosed it in under a week—some welcome hustle from a large company. And it seems Under Armour had done a good enough job setting up its data protections that the hackers couldn't access valuable user information like location, credit card numbers, or birth dates, even as they were swimming in login credentials.

The company had even protected the passwords it was storing by hashing them, or converting them into unintelligible strings of characters. Pretty great, right? There was one crucial issue, though: Despite doing so many things well, Under Armour admitted that it had only hashed some of the passwords using the robust function called bcrypt; the rest were protected by a weaker hashing scheme called SHA-1, which has known flaws. This means that attackers likely cracked some portion of the stolen passwords without much trouble to sell or use in other online scams. The situation, while not an all-time-worst data breach, was a frustrating reminder of the unreliable state of security on corporate networks

DDoS attacks

In a DDoS (Distributed Denial-of-Service) attack, lots of computers try to go to a website at the same time. That causes the website to be overloaded by traffic. The computers that are part of a DDoS attack, are often computers of consumers infected with malware. The consumers often don't even know that their computers take part in a DDoS attack. There is a good chance that even your computer takes part in a DDoS attack.

The size of a DDoS varies from attack to attack, but it depends on the number of computers that take part. Websites are often the target of a DDoS attack. Websites try to defend themselves by getting more servers to handle their traffic and by trying to separate real traffic from fake traffic. Still, it happens quite often that a website gets shut down for a few hours.

In January 2018, the websites of some major Dutch banks (Rabobank and ABN Amro) were shut down after a DDoS attack. An 18-year-old boy was arrested a few days later. This example shows us that a DDoS attack can be executed by anyone. DDoS attacks can be executed by a military army for strategic purposes, or by a bored teenager.

Causes of cybercrime attacks

The causes of the attacks above mostly overlap. Let's have a look at the most common causes of cybercrime attacks.

Easy to access
The problem behind safeguarding a computer system from unauthorized access is that there are many possibilities of breach due to the complex technology. Hackers can steal access codes, retina images, advanced voice recorders etc. that can fool biometric systems easily and bypass firewalls can be utilized to get past many security systems.

Capacity to store data in comparatively small space
The computer has the unique characteristic of storing data in a very small space. This makes it a lot easier for the people to steal data from any other storage and use it for own profit.

Complex
The computers run on operating systems and these operating systems are programmed of millions of codes. The human mind is imperfect, so they can do mistakes at any stage. The cybercriminals take advantage of these gaps.

Loss of evidence
The data related to the crime can be easily destroyed. So, loss of evidence has become a very common & obvious problem which paralyzes the system behind the investigation of cyber-crime.

Major Parties Involved

Organisations

Antivirus Software Companies
Antivirus Software Companies, such as Kaspersky, McAfee, or BitDefender, make antivirus software that protects the computer against malware. They do their best to keep up in the cat-and-mouse game against the hackers, but obviously, their software is not always perfect.

Countries

Cybercrime attacks are a problem for both developed and developing countries. However, there are subtle differences.

Developed Countries
Developed countries have more experience with the internet dan developing countries. Therefore, they generally have better protection against hackers than developing countries. A lot of countries, especially developed ones, have special agencies to protect the cyber infrastructure of a country.

Developing Countries
A lot of developing countries have only recently got access to the internet. They don't have a lot of experience with cybersecurity. That is a major problem for their cybersecurity.

Timeline of Key Events

Cybercrime is as old as the Internet itself. As the internet continued to grow, so did cybercrime. So hereby a brief overview of the development of the internet.

Date	Description of Event
1983	TCP/IP (a set of rules that governs the connection of computer systems to the Internet) was implemented for the first time.
1990	Tim Berners Lee invents the World Wide Web, the form of the internet as we still know today.
1997	Larry Page and Sergey Brin launch "Google", a search engine for the new thing called the internet.
1999-2000	.Com bubble: Due to the hype of the internet, a lot of new internet companies gained a lot of value in the stock market. That bubble bursted in March 2000.
2001	Wikipedia was invented
2007	Due to the launch of the iPhone, more and more people will access the internet via their smartphone.
2010	29% of the world population has access to the internet. In the developed world, that is 66%.
2011	Snapchat was launched.
2018	55% of the world population has access to the internet. In the developed world, that is 86%.

Previous Attempts to Resolve the Issue

Cybercrime is a many-headed monster that is almost impossible to defeat. A lot of the solutions mentioned in Possible Solutions have already been implemented in some form.

In the Netherlands, we had a campaign where major banks urged people not to respond to phishing emails. They made a website for their campaign: www.veiligbankieren.nl

However, as cybercrime is still on the rise, those measures are not effective enough, and should be intensified.

Possible Solutions

Before we dive into possible solutions, we want to encourage you to come up with your own solutions. Furthermore, always keep in mind what your country's interests are: not all solutions will align with them.

Knowhow about cyber security – developed/developing countries
Developed countries have more experience in defending themselves against cybercrime. They have military units which are specialized in cyber security. If the governments of developed countries share their information with developing countries, developing countries could protect themselves better. However, if you represent a developed country, please keep in mind whether this proposal aligns with your national security interests.

Cyber Security - individuals
A lot of hacks happen because individuals don't take proper measures to protect themselves against malware. They have the same password for every website, they do not install antivirus software, and they click on suspicious web links. It would help a lot if delegates take measures to increase the awareness of individuals about the risk of cybercrime.

Cyber Security – *organisations and companies*
Organisations and companies store sensitive information of their clients on their servers. Due to a lack of awareness and financial considerations, cyber security is not always their top priority. For the delegates, please think if you would be an favour of measures that would make cyber security a higher priority. Those measures could vary from awareness campaigns to fines if a company does not invest in cyber security.

More resources to Interpol
It is difficult to arrest hackers: often, they work internationally. We will not dive into the technical details how police organisations arrest hackers, but we should know that it is very time consuming: thus, it costs a lot of money. Interpol is an international organisation that facilitates international police cooperation. Although Interpol is independent from the CCPCJ, the CCPCJ could ask their member states to direct more money to Interpol, so they can do their work better.

Legislation cyber crime

Cybercrime is an international problem, and hackers operate from all over the world. Some countries have no legislation against cybercrime in place. That makes it harder to tackle the problem. It would help a lot if the countries that don't have laws against cybercrime would pass the legislation as well. However, keep in mind that the CCPCJ cannot force those countries to do so.

Further Reading

For those who want to make a little bit of extra money:

- https://null-byte.wonderhowto.com/forum/complete-guide-creating-and-hosting-phishing-page-for-beginners-0187744/

A good article about cybersecurity in developing countries:

- https://disruptionhub.com/developing-countries-hotbed-cybercrime/

More statistics on the subject of cybercrime:

- https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

Bibliography

- https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHd&utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-bb9303ae70-1940938
- https://www.google.com/search?q=social+media&oq=social+media&aqs=chrome..69i57j0l5.7221j0j7&sourceid=chrome&ie=UTF-8
- https://www.comparitech.com/blog/vpn-privacy/phishing-statistics-facts/
- https://metro.co.uk/2018/03/22/when-was-the-internet-invented-7408002/
- https://www.theguardian.com/technology/2016/jul/15/how-the-internet-was-invented-1976-arpa-kahn-cerf
- https://www.theguardian.com/commentisfree/2018/jul/24/darknet-dark-web-hacking-forum-internet-safety
- https://www.kaspersky.com/blog/simda-botnet-check/8304/
- https://krazytech.com/technical-papers/cyber-crime