A STUDY OF CYBERCRIMES

JEDDAH, SAUDI ARABIA

Prepared for:

Dr. Shireen Saif Al-deen

Prepared by:

Raneem Saaty, Batol Alwagdani, Elaf Aloufi, Aseel Alshahrani

November 30, 2019

1 King Abdullah Street

Jeddah Saudi Arabia 83479

(505)572-8026

Dr. Shireen Project #5

November 30, 2019

Cybercrime Awareness Program

City of Jeddah

555 Tahlia Street

Jeddah

Kingdom of Saudi Arabia

Attention: Dr. Shireen Saif Al-deen

We have completed our one-month group project on cybercrime. This report mentioned some of the famous types of cybercrimes, how they work, along with some examples of big attacks in Saudi Arabia. We have also mentioned some ways to protect yourself against this type of crime.

PAGE OF CONTENTS

ILLUSTRATIONS

FIGUERS

TABELS

APPENDICES

Executive Summary

The purpose of this document is to introduce cybercrimes and some of its famous types, how they work, the harm that they cause, how to protect one's self, and the best way to avoid them.

Cybercrimes are every crime that have been committed using the computer. These offences have many types such as malware, hacking, etc. Every type has a certain way of working and a specific goal to achieve; some of them can be dangerous.

Cybercrimes are one of the biggest and the most underrated by the people threats. cyber-attacks have already done a lot of damage around the world. The internet is improving annually and everything is changing to be dependent on internet, which makes cybercrimes more dangerous.

Introduction

In today's world, any computer connected to the internet is under threat of viruses, worms or attacks from hackers. The growth of social media has resulted in the emergence of cybercrimes. Cybercrimes are crimes that have been committed using the network. These crimes can act differently depending on the action that has been used against the other network devices. There are many examples, however, the most prominent ones are: spreading viruses, hacking, DDos, and malware. Cybercrimes depend greatly on what the attacker wants from the other network device.

Document Description

The internet is now considered as an important part of our lives and most people trust it with sensitive information, such as their bank accounts, photographs, passwords, internet browser history, etc. but are people aware of the risks of trusting the internet? The growth of the internet brought with it an abundance of risks. In this report, we are going to discuss cybercrimes and how to protect oneself from them.

The scope of the study

The main types of cybercrimes are:

- Malware
- Hacking
- Distributed denial of service attack (DDos)
- Spam

Report format

The main purposes are:

1. Investigation: a complete discussion of all the type of cybercrimes
2. Types of attackers
3. Real life incidents: examples of real-life cybercrime incidents
4. Protection against cybercrimes
5. Conclusions and Recommendations

Investigation

Cybercrimes are crimes or incidents that target IT and it is an advanced technological crime that depends on the target. In general, there two types of cybercrimes. The first type is "new" crimes that are aimed at IT and committed through the use of IT, for example, hacking. The second type is "traditional" crimes that are not focused on IT, but where IT is a substantial facilitating factor for committing the offense, for example, fraud via the internet.[5][2]

Malware

The first main form of cybercrime is malware. Malware means malicious software. It spreads from one computer to another and interferes with their operations. Malware can be used to crash systems and to steal personal information. Malware has many forms such as:

1. Viruses

One of the most known types of malware are viruses. Viruses can be harmless or they can damage data. Their damage ranges from mild to major. An example of mild damage is mild computer dysfunction. An example of major damage is deleting hardware. Viruses self-replicate and spread between and within computers. They require a host, such as a file, to act as a carrier. However, viruses need human action to be able to infect a file. The virus spreads

when an infected file is passed from system to system. Once a virus is active, it will infect other programs on the computer.[7]

2. Worms

This type of malware can spread between different computers and within the same computer as well as self-replicate. The worms have a stronger effect than viruses, which is because they don't require host or any human action. The worms can also drop another type of malware, called Trojans Horses, and cause an interruption in the network.[7]

3. Spyware

This type is one of the most dangerous types of malware. The main use of the spyware is to collect sensitive information from the victim. This information can be shared to another person. Some of the spyware is hidden within some of the advertisements online; this type of spyware is called adware. There are many types of spyware, such as the spyware that captures screen shots and spyware key-logging.[7]

4. Trojan horses

Trojan horses are a type of malware that appear as a legal program, when in reality, it preforms illegal actions such a stealing information without the user's permission. The Trojan horses are different from the other types of malware because they link themselves with non-executable files.[7]

5. Ransomeware

Ransomware imprisons a computer system or the data in a computer contains until the victim gives the criminal the amount that they want. Ransomware encrypts data in the computer with a key which is unknown to the user. The user has to pay a ransom to the criminals to retrieve data. Once the amount is paid the victim can resume using his/her system.[1]

6. Shamoon

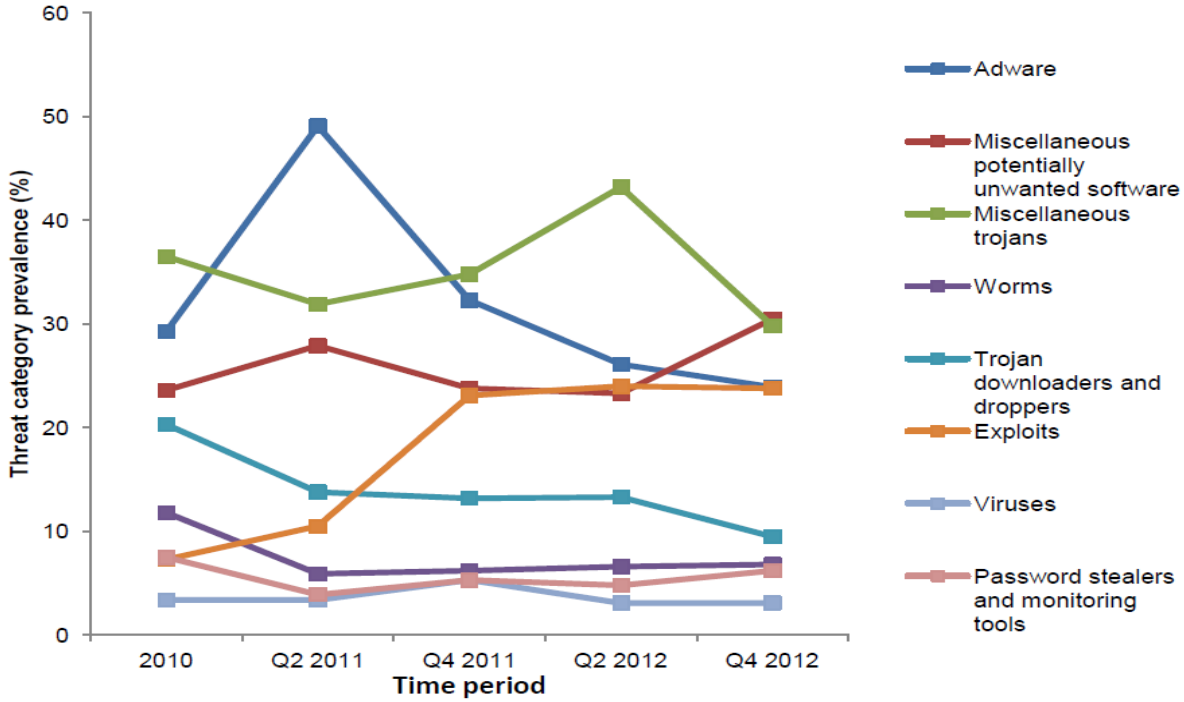
Iran has created Shamoon based on other types of malware. Shamoon targeted Saudi Arabia's oil company, Saudi Aramco. Shamoon is a very destructive wiper malware. Wiper is the class name of the malware that wipes out hard drives. Data that is wiped cannot be recovered. Shamoon is the most famous wiper. Shamoon 2.0 includes a fully functional ransomware module, in addition to its common wiping functionality.[1]

This type of malware has additional properties:[1]

- it has both 32-bit and 64-bit components.
- it samples do not implement any command and control (C&C) communication.
- it embeds Arabic-Yemen resource language sections.

The following figure shows the prevalence of certain types of malware:

Figure 1: Malware threat category prevalence in the UK, (percentage of detections of each malware threat based on computers cleaned for every 1,000 executions of the Microsoft Malicious Software Removal Tool), Microsoft 2010–2012



Source: [5]

Hacking

Hacking is a form of trespassing. Hacking is the gaining of access to a computer and viewing, copying, or creating data without the intention of destroying data or maliciously harming the computer.[6]

Hacking can be used to:

- gather personal information that is of use to criminals
- deface websites
- be employed as part of DDoS attacks

Hacking and hackers are commonly mistaken to be the bad guys most of the time. Crackers are the ones who are bad as far as creating viruses, cracks, spyware, and destroying data. A hacker first attacks an easy target, and then uses it to hide his or her traces for launching attacks at more secure sites.[7]

Distributed denial of service attack (DDos)

DDoS relates to the flooding of internet servers with requests (for example, links that have been clicked) that they are unable to respond quickly enough. This can overload servers causing them to freeze or crash. A DDoS attack is a crime that renders network resources inaccessible to their intended users. Although DDoS attacks may be via different means, motives, and targets, they generally include the concerted, malevolent efforts of a persons to make an Internet site or service unable to perform normally or even at all. A DDos attack is characterized by an attempt by attackers to prevent legitimate users of a service from using the service. There are two general forms of DDoS attacks: those that crash services and those that flood services.[7][8]

Spam

Electronic spamming is the use of electronic messaging systems to send numerous unsolicited messages (spam), especially advertising. While the most widely recognized form of spam is e-mail spam, there are other forms, including: instant messaging spam, online classified ads spam, mobile phone messaging spam, social networking spam, social spam, television advertising, file sharing spam, etc. It is difficult to hold senders accountable for their mass mailings. Because the barrier to entry is so low, spammers are numerous, and the number of unsolicited mail has increased dramatically. Spamming has been the subject of legislation in many jurisdictions.[7]

Types of attackers

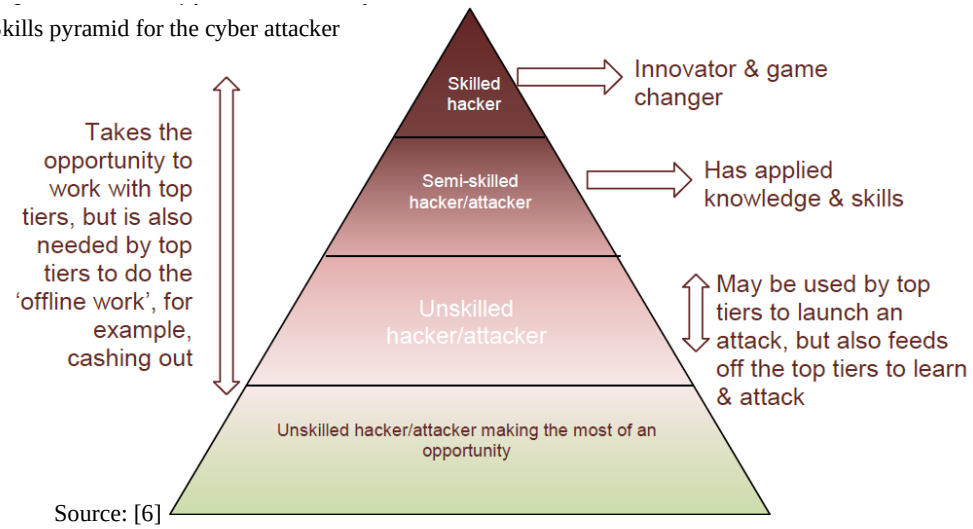
Published evidence is very important in offender case-studies or interviews and tend to focus on their methods and motivations. There is little published evidence around criminals' characteristics, their backgrounds, career paths, the links between online and offline offending, and progression into reoffending. The most common technology-related activity amongst young people is illegal downloading. In the OCJS (Offending, Crime and Justice Survey) around 26% of 10 to 25-year-old internet users reported that they had illegally downloaded files or music. When it comes to cyber-dependent crimes, 1% of internet users aged 10 to 25 years sent a computer virus and the same proportion reported using a computer to access another person's files illegally. Men were more likely than women to report sending viruses (2% compared with 1%) and gaining unauthorised access (2% compared with 1%). Age differences are also very prominent, 10 to 17-year-olds more likely than 18 to 25-year-olds to hack, send viruses, or take part in any of the previously mentioned two. Cyber-enabled crimes are rare. The number of young people who reported obtaining someone else's card details through the internet is very low (0.1% of all 12 to 25-year-olds), and the same percentage reported purchasing items online using someone else's card details without the card owner's permission.[6]

The survey also found that 3% of 10 to 25-year-olds reported visiting a website which detailed how to commit a cybercrime. Similarly, 1% of OCJS internet users (aged 10 to 25 years) reported sending an email with the intent to threaten, harass, or scare. Research has attempted to categorize of cyber offenders. Hackers are often two types: the first type is 'ethical' hackers, hackers who infiltrate systems to help find vulnerabilities, and the second type is 'crackers', hackers who are intent on malicious criminal damage. A number of hacker classifications exist. For example, Rodgers suggests that there are seven subtypes of hackers:[6]

1. Newbies. Those who have limited skills and experience, and are reliant on tools developed by others
2. Cyberpunks. Those who deliberately attack and vandalise
3. Internals. Those who are insiders with privileged access
4. Coders. Those who have high skill levels
5. Old guard hackers. Those who have no criminal intent and high skill levels (ethical hackers)
6. Professional criminals
7. cyberterrorists

Cyber-dependent attackers have also been categorised in terms of skill level. Holt and Kilger outline the skills distribution of hackers in terms of a pyramid:[6]

Figure 2: Skills pyramid for the cyber attacker



Source: [6]

A small group of skilled hackers sits at the top of the pyramid; the only group with sufficient knowledge to engage in truly advanced attacks on their own. They are responsible for identifying new weaknesses of devices and creating the required techniques to undertake cybercrimes. Beneath this group are a larger group of semi-skilled hackers who can use the techniques of the skilled group, but lack the skill to create their own techniques. The lowest and largest group of hackers are the unskilled group, which includes newbies. The people in this group have little real understanding of the techniques behind cyberattacks, but can still be a nuisance to security officials.[6]

Real-life incidents

Due to the increase in economic activity, the Kingdom of Saudi Arabia has become a major target of cybercrimes. The first example is when there was a cyber-attack against Aramco, the world's largest oil producer company. Thousands of client computers at the company were hit by a devastating virus in 2012. The attack destroyed data and erased hard-drives of computers. The second example is when the Official Website of King Saud University got hacked by an unknown hacker. Personal information of 812 users was hacked and dumped on the internet on a file sharing site including mail address list, mobile phones, and passwords. The third example is when several government websites in were sabotaged in a series of cyber-attacks from abroad, disabling them.[1]

The attacks on the middle east were initiated by Stuxnet attack in 2010 with the of goal of stopping or delaying the Iranian nuclear program. The shamoon technique enabled the worm to penetrate a network that is separated from other networks. "Iran, having been a victim of a similar cyberattack against its own oil industry in April 2012, has demonstrated a clear ability to learn from the capabilities and actions of others." The NSA document states, which means that Iran may have launched the attack against Saudi Aramco. When shamoon 2.0 attacked the KSA, it prompted Saudi Arabia telecom authorities to issue a warning for all organizations to be alert. 15 government entities and private organizations had been hit with Shamoon 2.0.[1]

Protection against cybercrimes

Cybercrimes can take many shapes. The following table shows the statistics of the types of cybercrimes and how they can enter a computer:

Table 1: Negative experiences in the last year among internet users aged 16 and over, Crime Survey for England and Wales, 2010/11 and 2011/12

	A computer virus (%)	Unauthorised access to/ use of personal data (%)	Upsetting/ illegal images (%)	Loss of money (%)	Abusive/ threatening behaviour (%)	One or more negative incidents online (%)
All internet users 2010/11 (unweighted base = 8,383)	33	6	4	3	2	39
All internet users 2011/12 (unweighted base = 8,373)	31	7	4	3	2	37

Source: [5]

Below are some tips for to stay safe:

1. Talk to a trusted person

Always talk to someone you trust about what you experience online. Help each other by making sure you stay safe.[9]

2. Do not reveal personal information

While the Internet is great for making new friends, it's important not to reveal too much about oneself. Some people will hide their real identity and try to approach young people for sexual purposes. Stay in control of your information and actions by doing the following: [9]

- Use the privacy settings in social media sites
- Don't post your full name, date of birth, address or school
- Think before you post

- Show the post to a trusted one before posting
- Do not, under any circumstances, meet with a virtual friend without discussing it with an adult or bringing a close friend.
- Never make plans online.

To keep your computer safe from being infected by technical problems you should use the following and make sure you keep them up to date: [9]

- Firewall
- Anti-virus software
- OS Update

Other things you can do: [9]

- Install anti-spyware tools and run them regularly
- If there is a need for installing a software, make sure it's done properly
- Make sure wireless networks are encrypted
- Block browser pop ups or try using different browsers
- Ignore spam or just delete it
- If you get an abundance of spam, close down your email account and open another.
- Only open attachments sent by people you know and trust.
- Never give passwords to anyone.
- Be alert to phishing. A trusted website will never ask you to confirm sensitive information.

People have to be careful about sharing private information. To do that they have to avoid dangerous online websites, use strong passwords, avoid clicking on pop-ups, stay as far away from internet banking and online purchases as possible, and have up to date antivirus software.[8]

Conclusion

In conclusion, cybercrimes are crimes that have been committed using the internet. These crimes depend on the action that has been used against the other devices and the type of attacker that is attacking the device. Everyone is they at risk of exposure to cybercrimes. Crimes by computer don't always occur behind the computer, but they are always executed via computer. The victim wouldn't even know they were being hacked until it's too late. Crimes done behind the computer are prevalent and gaining even more popularity; they are the world's current problem. With technology being on the rise, criminals don't have to be outside in order to commit a crime. They have everything they need at home. Cybercrimes are dependent on what the attacker wants. They use different types of attacks to achieve their goal; whether their goal is destroying a part of the computer or stealing important information. Social media users should be careful when using social media, should be mindful of their rights, and most importantly, they should tun on the privacy settings that social media sites provide. While it may not be possible to completely eradicate cybercrime, businesses can reduce their exposure to it by maintaining an effective cybersecurity strategy using an in-depth approach to securing systems, networks and data. Businesses should also backup their data and develop policies and procedures that should be followed by all employees.[2][8]

Internet users should always be careful when using the internet and they should always take advice from a trusted person before using the internet. Creating awareness is very important because people may not realize the risks, dangers, dangers and consequences of using the internet without proper security.[8]

Recommendations

To be able to tackle cybercrime effectively, we can do the following:

- Update existing laws to fight Cybercrime;

There should be an amendment to include the creation of cyber offences in the fields of criminal protection of systems and electronic data, illegal content, illegal access, illegal interception, data interference and system interference.[4]

- or enact a separate law criminalising cybercrime

The single law on tackling cybercrime should cover criminalisation; establishing offences for cybercrimes. It should also address measures of investigation. In regard to criminalisation, the law should criminalise access only with the intent to steal data retrieval and espionage.[4]

- Necessary amendments need to be taken

In order to allow the government to retrieve computer data from service providers to tackle cybercrime, but there should be a court procedure to get the data.[4]

- For procedural powers, specialised powers are required and should be stated

Such as for the gathering of electronically stored computer content, for the identification of computer devices, to freeze volatile computer data for a short time, and for undercover online investigations.[4]

- Harmonisation of the laws

Precautions should be taken to make sure the new law is compatible with already existing laws.[4]

Appendix A

Acronym and explanations

IT	Information technology.
OCJS	Offending, Crime and Justice Survey.
Non-executable files	such as image and audio.
Spyware that captures screen shots	secretly take screenshots of your desktop, The shots retrieved from the feature can be stored in the control panel for future usage.
Spyware key-logging	records every keystroke you make on your computer's keyboard.
Espionage	to practice spying by the government to obtain political and military information.

Appendix B

Planning Form

Name: Raneem, Batol, Elaf, Aseel

I. Purpose: Answer each question in one or two sentences.

A .**Why are you writing the document?**

Cybercrimes have become an international issue and this document is written to describe how these crimes are committed and how to protect ourselves from them.

B . **What response do you want from readers?**

We expect from the readers of this document to learn how to avoid or take precautions against cybercrimes. And if it occurs to them, how to deal with it in the best way.

II. Audience

A. Reader Matrix: Fill in names and position of people who may read the document

	DECISION MAKERS	ADVISERS	RECEIVERS
EXPERTS			Dr.Shireen Sifuddin
GENERAL READERS			FCIT Students

B. Information on individual Readers: Answer these questions about the primary audience or this document. If the primary audience includes more than one reader (or type of reader) and there are significant differences between the readers, answer the questions for each (type of) reader. Attach additional sheets as necessary.

Primary audience:

1 **. What this reader's technical or educational background?**

Different background.

2 **. What main question does this person need answered?**

What is the cybercrime? How to protect myself from it?

3. What main action do you want this person to take?

Try to follow the safety tips in the document.

4. What of this person's personality might affect his or her reading?

The lack in her/his knowledge about the cybercrimes.

III. Document

A. What information do I need to include in the

1. Abstract?

Introduction to the cybercrime world, a summary about the contents of the document, a table of contents, and a cover page.

2.Body?

The information details and the appendices after the body.

Conclusion

A summary of the information and the recommendations.

B. What organizational patterns are appropriate and purpose?

From general ideas to details.

C. What style choices will present a professional image for me and the organization I represent? Depending on reliable sources and information.

Appendix C

Gantt chart

	WEEK1	WEEK2	WEEK3	WEEK4	TOTAL TIME
BATOL ALWAGDANI	Summarized: Chapter 6. Cybercrime: a review of the evidence pdf. divide the work on the team. Read all the references to choose what we need. (1 hour and a half)	plan form + the abstract (1 hour and a half)	Rewrite the body of the group project based on the sources (2 hours)	Wrote part of conclusion and recommendations +make table of contents + make page cover+ Edit the whole document (4 hours)	9 hours
RANEEM SAATY	Summarization of the first 25 pages of the research agenda+ Interpol's staying safe on the internet+ cyber law in Saudi Arabia/ crimes committed using social media+ anti cybercrime law in KSA + chapter 1 (2 hours)	wrote the abstract+ plan form (1 hour and a half)	Made the presentation + wrote the comments for the speech (2 hours)	Wrote part of conclusion and recommendations +make table of contents + make page cover+ Edit the whole document (4 hours)	9 hours and a half
ELAF ALOUFI	Summarized: chapter 3 Chapter 2 found 4 references, collected the sources and information in google drive (2 hours)	wrote the plan form+ the abstract (1 hour and half)	Made the presentation + wrote the comments for the speech (2 hours)	Wrote part of conclusion and recommendations +make table of contents + make page cover+ Edit the whole document (4 hours)	9 hours and a half
ASEEL ALSHAHRANI	Found two references cybercrime a review of the evidence, Research Agenda The Human Factor in Cybercrime and Cyber security, Summarized Chapter 2 Ch2,3 from Research Agenda The Human Factor in Cybercrime and Cybersecurity (1 hour and a half)	plan form + the abstract (1 hour and a half)	Read all the recourses and collect the information for the body of the group project (1 hour and a half)	Wrote part of conclusion and recommendations +make table of contents + make page cover+ Edit the whole document (4 hours)	8 hours and a half

Appendix D

References

[1] Alelyani, Salem, and Harish Kumar. “Overview of Cyberattack on Saudi Organizations.” Naif Arab University for Security Sciences, 2018.

[2] Alqahtani, Saeed. “Social Media Cyber Crime: Cyber Crime in Saudi Arabia.” *Al Tamimi & Company*, Nov. 2016, www.tamimi.com/law-update-articles/cyber-crimes-committed-by-social-media-users-in-saudi-arabia/.

[3] “Cybercrime.” *Migration and Home Affairs - European Commission*, 6 Dec. 2016, ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en.

[4] Erinle, Femi. “CONCLUSIONS AND RECOMMENDATIONS.” *Scribd*, Scribd, 2019, www.scribd.com/document/238507805/CONCLUSIONS-AND-RECOMMENDATIONS.

[5] Leukfeldt, E. R. *Research Agenda The Human Factor in Cybercrime and Cybersecurity*. Eleven International Publishing, 2017.

[6] McGuire, Mike, and Samantha Dowling. “Cyber Crime: A Review of the Evidence.” *Gov*, Oct. 2013, assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf.

[7] Ranjan, Abhishek. “Malware and Its Types.” *GeeksforGeeks*, 25 Jan. 2019, www.geeksforgeeks.org/malware-and-its-types/.

[8] Rouse, Margaret, et al. “What Is Cybercrime? - Definition from WhatIs.com.” *SearchSecurity*, 2010, searchsecurity.techtarget.com/definition/cybercrime.

[9] “Staying Safe on the Internet.” Interpol, 2015.