Cybercrime: An Investigation of the Attitudes and Environmental Factors that Make People more Willing to Participate in Online Crime

Dearbhail Kirwan

D13128910

A dissertation submitted in partial fulfilment of the requirements of Dublin Institute of Technology for the degree of
M.Sc. in Computing (Forensics and Security)

July 2017

DECLARATION

I certify that this dissertation which I now submit for examination for the award of M.Sc. in Computing (Forensics and Security), is entirely my own work and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work.

This dissertation was prepared according to the regulations for postgraduate study of the Dublin Institute of Technology and has not been submitted in whole or part for an award in any other Institute or University.

The work reported on in this dissertation conforms to the principles and requirements of the Institute's guidelines for ethics in research.

Signed: DocuSigned by: Dearbhail Kirwan
026969EFDE114F7...

Date: 9/16/2017

ABSTRACT

Cybercrime incidence rates are increasing. In order to identify solutions to this problem, the sources of cybercrime need to be identified. This research attempted to identify a potential set of circumstances that create an environment in which people are more likely to engage in cybercrime.

There are three aspects to this; (1) Behaviour on the internet – Are people more likely to engage in illicit activities online than in the physical world? (2) Crime Perceptions – Do people perceive cybercrime as being less serious than non-cybercrime? (3) Resources on the Internet – Are people aware of the types of free hacking resources that are available online?

In order to address the first question, a review of the existing literature on the matter was carried out and conclusions drawn from it. The *Online Disinhibition Effect* is a key theory in this matter. Results from this review suggest that people are more likely to engage in illicit activities online than they are in the physical world.

Addressing the second question was carried out in two stages. The first was an assessment of some of the free hacking resources that are available online such as tools and educational courses, based on predefined selection criteria. The content or function of these were established and they were rated across a number of factors. This information was fed into a survey to establish awareness of the existence of some of the tool functions, and opinions on course availability. The results from this research indicate that people are aware of the kind of functionality that is available from hacking tools online.

The third question was addressed through another section of the survey in which participants were asked to rate the seriousness of 6 crime scenarios, three of which were cybercrimes, and three of which were non-cybercrimes. The same scenarios were used throughout the survey as participants were asked to determine appropriate sentences for each crime, and then judge the actual sentence that the crime was given. Results from this investigation indicate that people do view cybercrime as less serious than non-cybercrimes.

The results from these three streams of research indicate that they are combining to create an environment in which people more readily engage in cybercrime.

Key words: cybercrime, cybersecurity, ethical hacking, script kiddies, hacking

ACKNOWLEDGEMENTS

Firstly I would like to express a most enthusiastic thank you to my supervisor Damian Gordon, who has been an incredible source of inspiration, support and knowledge. His guidance was an invaluable factor in my success in completing this dissertation. I would also like to thank all the other lecturers and members of the DIT staff that have helped me along the way in my progression through this M.Sc.

Additionally I would like thank the cybersecurity professionals that participated in this research, their knowledge and insights helped to form the conclusions for this dissertation.

I would also like to thank all of my family and friends for their support in this undertaking, it means a great deal, and I know you will all be happy to know that I will no longer be the perpetual student. My housemate Ciaran – thank you for letting me take over the guest room and convert it into my study, I’m not sure I could have done it without that. And last but most certainly not least, I want to thank my fiancé Alan, for his unwavering support and all the countless things he has done for me during the course of this semester. Thank you Alan, I couldn’t have done it without you.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1 INTRODUCTION

1.1 Project Background

Chapter One sets out the background to this research, it gives a description of the research question, sets out the aims and objectives, and provides the outline of this dissertation.

There are multiple separate factors in this research which will now be summarised.

It is very difficult to measure the extent and rate of cybercrime as it often goes unreported, undetected, or unprosecuted. However, there has been a steady increase in the number of annual incidents. e.g. in 2003 the total number of complaints received by the US Internet Crime Complaints Centre was 124,509 with an estimated loss of $125.6 million in total (IC3, 2003), while in 2016, that number had increased to 298,728 total complaints with losses in excess of $1.3 billion (IC3, 2016), indicating not only an increase in frequency, but also in losses per incident.

There has been some research into perceptions of white collar crime compared to perceptions of violent crime indicating that white collar crimes are being perceived as less serious or deserving of punishment than violent crimes (Holtfreter, van Slyke, Bratton, & Gertz, 2008; Michel, 2016). Cybercrime has always been classified as a subtype of white collar crime, however, there has not been much research into perceptions of cybercrimes in comparison to violent crimes, or other non-cyber white collar crimes so there is no concluding evidence to determine if cybercrimes are perceived differently than other crimes.

The concept of ethical hacking is said to date back to as much as 1500 years ago when tactical games were used to help develop skills to think like the opposition and anticipate their moves. These underlying concepts still remain. The US Air Force conducted one of the first ethical hacks in 1974 in order to test the Multics OS (Chandrika, 2014). Since then the industry has evolved. The OWASP (Open Web Application Security Project) Testing Guide was released in 2003 which includes a framework for penetration testing best practices. In 2009, the Penetration Testing Execution Standard (PTES) was launched, offering businesses and security service providers a common language and scope for performing penetration tests. In more recent years, security executives have begun to use on-demand penetration testing services in order to manage their security.

The growth and nature of the ethical hacking industry has led to the propagation of many free hacking tools and educational resources online. These resources are available for anyone to use, regardless of intent. This easy access to hacking resources, combined with a more casual attitude towards cybercrime, could contribute to an increase in the occurrence of malicious hacking activities, particularly from a specific type of novice hacker, also known as a script kiddie.

1.2 Research Description

This research will examine free hacking resources that are available online, and investigate the perception of cybercrimes when compared to the perception of non-cybercrimes. Figure 1-1 below provides an overview of how the research will be carried out.

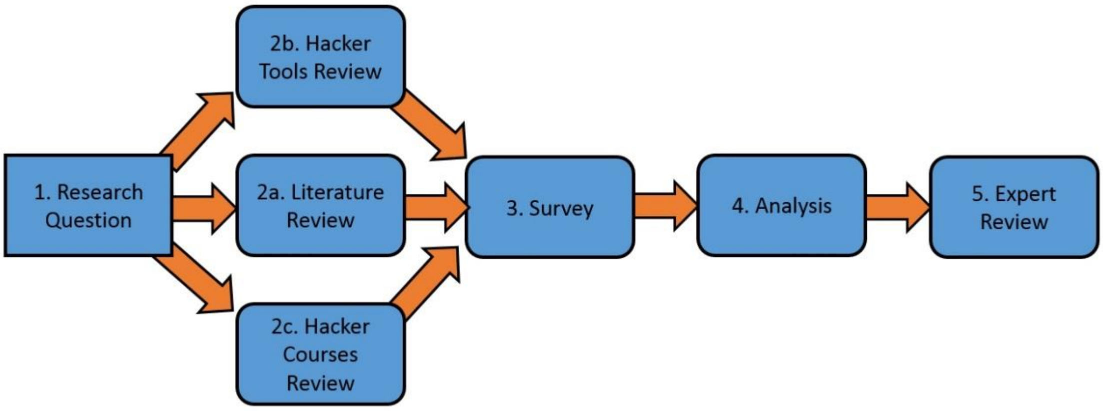


Figure 1-1 Overview of Research

The results from the hacking tools and courses reviews along with the literature review will contribute to the content in the survey in order to assess awareness and opinions around the availability of these hacking resources.

In addition to this, the literature review will assist in the development of the crime perceptions section of the survey, with the aim of investigating whether cybercrimes are perceived as being less serious than non-cybercrimes.

The results from the survey will be analysed to determine the findings for these investigations. The survey and some of the most relevant findings will be presented to a number of experts in the field of cybersecurity for assessment and discussion. This will allow the research to confirm and validate the quality of the survey and the findings with individuals knowledgeable in the field.

The conclusions derived from analysis of the survey results, and feedback from the security experts will assist in the answering of the research question defined below.

1.3 Research Objectives

The aim of this study can be summarised by the main research question:

> *Does the nature of behaviour online and the landscape of the world-wide web combined with current attitudes towards cybercrime, create an environment that encourages people to more readily engage in criminal activities online?*

Answering this research question will be undertaken by addressing the following research sub-questions:

1. *Are people more likely to engage in illicit activities online compared to in the physical world?*
2. *Are cybercrimes perceived as being less serious than non-cybercrimes?*
3. *Are people aware of the type of free hacking resources that are available online?*

The first research sub-question will be addressed through a review of the existing research on the matter. Conclusions will be drawn from this review in order to answer this question.

The second research sub-question will be addressed by the survey component of the research in which participant choices regarding rankings of seriousness and punishments for crimes will be compared across various types of crimes.

The third research sub-question will also be answered by the survey component of the research, the content of which will be informed by the assessment of hacking resources.

The answering of these three research sub-questions will allow a conclusion to be drawn regarding the answer of the main research question.

1.4 Research Methodologies

Multiple methods will be employed in the execution of this research. The first stage will consist of a literature review which will provide an overview of cybercrime and hacking, ethical hacking, and behaviour on the world-wide web.

The next method will first employ investigative methods in order to determine the landscape of hacking resources that are available online, and use this to define selection criteria for further assessment. These selection criteria will then be applied to the hacking resources and those that meet it will be systematically assessed based on a number of factors.

A quantitative survey will be conducted in order to assess attitudes towards cybercrimes compared to attitudes towards non-cybercrimes, and awareness and opinions on the availability of the free hacking resources as found in the review of hacking resources.

Findings from the survey, and the survey itself will be reviewed by some experts in the field of cybersecurity in order to confirm the validity of the survey and the findings.

Conclusions will be drawn from the analysis of the descriptive statistics derived from the survey, and the feedback from the cybersecurity experts.

1.5 Scope and Limitations

The literary research for this dissertation touches on multiple disciplines, from cybercrime and cybersecurity to psychology. The assessment of hacking resources was restricted to free resources, however, it was necessary to define further selection criteria for these resources as there is such a wide range of these resources available, e.g. small hacking tools made available by hackers on GitHub etc., and tutorial videos on YouTube. It would be egregious to attempt to assess all of these so the scope of this research is limited to those that meet the defined selection criteria and is indicative of a smaller representation of that which is available.

The survey will attempt to assess attitudes to a variety of different crimes, however, given the need to go into sufficient depth on the assessment of each crime in order to ensure consistency and validity of results, it is difficult to cover a wide range of different crimes.

The first research sub-question relates to behaviour online and will be answered through a review of existing research on the topic. Ideally the research questions would be answered by first hand empirical research, but in this case would involve a psychological study that was deemed to be outside of the scope of this research.

1.6 Thesis Roadmap

Chapter Two; Cybercrime & the World-Wide Web: A Roadmap, consists of the literature review, which will provide an overview of cybercrime, hacking, and ethical hacking, and review literature on crime perceptions and behaviour on the internet.

Chapter Three; Experimental Design: Hacker Resources Review, will provide the design and results of the review of the hacking tools and hacking courses which will then contribute to the content in the survey in order to assess awareness and opinions surrounding them.

Chapter Four; Experimental Design: Cybercrime Survey, will detail the design of the survey, including a discussion of the previous research that various sections of the survey were inspired by or drawn from.

Chapter Five; Cybercrime Survey Results, will step through each of the sections of the survey reporting and discussing the results.

Chapter Six; Cybercrime Survey Results: Meta-Analysis by Experts, will detail how the results and the survey will be presented to a number of cybersecurity experts and discuss the feedback received from the exercise and its' implications.

Chapter Seven; Conclusions and Future Work, is the final chapter and will describe the context of the research and outline the resulting conclusions and make some recommendations of solutions and future work.

2 CYBERCRIME & THE WORLD-WIDE WEB: A ROADMAP

2.1 Introduction

In this chapter, a range of topics will be covered that will give an overview of cybercrime and some important methods and factors in the growth of certain types of cybercrime. First, a number of definitions of cybercrime will be presented, followed by a range of other terminology relevant to cybercrime, including, the concepts of script kiddies and ethical hacking, in addition to a discussion of the research on human behaviour on the internet and how this is also a potential factor for cybercrime.

The purpose of this is to make clear the concepts that are relevant to the research question, and to explore and identify gaps in the existing research around the topics of the landscape of the internet and cybercrime, and the perception of cybercrime so that research for this study can draw on previous research and form a well-rounded approach to the research question.

2.2 Defining Cybercrime

The term "cybercrime" is widely known, however, in spite of its' notoriety, there is no universal definition for it. There have been many definitions and yet there exists many varied views of exactly what it is. These views are not drastically different, it has simply not been agreed upon and pinned down to a single definition. In a paper over ten years ago, Gordon and Ford attempted tackle the matter in order to address the confusion around the term. They defined cybercrime as "any crime that is facilitated or committed using a computer, network, or hardware device" (Gordon & Ford, 2006).They proposed the division of cybercrime into two types - Type I crime has the following characteristcs:

> *"**1.** It is generally a singular, or discrete, event from the perspective of the victim.*
>
> ***2.** It often is facilitated by the introduction of crimeware programs such as keystroke loggers, viruses, rootkits or Trojan horses into the user's computer system*

> ***3.** The introductions can, but may not necessarily be, facilitated by vulnerabilities.”*

(Gordon & Ford, 2006)

While Type II cybercrime has the following characteristics:

> *“**1.** It is generally facilitated by programs that do not fit under the classification crimeware. For example, conversations may take place using IM (Instant Messaging) clients or files may be transferred using the FTP protocol.*
>
> ***2.** There are generally repeated contacts or events from the perspective of the user.”*

(Gordon & Ford, 2006)

That is, Type I cybercrime is more technological in nature, whereas Type II has a stronger human element to it. These are not distinct categories and occur more along a continuum; at one end (Type I), crimes occur entirely in cyberspace while crimes at the other end may only have a small cyber element to them (Type II), but all that comes in between can be combinations of both to varying degrees.

There have been many papers in the last ten years that have looked at the issues surrounding the definition and classification of cybercrime. For some of these, like Gordon and Ford, it is the sole focus of the study. Examples of these include Ngafeeson (2010), who proposed a motivational model for classification which is intended to help combat cybercrime. Or Poonia (2014), who looked at some of the challenges of that cybercrime provides and proposed a classification of cybercrime into four types, based on the victim of the crime, i.e. crimes against individuals, property, organisations, or society. On the other hand, there are many studies that do not deal with this directly (Aiken, McMahon, Haughton, O'Neill, & O'Carroll, 2015; Diamond & Bachmann, 2015; Leukfeldt, Veenstra, & Stol, 2013) but as a result of discussing cybercrime, like in the case of this study, it becomes necessary to discuss definitions and classification.

Over ten years after Gordon and Ford, Ngo and Jaishankar (2017) discussed the matter that a universally agreed upon definition of cybercrime still does not exist. They highlighted that there are now also a number of terms that are sometimes used interchangeably with cybercrime that serve to muddy the waters further – these are terms such as “computer crime, Internet crime, computer-related crime, online crime, high tech crime, electronic crime, technology crime, and information age crime” (Ngo & Jaishankar, 2017). They do however, agree that Gordon and Ford’s basic definition is the most widely adopted. The image below (Poonia, 2014) illustrates the numerous methods used in cybercrime and highlights just how varied the techniques that fall under the umbrella term of cybercrime are.

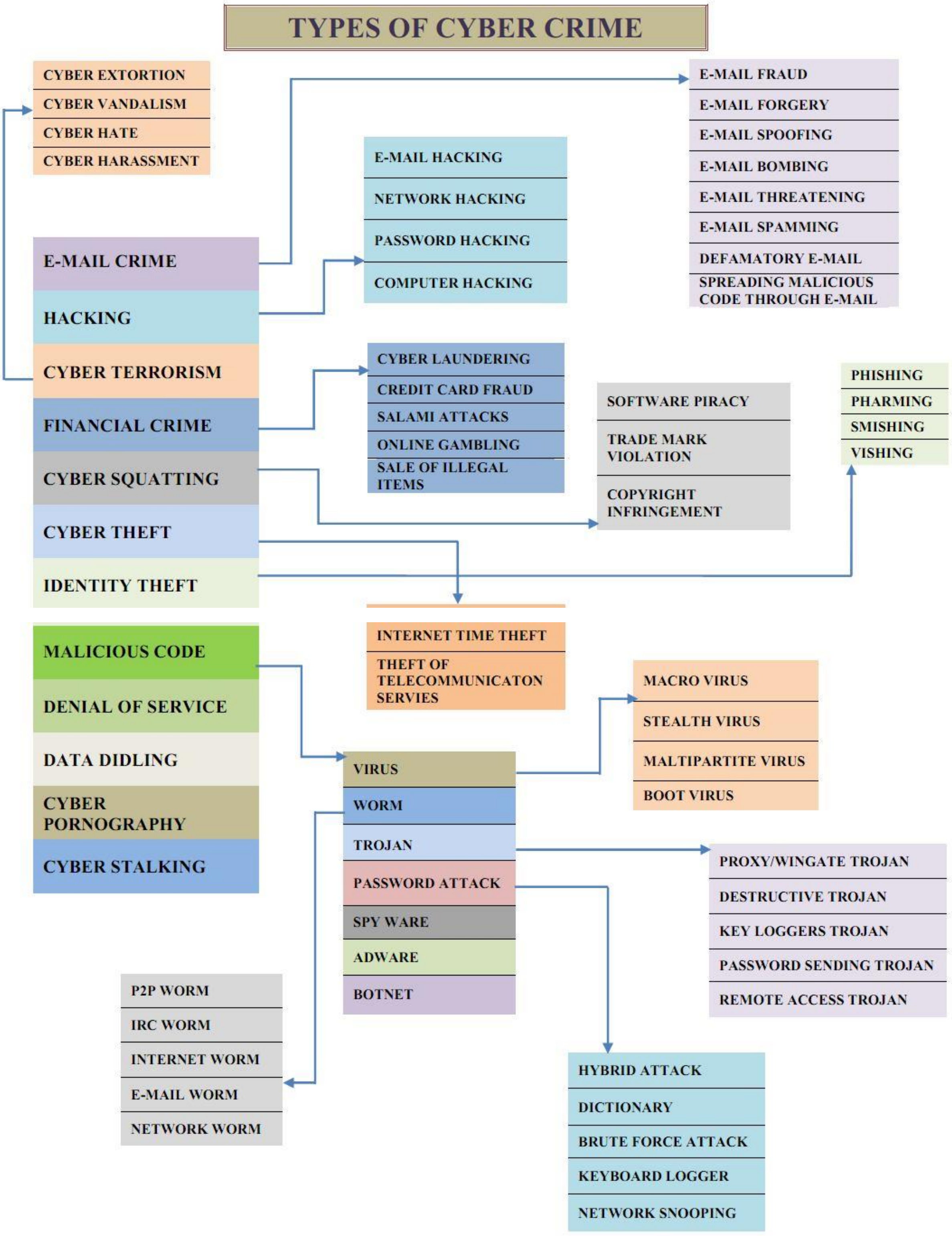


Figure 2-1 Types of Cybercrime (Poonia, 2014)

It is clear that while a broad concept of cybercrime may be understood, there are multiple varying approaches to more a specific definition, and classification. In the context of academia and research, this may not pose a major issue as it stimulates research and further debate, however, in the context of law enforcement, where every attempt is made to prevent cybercrime, this is a significant issue.

Regarding cybercrime, Interpol state:

> *"Although there is no single universal definition of cybercrime, law enforcement generally makes a distinction between two main types of Internet-related crime:*
>
> - ***Advanced cybercrime*** *(or high-tech crime) – sophisticated attacks against computer hardware and software;*
> - ***Cyber-enabled crime*** *– many 'traditional' crimes have taken a new turn with the advent of the Internet, such as crimes against children, financial crimes and even terrorism."*

(Interpol, n.d.)

This broad classification relates quite strongly to the previously discussed classification of cybercrime into Type I (Similar to "Advanced Cybercrime" above) and Type II (Similar to "Cyber-enabled crime" above) from Gordon and Ford (2006). However, as stated by Interpol, this is a distinction that is "generally" made by law enforcement, not a universally utilised one.

This difficulty is further compounded by the jurisdictional issues surrounding the internet as an inherently cross-border technology. Prewitt and Callahan discussed some of these difficulties in a very recent Intellectual Property Law Handbook intended to assist lawyers (Prewitt & Callahan, 2017). They additionally examined some cases that have helped to set some standards for internet cases in the US. The fact that the intended audience of their publication is practicing lawyers, illustrates that it is an area where there is difficulty in ascertaining definite rules. The lack of agreement and the uncertainty surrounding the definition, classification, and jurisdiction determination can present significant barriers to the execution of justice in the fight against cybercrime.

2.3 Hackers and Crackers

2.3.1 Hackers, Crackers, Hacktivists & More

The answer to the question “What is a hacker?” is possibly more contested than the definition of cybercrime, and different answers may vary to a greater degree.

Although quite old, the “*Jargon File*” (The Jargon File (4.4.7), 2003) is as good a place as any to look at hacking related terminology under the context of the current discussion. The contents of the Jargon File have also been published as a book called “*The New Hacker’s Dictionary*” (Raymond, 1996) and it gives a glimpse into the world of hacker culture.

There are many definitions offered for “*hacker*” in the Jargon File however, the general gist of all of the definitions combined is that it relates to someone who enjoys and is an expert in the use of programmable systems, stretching them to their limits, and overcoming or circumventing their limitations. These things may sometimes be done purely for the “*hack value*”, that is, they may seem pointless but are done for the accomplishment of carrying them out.

Hackers that call themselves so under the intent of the definition above would view it as having very positive connotations and conveying curiosity, intelligence, enthusiasm and expertise. This may not coincide directly with what the average non-hacker would consider a hacker to be. At the time of writing, the primary definition found in the Google answer box for the search “what is a hacker” is “a person who uses computers to gain unauthorized access to data” which is quite specific and does not appear to relate very strongly to the previous definition.

However, this is due to some confusion over the term that has become cemented over time, and through repeated use. The Jargon File claims that this arose out of journalistic misuse of the phrase. In an attempt to combat this misuse, hackers (those that would consider themselves of falling under the first definition – provided by the Jargon File) coined the term “*cracker*” sometime around 1985 to represent those who break security on systems (The Jargon File (4.4.7), 2003).

So in short, according to the hacking community, a hacker is good and a cracker is bad. This understanding may not be as clear in the non-hacking community, it is more likely to be that a hacker is thought of as a combination of the two.

Alternative terms used to describe these concepts are "white-hat hacking" "black-hat hacking" and "grey-hat hacking". These terms were derived from Westerns in which the good guys wore white hats and the bad guys wore black ones. Grey hat hackers can fall anywhere along the continuum in between white hat and black hat hackers. For example, it may be that one doesn't carry out any strictly illegal activities, but those activities may be morally questionable. There is additionally the concept of an ethical hacker – this will be discussed later in greater depth – for now, a brief description; Someone who carries out some of the actions of a cracker at the request of or with the permission of the system owner in order to identify security vulnerabilities with a view to fixing them to defend against real crackers.

Another category of hacker that does not quite fit into any of the former classifications is a hacktivist. Whilst having existed since as early as the eighties, hacktivism really came into mainstream focus in the late 2000's with the rise of Anonymous, and the WikiLeaks controversy. Hacktivism is:

> *"..the nonviolent use for political ends of "illegal or legally ambiguous*
> *digital tools" like website defacements, information theft, website parodies,*
> *DoS attacks, virtual sit-ins, and virtual sabotage."*

(Hampson, 2012)

Hacktivism utilises hacking and cracking methods in order to communicate a politically or socially motivated message.

2.3.2 Typology of Hackers

Many researchers have produced typologies of hackers over the years, e.g. (Landreth, 1985; Meyers, Powers, & Faissol, 2009; Rogers, 2006; Rogers, 2011). However, for the purpose of this study it is not necessary to go into the specific details of them or identify the "best" one. Seebruck's typology will be used for the illustration of this point (Seebruck, 2015). The image below represents the typology.

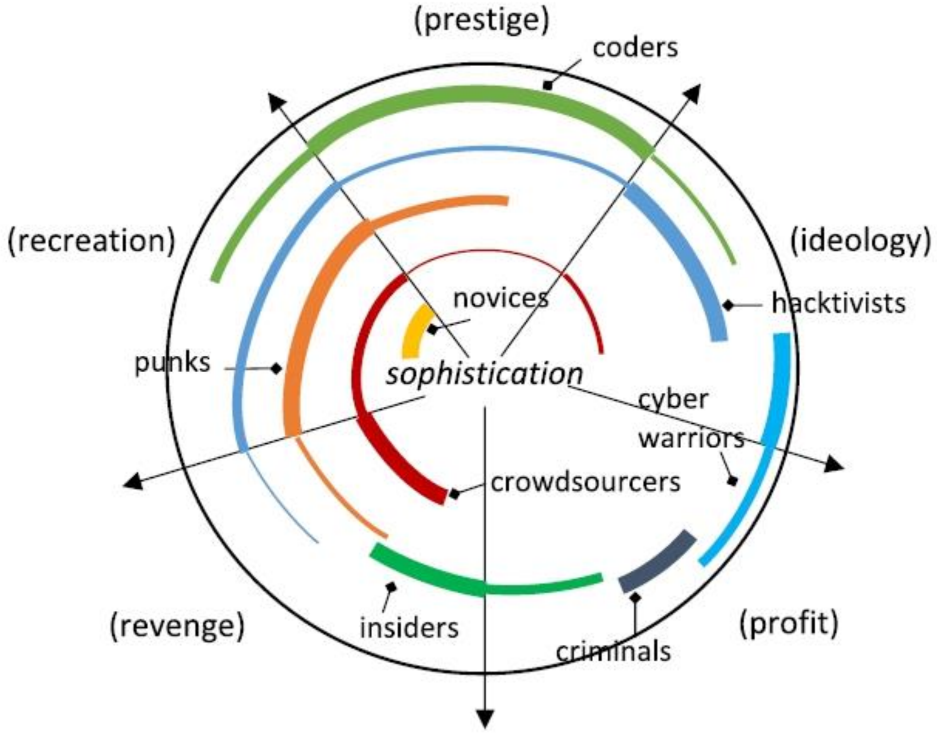


Figure 2-2 Weighted Arc Circumplex of Hacker Types (Seebruck, 2015)

As can be seen from the image, there are many routes to cybercrime and many different motivations. Multiple motivations and avenues of entry into cybercrime, coupled with the online disinhibition effect and the lack of deterrence in cyberspace, both of which will be discussed below, may contribute to an environment conducive to cybercrime.

2.3.3 Anonymous & LOIC

Anonymous, a widely known hacktivist collective, is said to have originated on the website 4chan.org. 4chan is a large internet forum that allows people to post anonymously – If the user does not enter a name in the name field with their post, it is credited as "Anonymous".

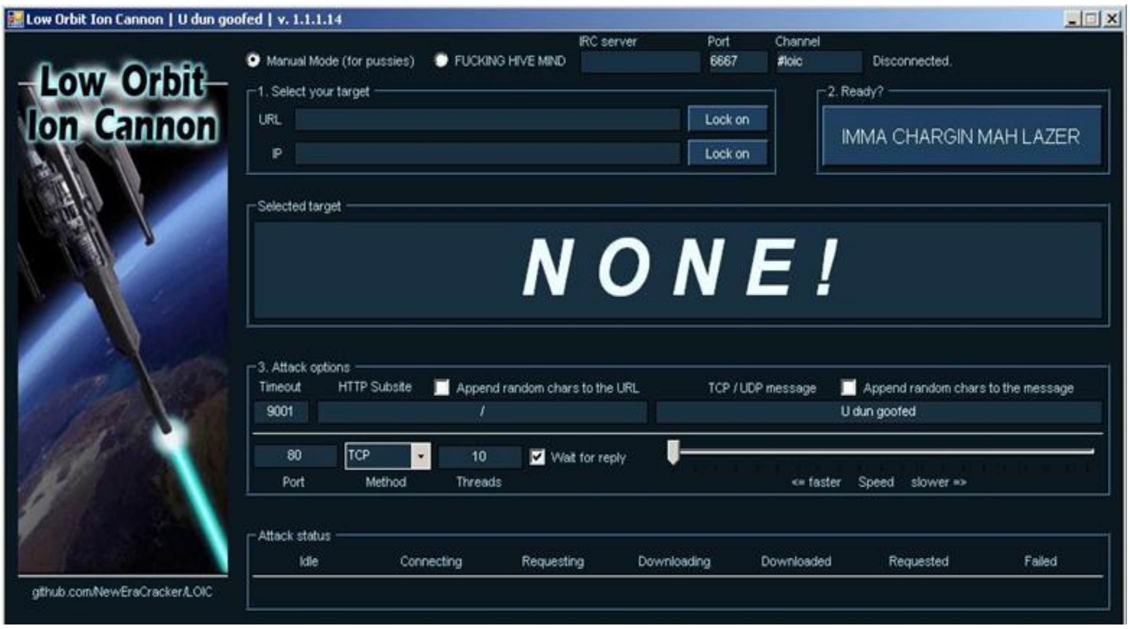
Before embarking on further discussion of Anonymous, it is important to mention DoS and DDoS attacks, the modus operandi of the group. (D)DoS – (Distributed) Denial of Service attacks are quite uncomplicated in concept – They are simply attempts to render a service unusable for legitimate users. This is usually done by overwhelming the infrastructure of the service to the point that the resources fail or are not available for legitimate users. There are multiple approaches to doing this but it is generally done by "flooding" the target with various types of requests. DDoS differs from DoS attacks in that they are carried out from a large number of machines – this can be achieved by compromising these machines and incorporating them into a “botnet” that can be used (generally unbeknownst to the machine owners) by the perpetrator to send large volumes of requests to the target. These attacks pose issues to the victims’ security, continuity and reputation, among other things. (Douglas, Santanna, de Oliveira Schmidt, Granville, & Pras, 2017; Zlomislic, Fertalj, & Sruk, 2014).

Figure 2-3 Anonymous (The Daily Mail, 2015)

As the name might suggest, the inner workings of Anonymous are not intended to be public knowledge so it is difficult to track an accurate and unbiased history of the collective. Many sources report that the groups’ first major operation was “Project Chanology”, a protest in response to the Church of Scientology attempting to remove from the internet all copies of a video of Tom Cruise talking about Scientology in a way that potentially framed the church in a negative light. Anonymous claimed this violated freedom of speech and took a stance against this and some of the other practices that the Church of Scientology is rumoured to engage in. Protests outside Church of Scientology Centres around the world were organised, and multiple DDoS attacks were launched against the church’s website.

There have been many “Operations” from the collective over the years, the victims vary from political figures to corporations. However, the group generally act in defence of freedom of speech and sharing of information on the internet. Operation Payback – in defence of the charges against popular torrent site The Pirate Bay, and WikiLeaks – An Attack on the companies that withdrew their services from WikiLeaks (for the site to receive payments/donations, etc.) are two of the more famous undertakings of the collective. (WikiLeaks is a website, founded by Julian Assange in 2006 that has been used by whistle-blowers such as Assange himself to release classified information to the public). While they are often accompanied by other activities, these operations generally always involved DoS attacks against the victims. (Fuchs, 2014; InfoSec Institute, 2011; Olsen, 2013; Pras, et al., 2010; Stryker, 2011).

In spite of how it may seem, participants in these operations do not need to be adept hackers, or even possess any considerable amount of technical ability. While a majority amount of the "firepower" of their attacks is reported to have come from botnets, there are tools readily available that Anonymous have utilised heavily in order to allow members of all capabilities participate in DoS attacks. A website called Gigaloader was utilised in the groups' early attacks – a browser based tool that was used by copying the target URL into the site and clicking go. This would repeatedly reload the links using up the target sites bandwidth. This website is now defunct, however, a tool called LOIC quickly became the group's tool of choice. LOIC is an open source network stress testing tool, standing for *"Low Orbit Ion Cannon"*, named so after a weapon from many video games, capable of causing considerable destruction. The user gives it a target and it floods that target with "rubbish" requests. LOIC was later given further functionality that allowed users to put it into "HIVEMIND" mode, allowing them to lend their computing power to someone in "command". These users may not even know who they were attacking, just that they were allowing their equipment to be used in the attacks.



Low Orbit Ion Cannon | U dun goofed | v. 1.1.1.14

● Manual Mode (for pussies) ○ FUCKING HIVE MIND

IRC server:
Port: 6667
Channel: #loic
Disconnected.

1. Select your target
URL: [Lock on]
IP: [Lock on]

2. Ready? [IMMA CHARGIN MAH LAZER]

Selected target: NONE!

3. Attack options
Timeout: 9001
HTTP Subsite: /
□ Append random chars to the URL
TCP / UDP message: U dun goofed
□ Append random chars to the message
Port: 80
Method: TCP
Threads: 10
☑ Wait for reply
<= faster Speed slower =>

Attack status
Idle Connecting Requesting Downloading Downloaded Requested Failed

Figure 2-4 LOIC GUI – Main version in use at the time of "Operation Payback" (Pras, et al., 2010)

Two of the hundreds of participants in the DoS attacks against the Church of Scientology were tracked down by the FBI, and eventually sentenced to a year and a year and a day imprisonment respectively. The LOIC readme file was altered at an early stage to include reference to the user operating it at their own risk and that they could be held liable for their actions. One of the defendants sentenced, Brian Mettenbrink, admitted that he knew using the tool against the Scientology website was illegal, but still let it run in the background for a few says, hardly thinking much of it, believing it was very much a minor offense and not realising it could lead to a prison sentence. There are a number of other tools that Anonymous have used and more recent operations that they have undertaken, however the discussion of the LOIC tool is sufficient coverage in the context of this study. (Fuchs, 2014; Hampson, 2012; Olsen, 2013; Pras, et al., 2010; Prendergrass, 2013; Serracino-Inglott, 2013; Stryker, 2011)

2.3.4 Script Kiddies

The LOIC tool provides an example of how tools are being created that enable participation in attacks without requiring any specific knowledge of what is actually being done or how to do it. Individuals that carry out these activities are often referred to as *script kiddies* (Simmonds, Sandilands, & van Ekert, 2004). The Jargon File primarily defines script kiddies as:

> *"The lowest form of cracker; script kiddies do mischief with scripts and rootkits written by others, often without understanding the exploit they are using. Used of people with limited technical expertise using easy-to-operate, pre-configured, and/or automated tools to conduct disruptive activities against networked systems."*

(The Jargon File (4.4.7), 2003)

Therefore, script kiddies are generally only as dangerous as the tools that are available to them. However, in divergence with the physical world, the distribution of online "weapons" (tools for breaking, entering, stealing (usually data) and generally causing damage or disruption) is not restricted to regulated markets, or illegal black markets. With the growth of the industry of *ethical hacking,* these tools can be distributed quite freely regardless of the intended use, or the potential abusive use of the tools.

Some recent events that may have an impact on the distribution of hacking tools in the future are worthy of mention. Taylor Huddleston, the creator of a Remote Administration Tool called NanoCore has recently been indicted. The charges being brought against him are one count of conspiracy and two counts of aiding and abetting computer intrusions. It has been reported that NanoCore has been linked to intrusions in at least ten countries and suggested that Huddleston designed the tool to be used for illicit purposes and marketed it intentionally in online locations frequented by those who would use it maliciously. Intent is the driving force behind the charges as Huddleston was not accused of carrying out any hacking activities himself. Cases such as this one may shape the future landscape of hacking tool availability for script kiddies, but at the current time, there is little regulation or repercussions for the release of hacking tools on the web. (Krebs, 2017; The Daily Beast, 2017; United States of America v. Taylor Huddleston, 2017).

2.4 Hacking Techniques

2.4.1 Social Engineering

Techniques that utilise manipulation, persuasion and influence in order to exploit individuals have been around for a very long time. However, in more recent times, these social engineering techniques have been adopted by crackers in order to do things such as bypass strong security systems, e.g. there's no need to try to crack an access code, or clone a smart card in order to gain access to a restricted area if you can get someone to hold the door open for you (exploiting the general unwillingness of people to close a door in someone's face, particularly if that person is moving with purpose and confidence).

Social engineering is a method of deception that plays on a sense of decency, and exploits the human characteristic that is the tendency to trust (Meinert, 2016). There are a number of social engineering techniques employed in cybercrime. A notorious and widely known cyber based technique is *phishing*.

2.4.2 Phishing

Traditionally an email based attack, phishing has multiple forms, and these are usually used to persuade the victim to part with some personal information or money. These can be emails, websites, phone calls, SMS messages, Wi-Fi Access points, etc. Examples of common approaches are those that send out emails to large lists of people looking for investments or donations, etc., e.g. the notorious "Nigerian scam" in which someone supposedly in authority such as a government official or prince needs your help to get a vast fortune out of the country and will share his fortune with you in return for your help. This help could be providing your bank details for them to use, or "lending" them money required to fund the operation of procuring the fortune, etc. (Stajano & Paul, 2011). These mails can often be poorly crafted even including spelling mistakes as the people that fall victim to them are quite gullible and that is the intention.

Others may be more complex and involve cloned emails (i.e. copies of mails from legitimate organisations) that can sometimes be spoofed (technique to make an email look like it came from someone else) and they can contain links to fake websites that are also clones of the legitimate websites. There are numerous ways in which people obfuscate URLs to fool people. The use of similar appearing domain names and email addresses can be used, and merely taking advantage of the fact that people may not fully understand URL structures and be able to identify suspicious ones e.g.:

www.fakephishingsite.com/example/.www.paypal.com/login.html

Spear phishing is another common approach, in which specific people are targeted. That is, they might already have some information about their targets, e.g. name, phone number, which would be included in a cloned email to encourage the victim to accept it as legitimate as they may be inclined to think that a source other than the legitimate one would not have their personal details. (Abraham & Chengular-Smith, 2010; Banu & Banu, 2013; Dhamija, Tygar, & Hearst, 2006; Ekawade & Mule Snehal, 2016; Garera, Provos, Chew, & Rubin, 2007).

2.4.3 Ransomware

Another phishing attack that is particularly relevant in 2017, is an email that contains malware – the current trend is an email with a file attached that contains a form of ransomware. The email would attempt to convince the target to open the attached file using techniques mentioned above (e.g. cloned emails, spear phishing etc.). There are two main types of ransomware, the first – locker ransomware, locks the device so that it cannot be used and the data on it is generally untouched but inaccessible to the victim, demanding a ransom payment in order to unlock it. The other is crypto ransomware - once executed it spreads through a system encrypting all the files on it. These files are essentially held hostage, although still residing on the victims' computer, they cannot be any use to the victim without a decryption key. The perpetrators will not release this decryption key until a ransom is paid (although there is no guarantee that they will give the key once paid). (Abraham & Chengular-Smith, 2010; Ali, Murthy, & Kohun, 2016; Pathak, 2016; Richardson & North, 2017; Salvi & Kerkar, 2016; Scaife, Carter, Traynor, & Butler, 2016).

While ransomware has been a pertinent threat for some time, it took the worldwide stage on 12th May 2017 with a variation called WannaCry and again on the 27th June 2017 with a variation called Petya. Further details relating to WannaCry and Petya, and what enabled them to spread so rapidly will be discussed in a later section. The images below illustrate the magnitude and widespread nature of WannaCry.

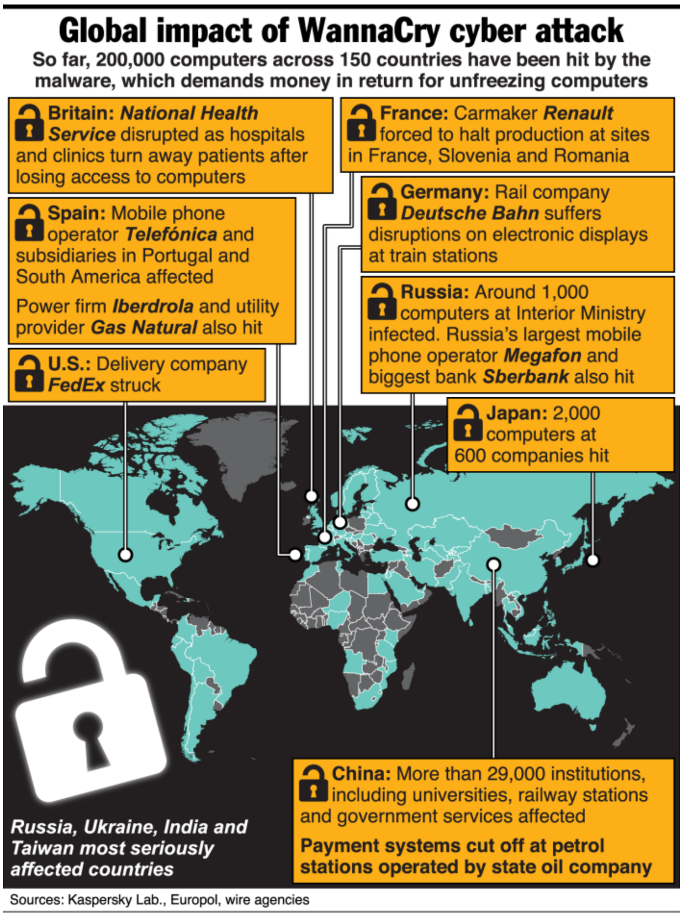

Global impact of WannaCry cyber attack
So far, 200,000 computers across 150 countries have been hit by the malware, which demands money in return for unfreezing computers
Britain: National Health Service disrupted as hospitals and clinics turn away patients after losing access to computers
France: Carmaker Renault forced to halt production at sites in France, Slovenia and Romania
Spain: Mobile phone operator Telefónica and subsidiaries in Portugal and South America affected
Power firm Iberdrola and utility provider Gas Natural also hit
Germany: Rail company Deutsche Bahn suffers disruptions on electronic displays at train stations
Russia: Around 1,000 computers at Interior Ministry infected. Russia's largest mobile phone operator Megafon and biggest bank Sberbank also hit
U.S.: Delivery company FedEx struck
Japan: 2,000 computers at 600 companies hit
China: More than 29,000 institutions, including universities, railway stations and government services affected
Payment systems cut off at petrol stations operated by state oil company
Russia, Ukraine, India and Taiwan most seriously affected countries
Sources: Kaspersky Lab., Europol, wire agencies

Figure 2-5 Global Impact of WannaCry Ransomware (Graphic News, 2017)

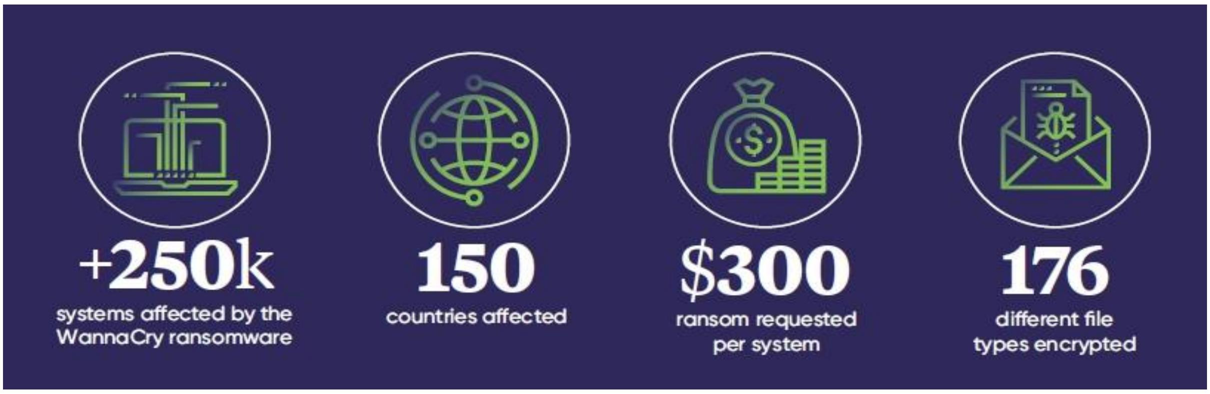

+250k
systems affected by the WannaCry ransomware
150
countries affected
$300
ransom requested per system
176
different file types encrypted

Figure 2-6 Summary Statistics of WannaCry Ransomware (Raconteur, 2017)

2.4.4 Patching

Patching is of vital importance to an organisation's security; when known vulnerabilities exist in systems, it is common that more skilled hackers (both white hat and black) create and make freely available exploits for many of these vulnerabilities. Therefore, the longer a company waits before patching, the more vulnerable they become. A vulnerability statistics report for 2016 was released by edgescan™, a Software-as-a-Service vulnerability management service, based on the continuous assessment of over 57,000 systems distributed globally (edgescan™, 2016). It was found that 36% of host layer vulnerabilities were due to unsupported systems and patching vulnerabilities. The other largest factor was configuration vulnerabilities; these may take skill and knowledge of systems to remediate, which contrasts with the patching issue, as this does not take much skill to remediate and can greatly improve the security stance of an organisation. These statistics were derived from companies that engaged edgescan™ to continuously assess their systems which demonstrates a proactive approach to their security. Therefore these are a kind of "best-case" set of statistics. Organisations that fail to regularly install patches leave themselves vulnerable to all kinds of hackers, script kiddies included.

2.5 Hacking Locales

2.5.1 The Dark Web

The web is made up of what is generally called the "surface web" and the "deep web". The surface web is made up of that which is indexed by search engines and can be accessed with a standard web browser. The surface web makes up a surprisingly small portion of the web – The majority of it is actually the deep web – this consists of a variety of different things, e.g. "staging" or pre-production environments, databases, content that is hidden behind paywalls, etc.

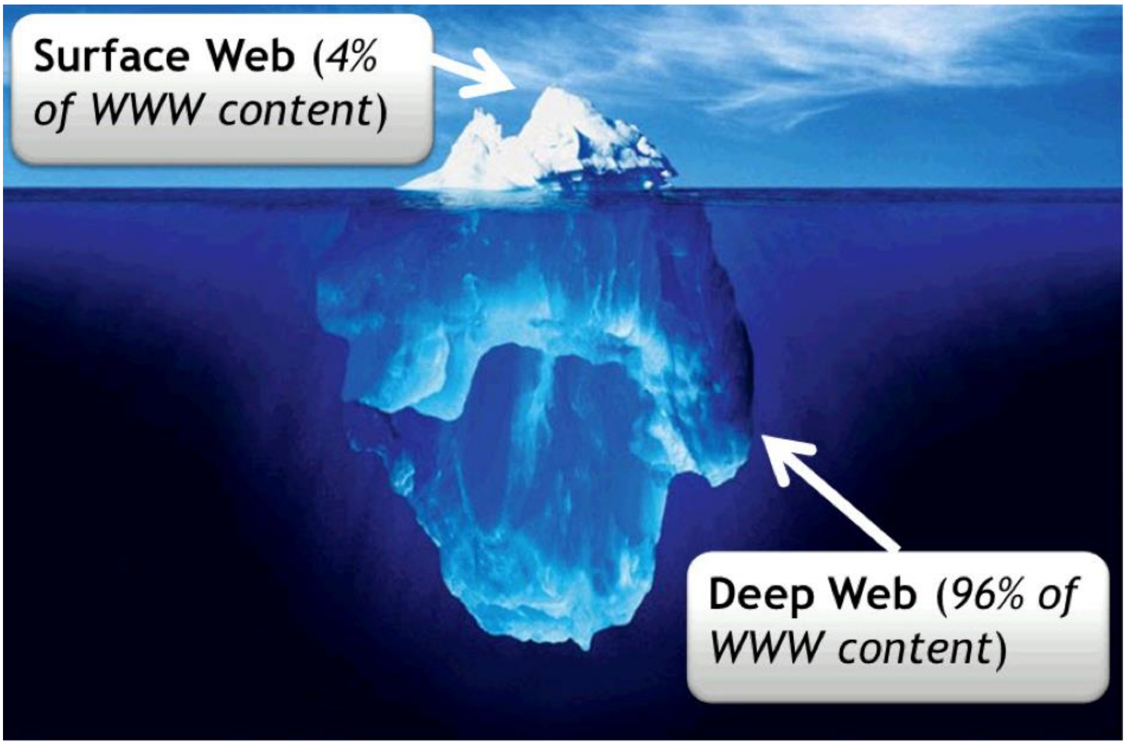

Surface Web (4% of WWW content)
Deep Web (96% of WWW content)

Figure 2-7 Surface web & Deep web (Sagargholap101, 2014)

A small subsection of the deep web is considered the dark web – and can only be accessed using specific software programs, the most popular of those being Tor, which uses multiple processes, including encryption and relaying traffic through up to 6,000 servers to anonymise it. The deep web is used by many for the anonymity it offers such as journalists and whistle-blowers wishing to operate in complete secrecy, possibly for fear of their own safety or otherwise. The high level of anonymity provided also means that the deep web is a haven for criminal operations – all kinds of illegal services can be bought on the dark web, including child pornography, illegal hackers for hire, and illegal drugs. (Chen, et al., 2008; Cole, 2016; Vogt, 2017).

Below is a screenshot of what was one of the most famous illegal drug markets on the dark web, which was shut down by the FBI in October 2013. Drugs of all types and quantities could be bought and sold on Silk Road and Bitcoin was the currency of choice for these transactions. The symbol ฿ is used to denote the currency and can be seen in the screenshot. In spite of the take down of Silk Road, the drug market on the dark web is still thriving. (RAND Corporation, 2016; Lacson & Jones, 2016).

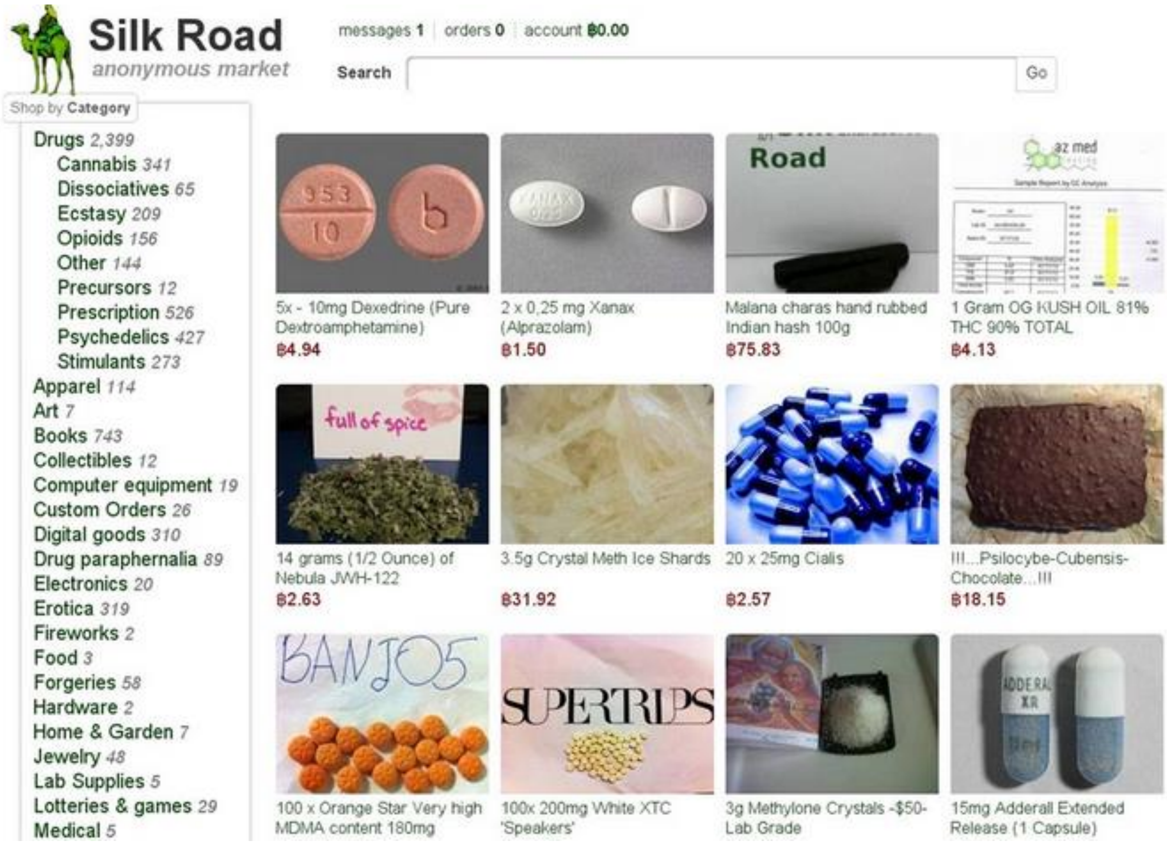


Figure 2-8 Silk Road Screenshot (Krebs, 2014)

2.5.2 Cryptocurrency

As shown in the discussion of ransomware, a ransom of $300 was demanded per each system infected by WannaCry, which would increase rapidly as time passed and the attackers did not receive payment. These payments were to be made in Bitcoin to the perpetrators, as is commonly the choice of currency for criminals online. In the early 2000s and before, online payments were not as easy to orchestrate, and victims would have to use methods such as payment via SMS, mailing prepaid cards, or calling premium rate phone numbers that earned the attackers money. These methods left the attackers quite exposed as these payments could be traced to them. The introduction of Bitcoin in the late 2000s changed this considerably as it made tracing the money to the attacker drastically more difficult and is considered to provide a good degree of anonymity. (Richardson & North, 2017).

Bitcoin was the first decentralised cryptocurrency, and is the most widely known and used one today. Cryptocurrencies are peer-to-peer digital asset systems that use cryptography to generate and distribute currency units (Mukhopadhyay, et al., 2016).

They generally utilise a technology called *blockchain* which allows the cryptocurrencies to be completely decentralised. This means that no one authority or group of authorities "own" the currency, they do not have any control over it. Attempts to create digital currencies prior to Bitcoin had utilised a central authority the same way that non-digital currencies do, e.g. money in a bank account – this is essentially a database entry that is only allowed to be increased by providing the corresponding number of coins and notes (or receiving a transfer etc., but at some point the initial entry that led to it was achieved by providing the equivalent amount of cash) and this is regulated by the bank who are the central authority in this case. Blockchain technologies allowed cryptocurrencies to be completely decentralised; a blockchain is public record of all transactions that have occurred since the first transaction using that currency. This blockchain is distributed (not copied) throughout the peer network and every time a transaction is carried out it must be confirmed and added to the blockchain. The details of how this is done are quite technical and were deemed to go beyond the scope of this discussion – a very high level view of the process is shown in the picture below.

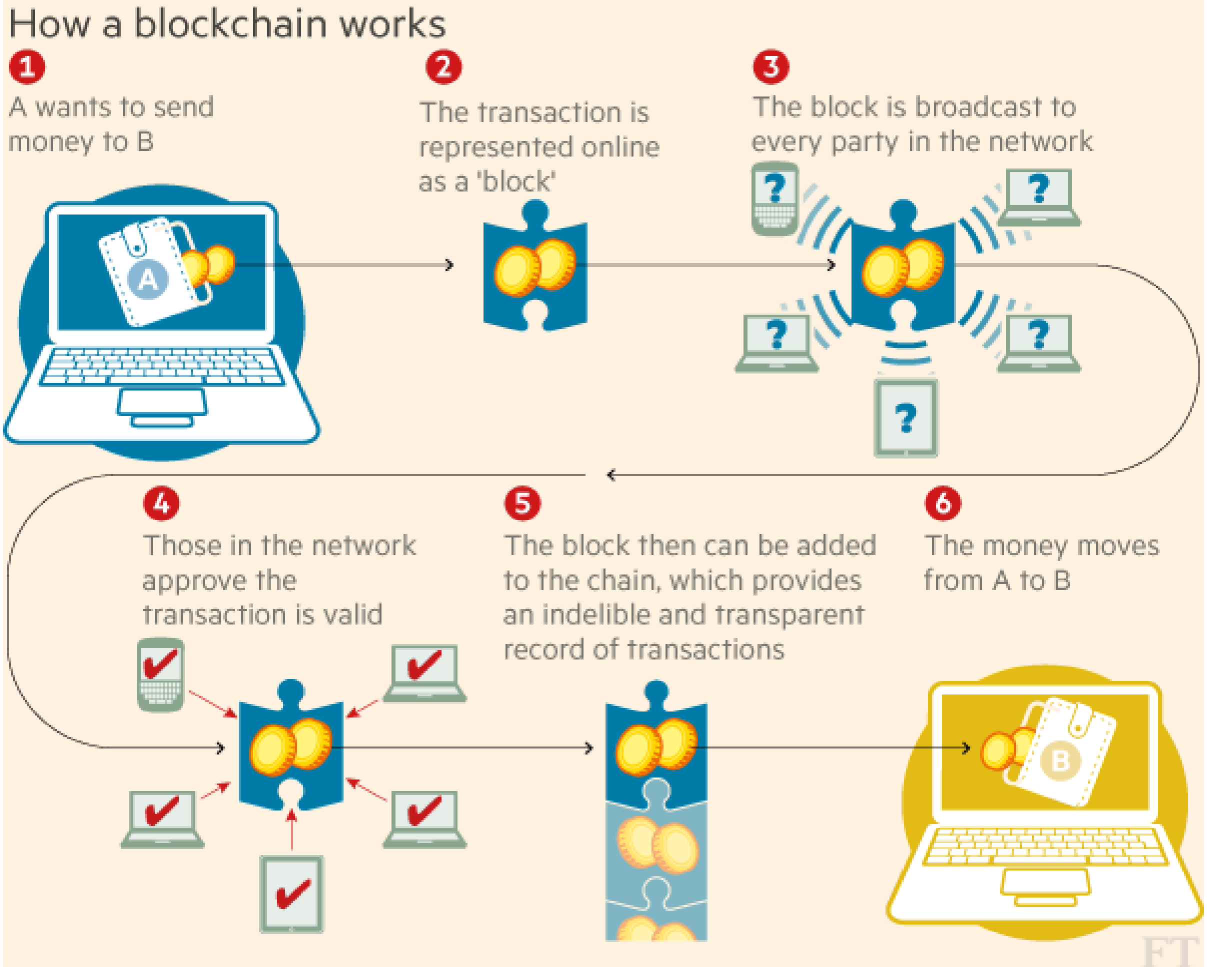

How a blockchain works
1 A wants to send money to B
A
2 The transaction is represented online as a 'block'
3 The block is broadcast to every party in the network
?
4 Those in the network approve the transaction is valid
5 The block then can be added to the chain, which provides an indelible and transparent record of transactions
6 The money moves from A to B
B
FT

Figure 2-9 How a blockchain works (World Economic Forum, 2016)

The result of how it operates is that there is no single point of failure that a malicious hacker can attack and alter. In theory it could be legitimately corrupted, but in order to do this, enough computing power would need to be provided to override the rest of the peer network – A massive and unlikely feat as this would then destroy the value of the currency making it purely a destructive and very costly exercise rather than a profitable one. (Al Shehhi, Oudah, & Aung, 2014; Bjerg, 2015; Mukhopadhyay, et al., 2016; Nakamoto, 2008; Nguyen, 2016). While Bitcoin is the most famous cryptocurrency in use, there are approximately 1500 cryptocurrencies, with Ethereum, Ripple, Litecoin and Monero being some other popular choices (BlockGeeks, 2017).

Bitcoin payments are sent and received from Bitcoin addresses, which are created from the encryption keys that are used for verification of users among other things. It is possible to associate a user's Bitcoin address with their IP address, and in doing so be able to track them down, however, this is not the case if the user is using an anonymising proxy such as Tor [The Onion Router] (Nakamoto, 2008). It is for this reason that Bitcoin is such a popular choice for criminals to receive payments.

2.5.3 The Shadow Brokers, WannaCry and Petya

A discussion of hacking tools and exploits available online is not complete in the current climate without reference to the hacking group called the Shadow Brokers. Note: Most of the details around the Shadow Brokers and events involving them are highly speculative in nature, however, they are included here in order to provide the context of the events and tools. The Shadow Brokers first emerged on Twitter in August 2016 and made a number of "teaser" posts between then and April 2017 in an effort to persuade people to buy access to files that supposedly contained exploits stolen from the Equation Group, a hacking group nicknamed so by Kaspersky Labs and suspected of being tied to the NSA. On April 14th 2017 they released 300MB of Windows exploits to the world-wide web. Many of these were zero day exploits, and within two weeks it was estimated that around 200,000 machines had been infected using some of the backdoor exploits. The tools don't come with clear instructions, but there are many posts appearing online, detailing exactly how to use the tools as people go through the source code and figure it out. (CyberScoop, 2017; Engadget, 2017; The New York Times, 2016; van der Walt, 2017)

The widespread impact of the 12th May 2017 WannaCry ransomware attack was illustrated in the "Ransomware" section above. One of the Shadow Broker's exploits known as ETERNALBLUE was utilised by WannaCry and it was this that allowed it to propagate so rapidly and so widely. Microsoft had released patches that remediated against vulnerability to ETERNALBLUE a month previously and the propagation of WannaCry suggests that these updates were not applied by many companies. Furthermore, over a month later, on 27th June 2017, another widespread ransomware attack broke out. This attack utilised an altered version of a ransomware strain known as Petya and also utilised the ETERNALBLUE exploit. It is unknown how many machines were affected but it is thought to have focused targeting on Russia and Ukraine where more than 80 companies were attacked initially but also affected companies in other countries such as Germany and the UK. (ARS Technica, 2017; Wired, 2017; ZD Net, 2017). The success of both of the attacks, although particularly the Petya attack highlight the less than adequate approach to patching that many companies employ.

2.6 Hacking Perceptions

2.6.1 Ethical Hacking

The basic concept behind ethical hacking; that is, thinking like the opponent in order to anticipate and counteract their moves, dates back hundreds of years. Ethical hacking itself was utilised from the early days of the development of computer systems. One of the earliest known ethical hacks was organised by the US Air Force in order to test the Multics Operating System in 1974 (Chandrika, 2014). The practice continued to evolve over the years and is now an established industry. A definition of ethical hacker activities by Palmer offers a good description of what they do:

> *"..'ethical hackers' would employ the same tools and techniques as the intruders, but they would neither damage the target systems nor steal information. Instead, they would evaluate the target systems' security and report back to the owners with the vulnerabilities they found and instructions for how to remedy them."*

(Palmer, 2001)

Hiring an ethical hacker to evaluate a security system involves placing trust in them – Picture the situation where an ethical hacker finds a vulnerability that enables them to access important confidential data; the ethical hackers must be trustworthy and in possession of sound moral judgement so that it can be trusted that they do not steal any of the data they come across. Additionally, it needs to be relied upon that they will not inform any malicious actors of the vulnerabilities found before the customer has remediated them (or after, but this is more a confidentiality matter than an immediate threat to the system). It is also important that ethical hackers carry out their jobs safely. Testing is sometimes carried out on pre-production environments, but it is often carried out on live production environments. Testing and scanning can sometimes use up considerable resources on the target, therefore care must be taken not to inadvertently "break" anything. Normal operations should not be adversely affected by the testing. Therefore it is important that ethical hackers know the limits of systems, and what is reasonable to carry out and what may cause damage, etc. (Curbelo & Cruz, 2013; Jamil & Khan, 2011; Saleem, 2006).

In the 2000's ethical hacking was growing more popular as a security management technique and it was becoming more common that universities and other institutions would teach ethical hacking techniques to students studying security and other relevant courses. During this time there was a surge in research focusing mainly on the ethics of teaching students to hack, and whether this was something that universities should be engaging in. (Curbelo & Cruz, 2013; Dimkov, Pieters, & Hartel, 2011; Jamil & Khan, 2011; Livermore, 2007; Logan & Clarkson, 2004; Logan & Clarkson, 2005; Pashel, 2006; Poteat, 2005). However, it appears that a consensus has been arrived at that it may be the best method for finding and addressing vulnerabilities and therefore bolstering the security of organisations, as there has been little to no research in more recent years raising those questions.

As mentioned above, most of the research raising questions about ethical hacking focused mainly on whether it was a good idea or ethical to teach it to students as that could potentially just be arming them with the knowledge of how to be better at illegal activities they may carry out. However, there has been little research looking at the repercussions outside of educational institutions.

The result of the widespread use of ethical hacking means there has been considerable growth in the amount of tools and informational resources on the web. Regardless of the intent of the creators, these tools and resources are now available for anyone to use – this makes it quite easy for script kiddies to find tools to carry out malicious acts with. There is a notable gap in research of the implications in this area.

2.6.2 Online Behaviour: The Disinhibition Effect and Other Theories

Another factor to consider when looking at online resources that enable malicious acts is human behaviour on the internet. That is, how do people behave differently on the internet? Are they more or less likely to engage in illegal activities? Suler (2004) proposed a theory of six psychological factors that interact and cause an "*Online Disinhibition Effect*" – The lowering of behavioural inhibitions that occur online (Alonzon & Aiken, 2004; Chesney, Coyne, B., & Madden, 2009; Hollenbaugh & Everett, 2013; Lapidot-Lefler & Barak, 2012; Reinig, Briggs, & Nunamaker, 1998; Udris, 2014; Wu, Lin, & Shih, 2017).

Disinhibition can work in two ways – *benign disinhibition*, or *toxic disinhibition*. As the name suggests, benign disinhibition manifests itself in seemingly positive ways such as uncharacteristic acts of kindness or generosity, or a willingness to share personal emotions, experiences, etc. Toxic disinhibition on the other hand manifests itself in more negative ways, such as rude, harshly critical, or threatening behaviour. Individuals displaying toxic disinhibition may visit places online that they would not visit the equivalent of in the physical world (e.g. of violence, crime, etc.). Toxic disinhibition is the phenomenon that could lead to an increased likelihood to participate in illegal hacking activities online.

Suler's six psychological factors that interact and cause the online disinhibition effect are

- *Dissociative anonymity* – By virtue of being anonymous online, personal features or characteristics that may usually restrict a persons' behaviour (consciously or not) do not need to be revealed. People are free to carry out behaviours that they feel may not usually be available to them e.g. due to expectations or constraints on them in their social environment (Hollenbaugh & Everett, 2013; Lapidot-Lefler & Barak, 2012; Suler, 2004; Wu, Lin, & Shih, 2017).

- *Invisibility* – There are two levels to this invisibility. The first is that a user can go places without people knowing they are there, e.g. one can spend hours on a chat forum without anyone knowing they are there if they do not post anything. The second is that even in the situations where users have posted and even revealed personal details, with the exception of video communications, they still cannot be physically seen when they act or communicate online. (Suler, 2004; Wu, Lin, & Shih, 2017).

- *Asynchronicity* – Online interactions do not generally occur in real time. Users can take their time for example in responding to text comments etc., or they can choose not to return to a conversation until they are in a particular mind-set. This allows people to avoid the immediate reactions of others that tend to guide behaviour towards social norms (Suler, 2004).

- *Solipsistic introjection* – As users do not know what other users look/sound like etc. they may read text from other users in their own voice in their head which can potentially lead to a merging process and possibly transference. Internal representations of other users are made up only partly of how those users present themselves online, but also how the user perceiving them expects, needs or wants them to be. (Joinson, 2007; Suler, 2004; Wu, Lin, & Shih, 2017).

- *Dissociative imagination* – The nature of the online world allows users to easily dissociate from it if they so wish, and when this property is combined with solipsistic introjection, it leads to a separation of the online world and the "real" world in a user's head. This online world can be perceived as a fictional one that can be left behind (along with all of the users actions in that world) if the user so wishes. This effect magnifies disinhibition (Suler, 2004; Wu, Lin, & Shih, 2017).

- *Minimisation of status and authority* – Authority figures are generally expressed within environmental settings through mediums such as dress and body language. However, online, these cues do not exist and the appearance of authority is minimised. Relationships are judged to be more like peer relationships which means that people are more likely to speak or act out (Suler, 2004).

There are other theories of how behaviour is altered in cyberspace, such as Jaishankar's "Space Transition Theory" which at first glance appears to be a different theory altogether, but upon closer inspection, it is apparent that the theory is largely an alternative expression of similar ideologies (Jaishankar, 2008). A dissection of the differences of various theories was deemed to be outside of the scope of this research as the concern in this case is not around the how or why of the matter, but simply the fact that the matter exists. The matter being the lowering of behavioural inhibitions online, often in a negative manner which is confirmed to exist by the theories.

There are many phenomena which can contribute to toxic disinhibition, such as *deindividuation*; a theory of behaviour that originates in social psychology as far back as the late 1800s, although not necessarily under the name of deindividuation (Le Bon, 1896). The theory proposes that it is a decrease in self-awareness and evaluation that occurs in groups. The theory does not apply solely to negative behaviour, however, much of the research has focused on that area. Studies have found that anonymity is a key factor (Dodd, 1985), and looked at interactions and resulting behaviours such as obedience, violence, antinormative online behaviour, and even genocide (Haney, Banks, & Zimbardo, 1972; Kiesler & Sproull, 1992; Milgram, 1963; Silke, 2003; Staub, 1996; Zimbardo, 1969). A more recent model of deindividuation called the *Social Identity Model of Deindividuation Effects* (SIDE) was proposed in 1995 (Reicher, Spears, & Postmes, 1995) which challenged aspects of the traditional model of deindividuation, however, all theories agree that deindividuation can lead to antinormative and disinhibited behaviour (Postmes, 1998).

These theories illustrate how groups such as Anonymous grow and result in a large group of users, willing to participate in illegal activities, as research in those areas has found that computer mediated communications (CMCs) "*provide a channel of social support fostering resistance*" (Spears, Lea, Corneliussen, Postmes, & Haar, 2002). This could also potentially be applied to hacker forums.

Social influence also impacts behaviour – the pressure that people perceive from others that motivates them to carry out, or not to carry out certain behaviours. There are a number of aspects to these influences. The *subjective norm* relates to the person's perception of what the people important to them would think of them carrying out the behaviour (Fishbein & Ajzen, 1975). The *descriptive norm* relates to what a person perceives as being normal in society – a standard that people do not want to deviate from, therefore deviant behaviour is that which is not "in line" with the norm (Berkowitz, 2004). The impact of this may be different on the internet due to the interaction with the online disinhibition effect and deindividuation (e.g. the internet could be a potential "secret" outlet for behaviours that would otherwise be avoided due to subjective norms).

Containment theory is another theory governing behaviour that is particularly relevant to behaviour on the internet. This is based on the assumption that the tendency to commit deviant behaviours is inherent in everyone. It proposes that the combination of strong *inner containment* and reinforcing *outer containment* combine to keep behaviour within societal norms (Reckless, 1961; Thompson & Dodder, 1983). Inner containment refers to a person's ability to affect their behaviour through self-control. Outer containment is the ability of society to confine behaviour to within the norms through three aspects – internalisation of rules, availability of meaningful roles and group reinforcement (Reckless, 1973). Outer containment can also be explained by deterrence theory (Wu, Lin, & Shih, 2017). That is, if punishment is swift, certain and severe, rational behaviour would involve weighing up the gains and losses associated with a criminal action and deciding not to engage in the activity as the potential losses outweigh the gains. There has been considerable research recently indicating that there is insufficient deterrence in cyberspace and that this is conducive to cybercrime (Carlin, 2015; Goldman & McCoy, 2016; Wilson, Sobesto, & Cukier, 2015).

2.6.3 Perceptions of Cybercrime

The perception of cybercrime also plays an important role in the likelihood of individuals to participate in these illegal activities online. It acts as a deterrent in itself if an individual perceives one act to be much more serious than another regardless of the punishment. There have been few studies into the perception of cybercrime. However, cybercrime is considered a subtype of white collar crime and there have been investigations into the perceptions of white collar crime. The results of these studies have been interesting, suggesting that the majority of people feel that white collar crime warrants punishment to a lesser degree than violent crime for example. However, people also express concern that white collar crime is a serious issue and that governments etc. should devote more resources to fighting it (Holtfreter, van Slyke, Bratton, & Gertz, 2008; Michel, 2016). It is not certain if these results can be applied directly to cybercrime, while it is classified as a subtype of white collar crime, it may be that it warrants its' own category. Nonetheless, research in the area is lacking significantly.

2.6.4 Cybercrime: Rates and a Notable Incident

It is uncertain the amount of individual users that fall victim to cybercrimes as they are often unlikely to be reported and may even go undetected. It is also difficult to estimate the incidence rates of cybercrimes against organisations for similar reasons; they can sometimes go undetected, and companies often do not report cybercrime for fear of the impact it will have on their reputation and their customers' confidence in them. In spite of this, it is known that the rates are increasing. The Internet Crime Complaint Centre

(IC3) in the US releases an annual report on the complaints they receive. In 2003 the total number of complaints received was 124,509 with an estimated loss of $125.6 million in total (IC3, 2003), while the 2016 edition of the same document reports 298,728 total complaints with losses in excess of $1.3 billion (IC3, 2016). This indicates that not only have the rates of cybercrime increased, but also the financial cost of falling victim to a cybercrime.

PWC conducted a survey of over 6000 organisations in 2016 and found that 36% of these organisations reported being victim to economic crime. Of this 36%, cybercrime is now the second most prevalent form of economic crime, comprising of 32% of these. This number has increased from the 24% it was reported at by PWC in 2014 (PWC, 2016).

One particular cybercrime incident discussed in a Verizon 2016 report is particularly relevant to this study (Verizon, 2016). A global shipping conglomerate fell victim to a number of attacks from pirates. This is not uncommon for shipping companies, however, what was unusual about these cases was that the pirates had prior knowledge of the contents of the containers and so were able to locate the containers that contained the most valuable cargo almost immediately. It was discovered that a malicious web shell had been uploaded to the company's Content Management System server using an insecure upload script and from this they were able to upload and download data and execute commands on the server. However, there were a number of notable points about the attack:

1. They did not enable SSL on the web shell so it was possible to recover all of the commands they executed as they were sent in plaintext.
2. From these captured commands, it was discovered that the attackers were not very competent hackers; numerous mistyped basic commands were observed and a general difficulty in interacting with the server.
3. In spite of obtaining password dumps, they attempted multiple times but were unable to move laterally within the network.
4. The attackers did not use a proxy and connected directly from their home system so they were very easily traced.

These factors indicate that the attackers in this case were script kiddies, and highlights the fact that even unskilled hackers can capitalise on vulnerabilities and unpatched systems.

2.7 Conclusions

In this chapter, a range of literature related to cybercrime was explored. First the definition of cybercrime was discussed as there is not a universal standard definition. Some of the key terms such as hacker, cracker and others were discussed as well as some key methods such as social engineering and phishing. Ransomware was covered as it is a particularly relevant method of attack in light of recent events with WannaCry and Petya (May & June 2017). There was also a glimpse into cryptocurrency, the dark web, and the criminal markets that it is home to, a haven for criminals and cybercriminals alike.

A discussion of Anonymous and some of their operations highlighted how collectives such as Anonymous, in their effort to enable anyone to participate in their activities, contribute to the propagation of powerful, simple to use hacking tools. These tools are then readily available on the world-wide web for anyone to use, and an example of a group that does make use of these tools for malicious purposes is script kiddies. In addition to this, the growth of the industry of ethical hacking has also created an environment online full of easily accessible tools and resources for hacking that can also be used by anyone with malicious intent.

Human behaviour on the internet is an important factor in the examination of what might lead a participant to engage in cybercrime. The online disinhibition effect is a key theory that dictates and explains a lowering of behavioural inhibitions online which play an important role in the decision to engage in malicious activities. In addition to this, an individual’s perception of the seriousness of cybercrime may also play a role in this decision, although there is very little research on these perceptions. It was confirmed that the rate and extent of cybercrime is increasing and that unpatched systems are a major issue for organisations as it leaves them vulnerable to attacks from all levels of hackers, including unskilled ones such as script kiddies, operating simple scripts or tools. The review of the literature on behaviour on the internet allows for a conclusion to be drawn on the first research sub-question that people are more likely to engage in criminal behaviour online than they are in the physical world.

3 EXPERIMENTAL DESIGN: HACKER RESOURCES REVIEW AND ANALYSIS

3.1 Introduction

Following the review of literature concerning cybercrime presented in the previous chapter, this chapter will look at identifying some of the free hacking resources that are available on the world-wide web as these resources not only assist the white hat hackers they may be intended for, but also provide education and tools for hacking to more malicious actors such as script kiddies. These resources will be broken down into tools and educational resources. The tools will be assessed based on a number of factors such as usability by a script kiddie, remote usage, target, and more. The topics covered by educational resources will be assessed in addition to recording the actions necessary in order to view the course content such as registering with an email address. This information will also be fed into the *Cybercrime Survey* for assessment of awareness and opinions.

3.2 Overview

One of the key aims of this research is to determine the public perception of cybercrime, and in particular, how it compares to more traditional crimes. In order to achieve this aim the Cybercrime Survey was designed and developed based on a combination of three factors; (1) addressing the objectives of this research project, (2) using previous research as a central guide, and (3) based on the themes uncovered during the review of the Kali Linux distribution. The topics that the Cybercrime Survey aimed to cover were perceptions of cybercrime and non-cybercrime, and awareness and opinions on the availability of hacking tools and resources freely available on the world-wide web. Information for these questions was obtained from the other stream of research which assessed hacking resources available on the internet. In addition to this, other measures were also taken in the Cybercrime Survey; "lawfulness", an internet attitude measure, and a small amount of demographic information.

Another main aim of this research is to assess resources available on the world-wide web that can facilitate script kiddies. In order to do this, the resources were separated into two categories; tools, and courses. Given the nature of hackers as discussed in the literature review, many solutions are created for hacking related tasks by hackers, and these are often then circulated to the community free of charge on sites like GitHub or Sourceforge for others to make use of. Therefore, the development and production of hacking tools is not necessarily restricted to software companies. This means that there is a plethora of tools available on the internet. Some of them are large comprehensive solutions, and others are small command line tools designed for a single specific purpose. It would be infeasible to attempt to identify and analyse all of these tools. In order to identify the tools that should be assessed, some initial research was carried out on Google to assess what was popular; what was being talked about in forums, included in "Best Tools" lists etc.

Rather than finding, downloading, installing and configuring tools for use, repeated recommendations were observed for installing and using operating systems pre-configured for penetration testing. Of the penetration testing focused operating systems, the Kali Linux distribution was observed to place at the top of all the "Best of" and "Recommendation" lists. Therefore, the tools that were selected for assessment were all the tools that come pre-installed in Kali Linux.

Regarding the selection of courses, the main criterion for selection was that they were free courses. It is likely that there is an abundance of videos, short guides, forum discussions, etc. for specific tasks, however, the other main selection criteria were courses with structured content and predefined learning outcomes or syllabuses. Standalone videos such as those that might be found on YouTube or SecurityTube were excluded.

3.3 Kali Linux Distribution

3.3.1 Overview

Kali Linux is a popular Linux distribution intended for use in penetration testing and security auditing. It is founded, funded and maintained by Offensive Security, a company that provide offensive security (i.e. penetration testing) training, certifications and services. Kali Linux is free to download and install from www.kali.org/downloads and can be downloaded in many versions including 32-bit, 64-bit, 32-bit Light, 64-bit Light and more. There are also "flavours" of Kali Linux available that are tailored for use in VMWare, VirtualBox and ARM architecture.

Figure 3-1 Kali Linux Background

The subdomain tools.kali.org on the Kali Linux website contains documentation of all the tools that are pre-installed in Kali Linux. Some of the tools have extensive information on the documentation pages and others have the bare minimum. This was the main source of information for this assessment.

A table was created containing all the names of the tools on the "Kali Linux Tools Listing" page (tools.kali.org/tools-listing). This table contained 275 tools that were assessed. A brief description of the functions of the tool was added to each tool in the table. These were not exhaustive descriptions but they give a good indication of the main function(s) of the tools. The tools were then classified across a seven categories; (1) *Single Script Kiddie*, (2) *Category*, (3) *Target*, (4) *Remote Execution*, (5) *Requires Machine Compromise*, (6) *Requires User Interaction*, (7) *Escalation to Physical Attack*. The meaning of each of these classifications within the context of this study are explained below:

- *Single Script Kiddie* – This classification had two options; *Yes* or *No*. The assumption was made that a script kiddie possesses only basic knowledge about common technologies and basic command line skills. Any tool that required coding input or the understanding of coding or other knowledge above the basic level that a script kiddie might possess was given a value of *No*. Any distributed or multiuser tools were also given a value of *No* as the focus was on the capability of a single script kiddie to execute the tool successfully. Tools that were relatively simple to execute or were accompanied with clear instructions for usage were given a value of *Yes.*

- *Category* – There were twelve categories to this classification; (1) *Attack Building & Examination*, (2) *Attack Maintenance & Data Extraction*, (3) *Authentication Attack*, (4) *Collaboration, Information Management & Reporting*, (5) *Deception Attack*, (6) *Information Gathering*, (7) *Malicious Injection*, (8) *Miscellaneous*, (9) *Network Attack*, (10) *System/Device Attack*, (11) *Web Application Attack*, (12) *Wireless Hacking*. The category names are self-explanatory; each tool was classified into one of the twelve categories based on its function.
- *Target:* This was divided into three categories; (1) *Generic*, (2) *Corporate* and (3) *Personal*. This was derived from the fact that some software or systems are likely to only exist in corporate environments. It is not impossible for them to be in use in a personal setting, but highly unlikely. Any tools that targeted these kind of technologies was classified as *Corporate*. Alternatively, there are some technologies that may be corporate owned, but the attack the tools execute against them may target individuals using these technologies rather than the corporation that owns them (e.g. web session hijacking – the website is "corporate" owned, but the victim of the attack is an individual user). Tools that executed these kind of attacks were classified as *Personal*. If the tool could be used to target at either the corporate or personal level, it was labelled as *Generic*.
- *Remote Execution* – This classification focused on what location was needed for execution of the tool. If the tool could be executed successfully remotely, then it was given a value of *Yes*. If the tool required physical, local or adjacent access for successful execution it was given a value of *No.*
- *Requires Machine Compromise* – Some tools are intended for use after a target has been compromised, e.g. data extraction or attack maintenance. Tools that perform these functions were given a value of *Yes* while all others were given a value of *No.*
- *Requires User Interaction* – Tools that required target user interaction in order to execute the attack successfully were assigned a value of *Yes* in this classification, e.g. user needs to click a link in order to execute a cross-site

scripting attack. Attacks that do not require any target user interaction were given a value of *No*.

- *Escalation to Physical Attack* – If the use of a tool increases the possibility of or is likely to lead to a physical attack based on information gained through the use of the tool or otherwise, the tool was given a value of *Yes*, e.g. scanning for locations of Bluetooth devices (could lead to attempted robbery of devices, or locating a specific person for attack, etc.). A value of *No* in this category does not mean this is not possible, it is just unlikely to be the intention or outcome of the attack.

The *Escalation to Physical Attack* Category was created after the assessment had started, and tools that had already been evaluated across the other categories were then evaluated for this category. After encountering the first tool that possessed this possibility, it was deemed to be relevant enough to warrant the extra category.

3.3.2 Analysis of Kali Linux Distribution

As part of this research project the Kali Linux distribution was analysed in some detail, and each of the tools documented and categorised. The purpose of this was two-fold, firstly to more clearly understand the types of tools that are available to novice hackers, and secondly, to help create questions for the survey part of this research.

275 tools that come pre-installed in the Kali Linux distribution were assessed and classified across seven categories; (1) *Single Script Kiddie*, (2) *Category*, (3) *Target*, (4) *Remote Execution*, (5) *Requires Machine Compromise*, (6) *Requires User Interaction*, (7) *Escalation to Physical Attack*

The table below shows the breakdown and totals of the *Single Script Kiddie* classification by each *Category*.

Category	**Single Script Kiddie ["No"]**	**Single Script Kiddie ["Yes"]**	**Grand Total**
Attack Building & Examination	14	12	26
Attack Maintenance & Data Extraction	-	23	23

Authentication Attack	-	26	26
Collaboration, Information Management & Reporting	2	15	17
Deception Attack	-	6	6
Information Gathering	-	38	38
Malicious Injection	-	1	1
Miscellaneous	-	6	6
Network Attack	2	59	61
System/Device Attack	-	11	11
Web Application Attack	-	43	43
Wireless Hacking	-	17	17
Grand Total	18	257	275

Table 3-1 Tool Categories broken down by Script Kiddie Usability

As can be seen, the majority of the tools are likely to be usable by script kiddies. Within this classification, in addition to those that required more advanced technical knowledge or skills, tools that are used for collaboration or required multiple users were also given a value of "*No*" in the *Single Script Kiddie* category. This is because the focus in this study is on script kiddies working alone.

Another interesting statistic is that derived from the *Escalation to Physical Attack* classification. The tools that were given a "*Yes"* value in this category are those that can or are likely to be used to establish a device's location. This could potentially be used to track a certain person in an area, or find people with specific devices e.g. in order to steal the devices. Three of the tools were given a value of "*Yes"* in this category, a very small fraction (Less than 1/90), however, as long as there is at least one tool that has this functionality then it is possible that attacks can be carried out. All of the tools that met this classification were Bluetooth based tools.

The table below contains only the counts for tools that were given a value of "*Yes"* in the *Single Script Kiddie* Category, summarised across the "*Category*", "*Remote Execution*" and "*Target*" classifications.

	Remote Execution ["No"]			**Remote Execution ["No"] Total**	**Remote Execution ["Yes"]**			**Remote Execution ["Yes"] Total**	**Grand Total**
Category	**Corporate Target**	**Generic Target**	**Personal Target**		**Corporate Target**	**Generic Target**	**Personal Target**		

Attack Building & Examination	-	11	-	11	-	1	-	1	**12**
Attack Maintenance & Data Extraction	-	8	-	8	-	14	1	15	**23**
Authentication Attack	2	8	1	11	2	12	1	15	**26**
Collaboration, Information Management & Reporting	1	6	-	7	1	7	-	8	**15**
Deception Attack	-	-	-	-	1	4	1	6	**6**
Information Gathering	1	8	-	9	22	7	-	29	**38**
Malicious Injection	-	1	-	1	-	-	-	-	**1**
Miscellaneous	-	3	-	3	-	3	-	3	**6**
Network Attack	3	16	1	20	10	28	1	39	**59**
System/Device Attack	3	1	-	4	5	1	1	7	**11**
Web Application Attack	-	-	-	-	40	3	-	43	**43**
Wireless Hacking	-	9	8	17	-	-	-	-	**17**
Grand Total	**10**	**71**	**10**	**91**	**81**	**80**	**5**	**166**	**257**

Table 3-2 Multiple Category Summaries for all Script Kiddie Usable Tools

As seen in the table, the majority (78%) of the tools that cannot be executed remotely can be used to target either individuals or organisations. The majority (65%) of the tools can be executed remotely, just under half of which (48%) can be used to target both individuals and organisations.

The final table in this section represents a count of all the tools that meet the following criteria; (1) Usable by a single script kiddie, (2) Can be executed remotely, (3) Does not require target user interaction, (4) Does not require the target machine to have already been compromised.

Category	**Grand Total**
Attack Building & Examination	**1**
Attack Maintenance & Data Extraction	**6**
Authentication Attack	**14**

Collaboration, Information Management & Reporting	**8**
Deception Attack	**2**
Information Gathering	**29**
Miscellaneous	**2**
Network Attack	**38**
System/Device Attack	**7**
Web Application Attack	**43**
Grand Total	**150**

Table 3-3 High Risk Tools

According the CVSS scoring specification document (FIRST, n.d.), a widely used scoring system for assessing the risk of vulnerabilities, low complexity (i.e. usable by script kiddies), remote execution, and no user interaction are all the highest risk ratings in their respective categories. 38 of these tools do not actually execute attacks ("*Attack Building & Examination*", "*Collaboration, Information Management & Reporting*", "*Information Gathering*") however, a significant number still remain in the other categories; 112 (41% of total tools).

3.4 Hacking Courses

3.4.1 Overview

The first step towards selection of courses for assessment was to search for the term "free hacking courses" on Google. All results found on the first five pages were investigated. The method of investigation was first to check if the course that came up in the search results met the criteria, i.e. was a free hacking related course with a defined syllabus. The next step was to carry out a search on that website to find any other courses on that site that meet the criteria. After the first two pages of the Google search results, all of the courses that were encountered that met the selection criteria were links to courses that had already been selected.

A table was created with the names and links of each of the courses and three further columns. The first was *Content*. For each course the syllabus or learning outcomes of the course were listed in this column. The next column was *"Requirement to View"*. As the name suggests, this column detailed what was necessary to do in order to access the course content, e.g. register with an email address. The final column was

"Categorisation". The information in this column was for use in the Cybercrime Survey which will be discussed below. The focus was on classifying each of the syllabus or learning outcome entries in each course into a broader category so that a shorter list of slightly broader topics could be obtained. An example of how this was applied is that *"Footprinting"* and *"Enumeration"* are two separate syllabus entries that were all assigned to the *"Information Gathering"* category. The results of the hacking resources assessment will now be discussed below.

3.4.2 Analysis of Hacking Courses

As part of this research project the sixteen hacking courses which met the selection criteria for assessment were analysed in some detail. The purpose of this was two-fold, firstly to more clearly understand the types of courses that are available to novice hackers, and secondly, to help create questions for the survey part of this research. Of these 16, 11 required registration with an email address in order to view them and the remaining 5 did not require any actions in order to view the course content. An example of two of the course syllabuses along with their categories as shown in the table below illustrate how it was established that there were common categories in the courses:

Course	Syllabus	Category
Ethical Hacking and Cyber Security Complete Course *https://www.udemy.com/the-ethical-hacking-course-for-cyber-security-hackers/*	Introduction to Ethical Hacking	Background info
	Introduction to Kali Linux	Using hacking tools
	Website Pen-testing	Web Attacks
	WordPress Website Pen-testing	Web Attacks
	Cracking FTP Using Medusa	Using hacking tools
	Password Cracking	Password Hacking
	Information Gathering Using Recon-ng	Information gathering

Course	Syllabus	Category
Introduction to Vulnerability Assessment	Learn a General Methodology for Conducting Assessments	Background info
	Scanning & Mapping Network Topology	Information gathering

http://opensecuritytraining.info/IntroductionToVulnerabilityAssessment.html	Identifying Listening Ports/Services on Hosts	Information gathering
	Fingerprinting Operating Systems Remotely	Information gathering
	Conducting Automated Vulnerability Scans	Information gathering
	Auditing Router, Switch & Firewall Security	System Hacking
	Auditing Unix and Windows Configuration and Security	System Hacking
	Performing Web App and associated DB Security Assessments	Web Attacks

Table 3-4 Course Content and Categories for two of the Free Hacking Courses that were assessed

A complete list of all the topics covered in the courses assessed is as follows:

- Denial of Service
- Cryptography
- Eavesdropping
- Information Gathering
- Mobile Forensics
- Password Hacking
- Smart Card Hacking
- Social Engineering /Manipulation/Deception
- System Hacking
- Techniques for Determining User Identity Online
- Techniques for Hiding Your Own Identity Online
- Using Hacking Tools
- Website Hacking
- Wireless Hacking

3.5 Conclusions

This chapter focused on the review and analysis of both hacking tools and hacking courses to determine what is freely available to novice hackers, and thus to explore the ease with which relatively naive users could get involved with criminal activities in an online environment.

The tools installed in the Kali Linux distribution were determined to be the best selection of tools to assess under the current research, and it was established that there is a considerable amount of tools that could be used by script kiddies to attack individuals or organisations. From this assessment, some tool descriptions were obtained for use in the survey to assess awareness of types of hacking tools.

A number of free hacking courses were assessed based on what content they contained, and what actions were necessary in order to access the course content. The course topics were established for use in the Cybercrime Survey in order to obtain feedback on opinions of their availability.

4 EXPERIMENTAL DESIGN: CYBERCRIME SURVEY

4.1 Introduction

Following on from the review and analysis of both hacking tools and hacking courses in the previous chapter, this chapter will present the detailed design of the survey to be used in this research to understand people’s attitudes to cybercrime, and how it may differ from their attitudes to non-cybercrime. First the chapter will provide an overview of the survey, followed by an explanation of how the survey was made more accessible to users who may not be familiar with hacking terminology. The chapter will then progress through each of the five sections of the Cybercrime Survey explaining the questions that were used and what the aim of the questions were in order to answer the research questions.

4.2 Overview of Survey

Some survey research on similar topics was reviewed in order to determine the best approach and the types of questions to ask (Brodsky & O'Neal Smitherman, 1983; Furnell, Bryant, & Phippen, 2007; Gibbons, Jones, & Garabedian, 1972; Hendrick, Fischer, Tobi, & Frewer, 2013; Liaw, 2002; Morse, Gullekson, Moris, & Popovich, 2011; Paulin, Searle, & Knaggs, 2003; Rossi, Waite, Bose, & Berk, 1974; Sherman & Dowdle, 1974; Tsai, Lin, & Tsai, 2001).

The Cybercrime Survey was designed and distributed using www.smartsurvey.co.uk. Convenience sampling was used. As there were no specific target audience or restrictions on eligibility for participation, the link for the Cybercrime Survey was circulated via sharing on social media platforms. Additionally the Cybercrime Survey was added to www.surveycircle.com – a platform that is intended for use in obtaining survey participants. It is based on mutual support – as a user completes more surveys, they are credited with more points. The more points a user has, the higher their surveys will be in the site’s survey rankings – the higher a survey is in the rankings, the more points other users get for completing the survey, thus boosting their own survey(s).

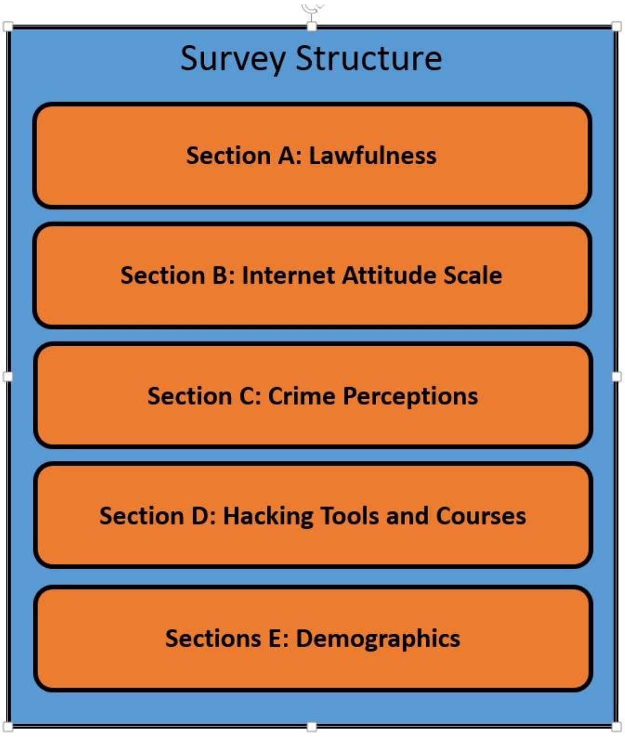

Survey Structure
Section A: Lawfulness
Section B: Internet Attitude Scale
Section C: Crime Perceptions
Section D: Hacking Tools and Courses
Sections E: Demographics

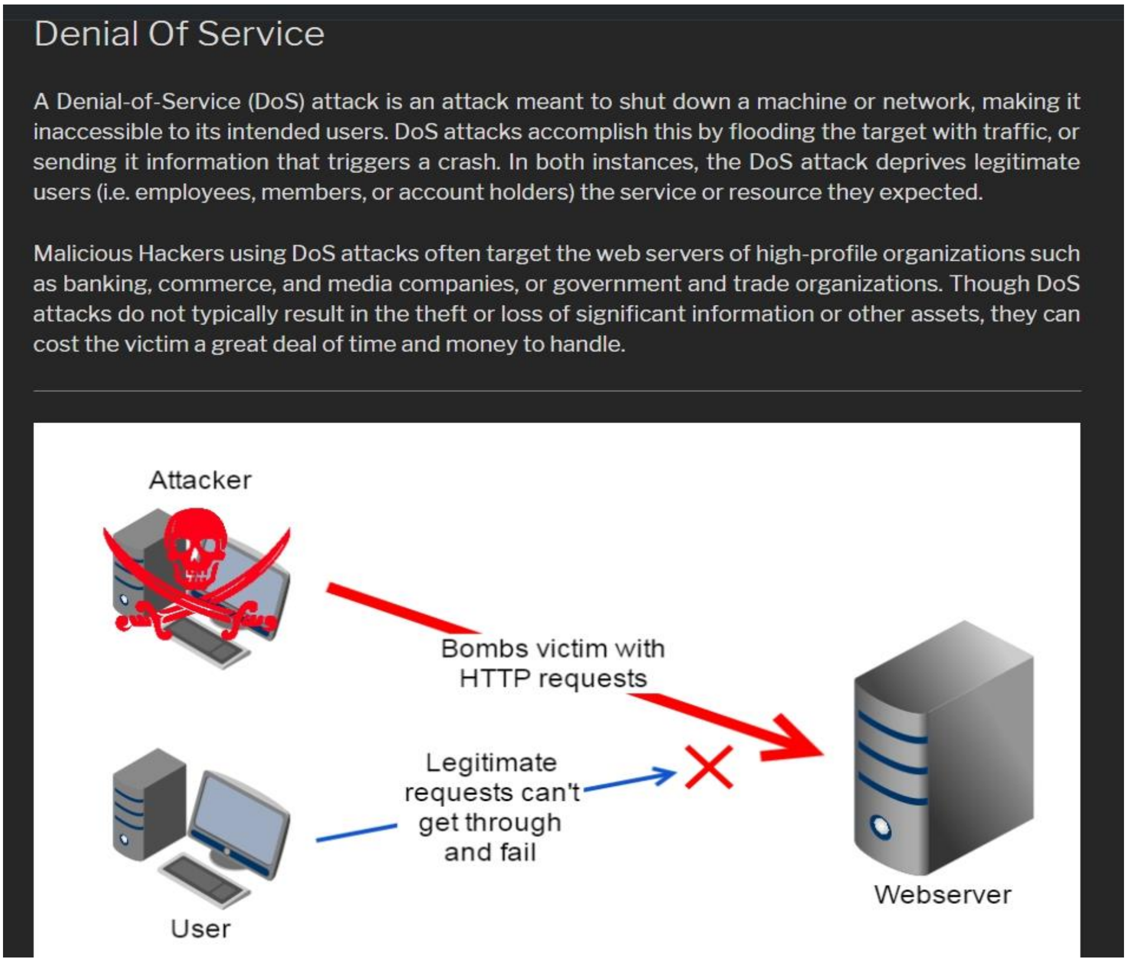
Figure 4-1 Overview of the Structure of the Survey

The overall structure of the survey will consist of four sections. Section A will consist of some questions on lawfulness and the legal system. The aim of this section is to get a measure of how much participants feel that people in general should obey the law, and how much they approve of some of the punishments used in the legal system in order to determine if these factors have any impact on the punishments they choose for crimes. Section B will consist of an Internet Attitude Scale. The aim of this section is to get a measure of participants' attitude towards the internet so that it can be investigated whether this has any impact on their views of cybercrime. Section C will investigate crime perceptions, the aim of which is to ascertain if there is a difference in the attitudes that people hold towards cybercrimes and non-cybercrimes. Section D will cover the hacking tools and courses as assessed in the previous chapter. The aim of this section is to get an indication of the awareness of the general public of the kind of tools that are available, and their opinions on the availability of free hacking courses online. Section E will consist of some demographic questions. This will allow the research to establish the nature of the sample and provide the opportunity to assess if there are differences in crime perceptions across different demographic subgroups.

The design of each of the sections of the Cybercrime Survey will be discussed in detail below, in the order that the topics were covered in the survey. The questions were drafted and re-drafted upon consultation with the research supervisor. The Cybercrime Survey was piloted on five participants and based upon their feedback, further changes were made. Some of these changes were cosmetic such as the prominence/colours of the progress bar and others were to alter phrasing. Some questions were re-drafted up to five times. Screenshots of the survey as seen by participants can be viewed in Appendix A.

4.3 Terminology definitions

Throughout the Cybercrime Survey, in order to ensure that all users could understand all the concepts/questions, hacking or internet related terminology that was deemed to potentially not be understood by all participants was hyperlinked to a description of the term which opened in a new window when clicked. These descriptions were hosted on a WordPress website that was created specifically for this purpose and did not contain any content other than these definitions. Each definition was a separate blog post. This linking of definitions was highlighted at the start of the Cybercrime Survey. An example of one of these definitions is shown in the image below.



Denial Of Service

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) the service or resource they expected.

Malicious Hackers using DoS attacks often target the web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

Attacker
Bombs victim with HTTP requests
Legitimate requests can't get through and fail
Webserver
User

Figure 4-2 Example terminology definition – Denial of Service

In the early drafts of the Cybercrime Survey, the definitions were included either before the relevant questions, or within the questions. This made the Cybercrime Survey quite text heavy with content that may be unnecessary for a lot of participants. Linking to an external definition was determined to be the optimal approach, as it still allowed participants who were uncertain of meanings to gain understanding but at the same time did not clutter the survey.

Definitions were sourced and combined from a number of websites directed at non-technical people such as www.techopedia.com in order to ensure that the language used was accessible to all. Pictures that were simple illustrations of the concept were included as they helped to clarify it to participants, and could enable understanding (or refreshing their memory if they had known it before) quickly if the participant did not wish to read through all the text.

4.4 Pre-amble

The Cybercrime Survey starts with a pre-amble, which is intended to provide context for all participants and reassure them of the anonymity of their responses. This step is particularly important as crime perceptions can be a sensitive subject and this may help to alleviate socially or morally desirable responding.

The pre-amble was as follows:

> *My name is Dearbhail Kirwan. I am a Masters student in the Dublin Institute of Technology. I am conducting a dissertation for my Master's degree examining the relationships between Crime, Cybercrime, and Ethical Hacking [Linked to Ethical Hacking Definition].*
>
> *Please note if you fill in this questionnaire, your answers will be treated in a highly confidential way. Neither I, the Dublin Institute of Technology nor any other third party will identify your name, email address or any other personal details, nor will it be possible to identify you in any way in the report I will publish as part of my MSc dissertation. I would like to personally thank you for your time in taking part in this survey. This survey should take no more than 10 minutes to complete. There is a progress bar at the top of each page that shows you your progress through the survey, and a contact*

form at the end of the survey should you wish to ask any questions or leave any comments regarding the survey/research.

4.5 Section A: Lawfulness

This section consisted of a few opening questions intended to gauge participants' attitudes towards prisons and sentencing, and the need to obey laws. All of these questions were placed on the same page. Question 1 and 2 were semantic differentials, with six radio buttons labelled 1 to 6 as the answer options:

- *I obey laws whether I agree with them or not, that's the foundation of a civil society (1 = Strongly Agree, 6 = Strongly Disagree)*
- *Other people should conform to laws and be punished for breaking them regardless of how big or small (1 = Strongly Agree, 6 = Strongly Disagree)*

The aim of these questions was to get a measure of how much participants felt that they themselves should obey laws and how much others should obey laws, This was separated into two questions rather than a single one stating "Everyone should obey laws…" as individuals may differ in the behaviour that they carry out compared to how they feel other people should behave and be accountable for their actions, and additionally if they felt people should not be punished for breaking laws, then they are unlikely to recommend strict punishment for a serious crime.

For the next question, participants were given a set of five statements, each one accompanied by a scale with seven options:

- *Strongly Agree*
- *Agree*
- *Slightly Agree*
- *Neutral*
- *Slightly Disagree*
- *Disagree*
- *Strongly Disagree*

The five statements were:

1. *Prisons are too soft and cushy*

2. *Judges are out of touch*
3. *Criminal sentences are often too lenient*
4. *Serving time in prison is the best method of punishment for a crime*
5. *Serving time in prison is the best method of rehabilitation of criminals*

The aim of these questions was to find out what participants thought of prison sentencing and aspects of the legal system. These questions were asked as prison is often viewed as the most serious punishment e.g. in Paulin *et al.* (2003) when asked to decide punishments, it appears that the answer options are in order of severity with prison sentences at the top of the list representing the most serious punishment. However, if a person feels that prison is a poor method of punishment or rehabilitation for a crime, they may be less likely to choose it as a punishment for a crime that they perceive as being very serious, which in turn may result in the research concluding that they perceived the crimes as less serious than they actually did.

4.6 Section B: Internet Attitudes

An internet attitude scale was included as it is possible that a persons' attitude to the internet may have an impact on their perception of cybercrime. A pre-existing scale was chosen to use for this part of the Cybercrime Survey. A number of scales were reviewed, however, many of these were created in the early 2000s. Given the growth of internet usage and the changes in the norms of internet usage, a slightly more recent scale was chosen – the refined ATIS [Attitudes Towards the Internet Scale] (Morse, Gullekson, Moris, & Popovich, 2011). Each statement was to be rated using the same 7 point scale: The statements that made up the scale were the following:

The statements that made up the scale were the following:

1. *I enjoy shopping online*
2. *I enjoy browsing (surfing) websites without any specific purpose*
3. *I feel anxious that online communications can potentially be seen, heard, or otherwise accessed by other people*
4. *I feel that the Internet has allowed me to keep in touch with many people*

5. *I feel anxious that my personal information may be available over the Internet*
6. *I like to look up information about businesses, services, and/or products on the Internet*
7. *I have had more good experiences than bad experiences using the Internet*
8. *I would prefer to communicate through writing a letter or a memo rather than an email*
9. *I feel uncomfortable using my credit card online*
10. *I enjoy using the Internet to pass time and/or to have fun*
11. *I would prefer to go online to conduct most of my banking*
12. *When searching for information, I would rather read books, magazines, and newspapers than browse the Internet*
13. *I only feel comfortable using online stores to browse or compare prices*
14. *I avoid using the Internet whenever possible*
15. *I enjoy using the Internet for instant messaging or other types of real-time communication*
16. *Overall, I enjoy using the Internet*

Morse *et al.* (2011) also included an extra item in the scale used in their research – “I feel that the Internet limits my productivity”. This was not included in the current research as they recommended that it be removed from future applications of the scale. The internet attitudes scales were the only questions on this page of the Cybercrime Survey.

4.7 Section C: Crime Perceptions

4.7.1 Overview

The crime perception questions were modelled on those in the research carried out by Paulin, Searle and Knaggs (2003). This research was carried out in New Zealand, in which researchers went from door to door and carried out the surveys verbally, using a script and scorecards, recording all the participants answers. The questions that were selected to model this section of the Cybercrime Survey on made up only part of the Paulin *et al.* survey. These questions related to ranking the seriousness of crime scenarios, deciding punishments for the crimes, and indicating the aim of the punishments as these were the sections determined to be relevant to this study. In addition to this the Paulin *et al.* research did not include any cybercrime, therefore, some of the crime scenarios were exchanged for cybercrime scenarios, these will be discussed in further detail below.

The first crime perception question was to rank six crimes in order of seriousness based on a very short description. Paulin *et al.* used the following crimes:

- A man assaults his female partner;
- Burglary with a weapon;
- Drunk driving;
- Importing heroin with a street value of $100,000;
- Fraud of $50,000;
- Possession of 10 grams of marijuana.

Three of these scenarios were not used in current research; it was decided to keep the crime scenarios that were all crimes “against people”. That is, while drunk driving is potentially a very dangerous crime, there is not always a victim. Additionally, importing heroin, and possession of cannabis do not necessarily harm any individual or company directly, be it physically, psychologically or financially. Whereas with domestic abuse, armed burglary and fraud, there is a definite victim to each of these crimes. This was done with the aim of discarding any scenarios that people may have ambiguous opinions on. As will be seen below, these crime scenarios are used throughout this section of the Cybercrime Survey, with further detail being added in later questions. Therefore, the cybercrime scenarios needed to be robust.

Very little was found in the way of previous survey research on attitudes towards or perceptions of cybercrime in order to use previously tested scenarios. As a sentence for each of the crimes needed to be provided in later questions, real crime scenarios and sentencing were used. This was done as the researcher has no experience in crime sentencing and a sentence generated for a fake scenario would be unsupported by current practice and may vary significantly from what the sentence for that crime would be if it occurred in reality. While this ensured validity of the sentences, it meant that control over the details of the crimes were surrendered to what was available as having occurred. The cybercrime occurrences chosen were all sentenced within the last year.

4.7.2 Real World Cybercrime Examples

The first cybercrime selected for use was that of Roman Valeryevich Seleznev, aka Track2. Seleznev was a Russian cybercriminal who stole and sold millions of credit card numbers. He hacked into point-of-sale systems and installed malware that stole the credit card numbers from more than 500 US businesses and sent them to servers he controlled. These card numbers were then sold on criminal websites. These crimes caused more than $169 million in damages to approximately 3700 financial institutions. In April 2017, Seleznev was sentenced to 27 years imprisonment. (The United States Department of Justice, 2017b)

The second cybercrime selected for use was that of Andrew Helton. Helton ran a phishing scheme over a period of two years and stole approximately 448 usernames and passwords from 363 email accounts. After obtaining these, he looked through their email accounts and found and stole 161 sexually explicit, nude and/or partially nude photos of 13 victims, some of whom were celebrities, and kept them for personal use. Helton was sentenced to six months imprisonment and a $3000 fine in July 2016. (The United States Department of Justice, 2016).

The third and final cybercrime selected for use was that of Deric Lostutter. Lostutter hacked into a fan's website for a Steubenville High School sports team to bring attention to an ongoing rape case in which two Steubenville High School football players had been arrested. He then also posted on the website a video and manifesto intended gain publicity for himself and an accomplice's online identities, and additionally threatened to reveal personal identifying information of students and claimed falsely that the website's administrator was involved in child pornography and directed a "rape crew". Lostutter was sentenced to 2 years imprisonment in March 2017. (The United States Department of Justice, 2017a)

4.7.3 Modifications to Real-World Cybercrimes

While gender is only mentioned for the domestic abuse crime in the short descriptions, it is revealed for each of the crimes in the later questions. This presented an issue as all of the scenarios that were retained from Paulin *et al.* were perpetrated by males, as were the three cybercrime scenarios that were chosen. In order to avoid some form of potential gender bias affecting the results, the gender in some of the scenarios were changed. The scenarios to switch were chosen in such a way to ensure that they aligned with traditional stereotypes – armed burglary, domestic abuse and stealing explicit images for personal use, regardless of actual statistics, are crimes more traditionally associated with males. The ideal approach would have been to switch the genders around between participants but this was deemed outside the scope of the current study as it would require a much larger sample. Therefore, the "Hack and deface website" and "Fraud of €50,000" were switched to female perpetrators. With the exception of this gender switch, no other details were changed in the scenarios obtained from Paulin *et al.*

4.7.4 The Questions

The aim of these questions is to assess perceptions of cybercrimes when compared to perceptions of non-cybercrimes. This will be done by comparing rankings and sentencing for brief descriptions of the crimes, and then assessing sentencing and aims of sentencing for more detailed descriptions of the same crimes.

The first question in this section was:

> *Arrange these crimes in order of most serious to least serious (1 being most serious and 6 being least serious:*
>
> - *A hacker steals a high volume of credit card numbers*
> - *Burglary with a weapon*
> - *A hacker uses phishing [Linked to phishing definition] emails to steal usernames, passwords and personal images from email and social media accounts*
> - *A man assaults his female partner*
> - *A hacker takes control of a website and defaces it*
> - *Fraud of €50,000 from a medium sized company*

The aim of this question was to ascertain a relative ranking of seriousness of the crimes, based solely upon short descriptions of crime scenarios. The order of the crime descriptions was randomised for each participant. This initial measurement of attitudes based on brief descriptions of the crimes was carried out as Paulin *et al.* (2003) reported that people display a tendency to become less punitive the more details they know about the scenario so it is good to get a measure with brief descriptions, and again with more detailed descriptions of the same scenarios.

The next question looked at crime sentencing.

Please decide the appropriate sentence for each crime:

- *A hacker steals a high volume of credit card numbers*
- *Burglary with a weapon*
- *A hacker uses phishing [Linked to phishing definition] emails to steal usernames, passwords and personal images from email and social media accounts*
- *A man assaults his female partner*
- *A hacker takes control of a website and defaces it*
- *Fraud of €50,000 from a medium sized company*

Each crime description was accompanied by a scale of 8 radio buttons, to choose one:

- *Life Imprisonment*
- *Prison for more than 10 years*
- *Prison for 5-10 years*
- *Prison for 1-5 years*
- *Prison for less than 1 year*
- *Probation*
- *Monetary Fine*
- *No Penalty*

The aim was to obtain participants initial impression of what punishment a crime merited based solely on the short descriptions. The order of the crime descriptions was also randomised for each participant.

The next page of the Cybercrime Survey presented more detailed descriptions of each of the crime scenarios and participants were asked to select an appropriate punishment. The following text was at the top of the page:

> *In the following questions that describe crime scenarios, please read the description of the crime and then choose an appropriate punishment for the crime.*

There were 9 radio button punishment options or an "Other" option accompanied by a text box, identical for each crime scenario. These were as follows:

- *Life Imprisonment*
- *Imprisonment for more than 10 years*
- *Imprisonment for 5-10 years*
- *Imprisonment for 1-5 years*
- *Imprisonment for less than 1 year*
- *Probation*
- *Community Service*
- *Monetary Fine*
- *No penalty*
- *Other (please specify): [Text Box]*

After they selected the punishment for each one, participants were asked to indicate 1-3 aims of the punishment as follows:

> *In relation to the sentence you gave [relevant criminal], what do you think the sentence is trying to achieve? You may choose up to three aims but if you think only one is necessary, then select only one.*
>
> - *Preventing the offender from committing further crimes through imprisonment*
> - *Discouraging the offender from committing further crimes*
> - *Providing punishment that reflects the seriousness of the offence*
> - *Assisting the offender so that he won't offend again*
> - *Discouraging others from committing crimes*
> - *Showing society's disapproval of the crime*
> - *Providing compensation to the victim where possible.*

The aim of these questions was to ascertain the punishments that participants would give the criminals based upon more detailed descriptions of the crimes and additionally look at the motivations behind each punishment.

The detailed crime scenarios given were as follows:

- *Paul, aged 22 and unemployed, broke into an elderly couple's house. When the elderly man got up to investigate the noise, Paul threatened him with a gun, and then fled. He has previous convictions for breaking and entering*
- *Jane, aged 29, hacked into a School related website and took control of it in order to post evidence related to an ongoing court case involving students of the school. She also used the site to post a video and manifesto promoting her online identity and threatening to reveal personal identifying information about the school's students. Jane, a member of the infamous hacktivist group "Anonymous", had no prior convictions.*
- *Peter, aged 32, threw a vase at his partner after a night out drinking with friends. His partner required several stitches to her head and she was off work for three days. Peter, a bank clerk, has prior convictions for this type of assault.*
- *Joe, aged 32, hacked into retail point of sale systems, (i.e. shop credit card machines) and installed software that collected credit card numbers and sent them back to him. He stole millions of credit card numbers from more than 500 businesses and sold them on the dark web [Linked to dark web definition]. Joe, the son of a foreign influential lawmaker, had no prior convictions.*
- *Mary, aged 45, used a client's money which should have been held in trust, as a €50,000 deposit to buy an apartment for herself. At the time of the offence, Mary was a partner in a city legal firm. She has no previous convictions.*
- *Andrew, aged 29, ran a phishing [Linked to phishing definition] scheme that he used to steal the usernames and passwords to over 300 email accounts, some of which belonged to Hollywood celebrities. He stole images from these accounts and stored them on his personal computer for personal use. It is not believed any of the information or images were publicly released. Andrew, who has two masters degrees in fields unrelated to technology, had no prior convictions.*

Due to the layout and configuration of this part of the Cybercrime Survey on www.smartsurvey.co.uk, it was not possible to randomise the order of the crime scenarios for participants, they were presented to participants in the order shown above. The questions on the next page deviated slightly from Paulin *et al.*'s approach. While they used the exact same scenarios, the current study changed some cosmetic details of the scenarios. This was done in order to allow the checking of consistency of answering, i.e. they are verifying questions. Participants were presented with briefer descriptions of the crime scenarios, slightly altered but fundamentally the same, along with the sentence the crime received and asked to judge the "heaviness" of the sentence. The following text was at the top of the page:

> *For the questions on this page please read the crime description and the sentence that was given for it. For each one please indicate if you think the sentence was far too heavy, a little too heavy, about right, a little too light, or far too light.*

Each question provided the following five radio button options:

- *Far Too Heavy*
- *A Little Too Heavy*
- *About Right*
- *A little Too Light*
- *Far Too Light*

The scenarios and sentences were as follows:

- *Robert, aged 30, used phishing [Linked to phishing definition] to steal personal data from approximately 350 people which he used to access their social media accounts. It is not believed that he distributed any data.*

  Robert was sentenced to six months imprisonment and a €3000 fine

- *Sophie, aged 32, hacked into a sports team website and took control of it. She used it to post criminal allegations against a member of the sports team.*

  Sophie was sentenced to two years imprisonment

- *Gerry, aged 24, broke into a single woman's house. When confronted by the woman, Gerry threatened her with a crowbar, and then ran.*

  Gerry was sentenced to two years imprisonment

- *Barry, aged 35, pushed his partner down a set of 4 steps. She sprained her wrist and suffered some cuts and bruises. Barry had been out drinking and this was not the first occurrence of an incident like this.*

  Barry was sentenced to 6 months' probation

- *Thomas, aged 28, hacked into ATMs, and stole millions of credit card numbers and sold them on the dark web [Linked to dark web definition].*

  Thomas was sentenced to 27 years imprisonment

- *Janet, aged 42, was a director in an investment company. She used €45,500 of a client's money as a deposit for a mortgage for herself.*

  Janet was sentenced to 150 hours of community service

These questions were designed to add another level to the perception investigation as they came from a different perspective and judging a sentence that has already been handed out is a different process to determining sentencing or seriousness.

4.8 Section D: Hacking Tools & Courses

This section of the Cybercrime Survey was developed in order to get feedback on awareness and opinions regarding the hacking tools and courses that were assessed under the Kali Linux distribution review. There were two main questions, the first relating to the tools and the second to the courses.

The following instructional text was placed at the start of the first question on this page:

> *Below is a list of hacking tool descriptions. All of them, some of them, or none of them, are real. Please indicate whether you think these tools are real or not:*

(Note: Many tools require certain vulnerabilities to exist, or specific situations to arise in order for it to be possible to use them - These have not been included in the descriptions for the sake of simplicity)

There were two answer options available:

- *I think this tool exists and is freely available on the internet;*
- *I do not think this is a real tool*

The tools descriptions were as follows:

- *A tool that connects to your browser and lets the attacker collect all kinds of information (e.g. cookies, sites you visit, etc.)*
- *A tool that steals data from your device through a Bluetooth connection*
- *A tool that will try hundreds of thousands different combinations of PINs in a very short space of time to gain access to a Wi-Fi network*
- *A tool that sets up fake Wi-Fi access points/Websites etc. that look like other legitimate ones to steal your usernames/passwords/access keys etc.*
- *A tool that floods a system with "fake" attacks so they can slip in a real attack that might get through unnoticed/unstopped*
- *A tool that can send you fake software updates that the attacker can use to install malicious software*
- *A tool that plants malicious software on your phone that will disable your house alarm once you connect to your home Wi-Fi*
- *A tool that can clone a mobile device and all the data on it (e.g. photos, messages, apps, etc.) by placing it next to it for approximately 2-3 minutes*
- *A tool that steals a phone's browser history over Wi-Fi and uses this to gain access to online banking accounts previously accessed on the phone*

The order of the tools was randomised for each participant. Six of the tools descriptions were those of real tools installed in the Kali Linux distribution, while the other three were fabricated. Ideally the survey would look at more of the tools reviewed in the Kali Linux distribution, however, it was deemed infeasible and impractical to include such a large number as there are also a lot of other questions in the Cybercrime Survey. If the survey got too long or repetitive it might increase the likelihood of respondents getting bored and abandoning the survey, or selecting quasi-random answers just to get the survey completed. Attempts to carry out such a task would significantly lower the quality of the survey.

Therefore, six tools were chosen from the set of tools. These tools were chosen because their functions were not exceptionally technical in nature and so they should be understandable to participants even of basic technical knowledge or ability. Below are the actual tool names paired with their descriptions:

Below are the actual tool names paired with their descriptions:

- ***BeEF*** - *A tool that connects to your browser and lets the attacker collect all kinds of information (e.g. cookies, sites you visit, etc.)*
- ***Bluesnarfer*** - *A tool that steals data from your device through a Bluetooth connection*
- ***Bully*** - *A tool that will try hundreds of thousands different combinations of PINs in a very short space of time to gain access to a Wi-Fi network*
- ***Ghost Phisher*** - *A tool that sets up fake Wi-Fi access points/Websites etc. that look like other legitimate ones to steal your usernames/passwords/access keys etc.*
- ***Inundator*** - *A tool that floods a system with "fake" attacks so they can slip in a real attack that might get through unnoticed/unstopped*
- ***Isr-evilgrade*** - *A tool that can send you fake software updates that the attacker can use to install malicious software*

- ***Fake tool #1*** *- House Alarm Disable - A tool that plants malicious software on your phone that will disable your house alarm once you connect to your home Wi-Fi*
- ***Fake tool #2*** *- Clone Phone - A tool that can clone a mobile device and all the data on it (e.g. photos, messages, apps, etc.) by placing it next to it for approximately 2-3 minutes*
- ***Fake tool #3*** *- Get Bank Creds - A tool that steals a phone's browser history over Wi-Fi and uses this to gain access to online banking accounts previously accessed on the phone*

The fake tool descriptions were generated with the intention of not being overly technical in nature, as with the real tools that were selected. They were chosen with the aim of being relatable to all participants. It is likely that the majority of participants have mobile phones and use online banking. While participants may not have Wi-Fi-enabled house alarms, the majority of people are likely to have lived in a property with a house alarm at some point and therefore can identify with the concept of it being possible to disable an alarm using wireless technology.

The courses question was placed on the same page as the tools question. The course topics were all derived from the hacking courses review. It was introduced with the following text:

> *There are a number of informative video tutorial based courses available online for free from legitimate educational sources. These courses cover a wide range of hacking methodologies. Some of the courses require registration with an email address, and others don't. (Note: This study is focusing only on free courses)*
>
> *Below is a description of course topics covered. For each one please indicate what you think should have to be done in order to access the course.*

There were five radio button options for each course topic:

- *Don't have to register*
- *Register with an email address*
- *Register with an email address and give proof of address and credit card for proof of identity*

- *Register with email, proof of address, credit card, and show why you need access to course (e.g. job related)*
- *Shouldn't be available online*

The course topics were as follows:

- *Denial of Service [Linked to definition]*
- *Cryptography [Linked to definition] (With the intent of trying to break it)*
- *Eavesdropping (e.g. on wireless communications)*
- *Information Gathering [Linked to definition]*
- *Mobile Forensics [Linked to definition]*
- *Password Hacking ("Cracking" Passwords)*
- *Smart Card Hacking [Linked to definition]*
- *Social Engineering [Linked to definition] /Manipulation/Deception*
- *System Hacking [Linked to definition]*
- *Techniques for Determining User Identity Online*
- *Techniques for Hiding Your Own Identity Online*
- *Using Hacking Tools*
- *Website Hacking*
- *Wireless Hacking*

The order of the topics was randomised for each participant. The aim of these questions was to gauge public opinion on the availability of free online courses instructing people how to carry out hacking techniques.

4.9 Section E: Demographics

The final page of the Cybercrime Survey was devoted to gathering some demographic information about participants. The following questions were included:

Age:

- *Under 18*
- *18-24*
- *25-34*
- *35-44*
- *45-54*
- *55-64*
- *65-74*
- *75+*

Gender:

- *Male*
- *Female*

What is your primary country of residence?

- *Ireland*
- *Other (please specify): [Text Box]*

Please choose the option below that best represents you:

- *I work in an I.T. security related field*
- *I work in a non-security field in I.T.*
- *I don't work in I.T. but I am familiar with computer related technologies*
- *I don't work in I.T. but use computers regularly (e.g. internet browsing or for work)*
- *I don't work in I.T. or use computers much*

Have you or anyone close to you been victim of a cybercrime? (E.g. phishing, passwords or personal data stolen, etc.)

- *Yes*

- *No*

If yes, add details if you wish: [Text Box]

These details were collected in order to allow comparisons across different groups, e.g. male and female, old and young etc. Information about whether participants work in IT security, or if they or someone close to them has been victim to a cybercrime was collected as it has the potential to influence opinions on the matter.

4.10 Reflections

Some important observations were made in the construction and execution of the Cybercrime Survey. It is very important to assess and redraft questions as they are rarely perfect on the first round. An example of questions that were redrafted in the Cybercrime survey are the very first two questions. In the first draft of the survey, there was only one question:

On a scale of 1-10 how lawful do you consider yourself, where 1 is extremely lawful and 10 is not very lawful.

This was then redrafted into two separate questions:

- *I obey laws whether I agree with them or not, that's the foundation of a civil society (1 = Strongly Agree, 6 = Strongly Disagree)*
- *Other people should conform to laws and be punished for breaking them regardless of how big or small (1 = Strongly Agree, 6 = Strongly Disagree)*

This redraft was very important as the first draft was quite ambiguous and may not have provided a useful statistic. In addition to this, there were some other accompanying questions in the Paulin *et al.* study that were originally included in the Cybercrime Survey, an example is as follows:

> *What about if Paul was given a fine, that is, ordered to pay money to the Court, rather than 2 years imprisonment?*

This was accompanied by the following answer options:

> *This would be:*

- *Much More Suitable*
- *Slightly More Suitable*
- *Slightly Less Suitable*
- *Much Less Suitable*

This was removed from the second draft of the survey as these question were determined to be irrelevant to the research question.

Given the complex nature of cybercrime, and the relevance of context to each individual cybercrime, it was more difficult to effectively summarise the crimes in such a way that was consistent with the approach to the descriptions of the non-cybercrimes. This was particularly difficult for the brief descriptions, but also in the detailed descriptions.

It is also important to plan out the "flow" of the sections of the survey, for example, the demographics questions were left to the end so that participants had already committed a considerable amount of their time and would be more willing to surrender personal details in order to complete the survey. They could potentially be off-putting for some participants if they were in the first section of the survey. It is also important to ask some questions in more ways than one in order to verify the results. The final subsection of the crime perception section, wherein the participants were told the actual sentences for the crimes and asked to judge if the sentence was about right, too heavy or too light performed this function in the Cybercrime Survey. Surveys should be kept as short as possible; as it gets longer, more people may dropout or the quality and accuracy of answers may degrade if participants get bored or fed up with the survey. This was found to be a surprisingly difficult feat.

One of the main aims of the survey was to assess perceptions of cybercrime compared to perceptions of non-cybercrimes in order to address the research sub-question "*Are cybercrimes perceived as being less serious than non-cybercrimes?*" This was done by asking participants to rank the crimes in order of seriousness, but also through a series of questions on sentencing and sentence aims in order to fully verify and confirm the findings. The other main aim of the survey was to assess opinions and awareness around hacking tools and resources in order to answer the research sub-question "*Are people aware of the type of hacking resources that are available online?*" It can be quite easy to state research questions, however it is considerably more difficult to develop questions that fully address those research questions.

4.11 Conclusions

The Cybercrime Survey was designed primarily based on pre-existing research and addressed two of the research sub-questions. It was delivered online using the platform www.smartsurvey.co.uk and consisted of five subsections:

- Section A: Lawfulness
- Section B: Internet Attitudes Scale
- Section C: Crime Perceptions
- Section D: Hacking Tools and Courses
- Section E: Demographics

The sample was selected using a convenience sampling approach; by distributing the link to the Cybercrime Survey on social media platforms and it was made as accessible as possible to people who were not overly familiar with computer related technologies by linked all such terminology to definitions of the terms.

5 CYBERCRIME SURVEY RESULTS

5.1 Introduction

The aim of this survey was to address the two research sub-questions; "*Are cybercrimes perceived as being less serious than non-cybercrimes?*" and "*Are people aware of the type of hacking resources that are available online?"* The survey took some additional measures; lawfulness, internet attitude, and demographic measures to investigate if they were a factor in the perception of crimes (both cyber and non-cyber). The survey was broken down into the five subsections in the following order: (1) Lawfulness, (2) Internet Attitude, (3) Crime Perceptions, (4) Hacking Resources Awareness and Opinions, and (5) Demographics.

This chapter will present an analysis of the results of the survey as follows, first it will look at the completion rates of the survey, and how it compares to other studies, following that, the demographics, lawfulness and internet attitudes distributions will be summarised. The cybercrime perceptions results will be analysed in greater detail, with comparisons across questions as well as investigations of comparisons across sub groups such as demographic subgroups, and an examination of notable answers. The results from the hacking resources section will also be reported in addition to the key findings of the Cybercrime Survey.

5.2 Completion Rates

Exactly 185 participants completed the Cybercrime Survey with an additional 65 people starting it but not completing it. The incomplete responses were not included in any of the statistical analysis. The mean time for completion was 23 minutes and the minimum time was 8 minutes. It is difficult to get a true maximum; as the survey was served over the internet, participants were under no pressure to complete the survey quickly, therefore, they may have stopped and returned to it as many times as they wished. For 10 of the responses, over an hour elapsed between start and end time, one of which was 5 hours 18 minutes. The average (mode and median) dropout point was on the thirty-fifth item, at the start of the fourth page; the beginning of the detailed descriptions of the crimes questions, and dropouts occurred most frequently at the start of pages. Hoerger's study on internet-mediated survey dropout rates (2010) concluded that 10% are expected to drop out early on with an additional 2% every 100 items. That puts the expected dropout rate at 12% which could indicate issues with the Cybercrime Survey as the actual dropout rate was 35%. However, Hoerger's participants were taken from a university psychology participant pool and participants were compensated for their participation with psychology subject pool credit (Hoerger, 2010). With the exception of 18 responses to the Cybercrime Survey that came from users of www.surveycircle.com (This could be considered a participant pool, and the incentive is there to complete the survey in order to boost their own survey in the ranking and so get more responses), this is different to the current study for multiple reasons; (1) Participants were not sourced from a pool, (2) Participants were not provided with any compensation, and (3) It can be of benefit for students (particularly psychology students) to participate in all kinds of research to improve their understanding of research methods that they will need to utilise in the future which acts as an incentive to participate. There was no incentive to complete the Cybercrime Survey other than interest in the topic, or goodwill. These factors could go a long way to explaining the relatively high dropout rate.

5.3 Section E: Demographics

Section E, which focused on the demographics of the participants, was the last section in the survey, but the results of which will be presented first in this chapter. When constructing the survey, it was felt that having the demographics questions too soon might increase the likelihood of participants dropping out before completing the survey, whereas in this chapter it makes sense to understand the composition of the participants before looking at the outcomes of other questions.

The breakdown of the genders of participants is shown in the pie-chart below:

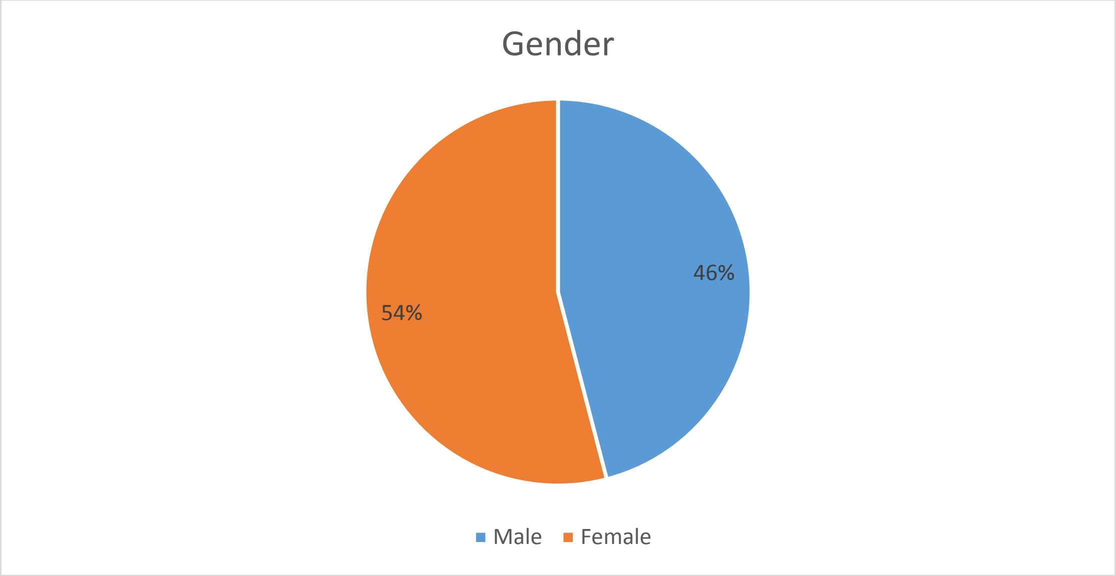


Figure 5-1 Gender Breakdown of Survey Sample

As the pie chart shows, the gender breakdown of the sample that participated in the Cybercrime Survey is quite an evenly balanced sample, not falling victim to the phenomenon that can often be an issue in I.T. related research; a shortage of females. The age distribution of the sample is show in the bar chart below:

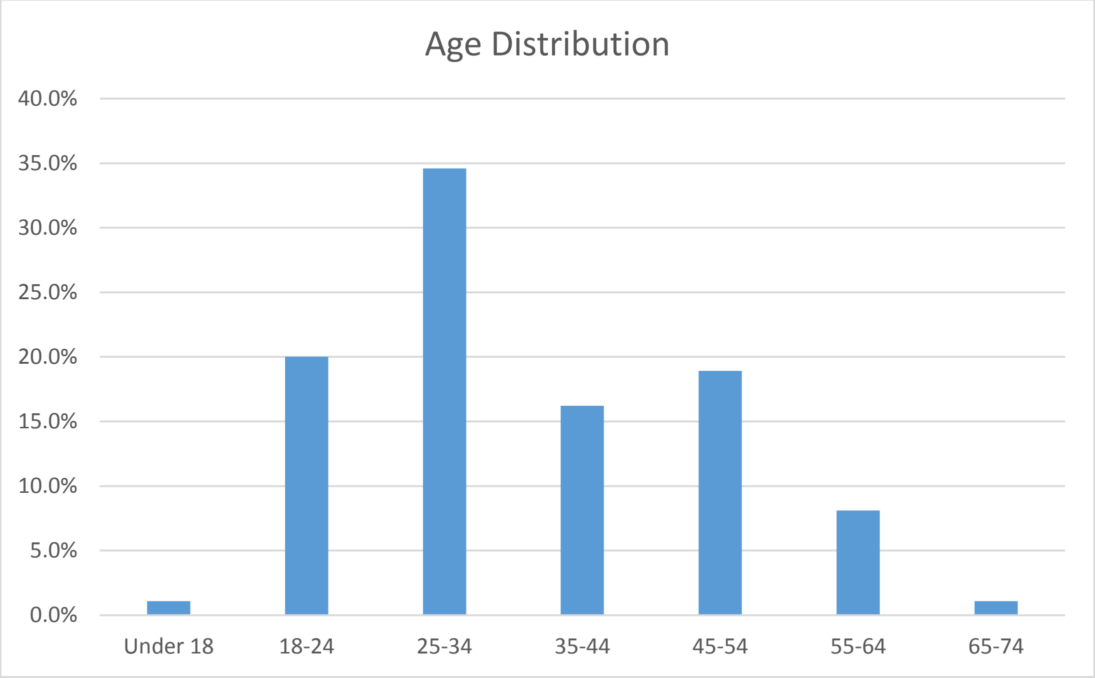


Figure 5-2 Age Distribution of Cybercrime Survey Sample (Note: Y-axis truncated at 40%)

The distribution of the sample is approaching normal distribution and does not display any significant skewing. Survey research is often skewed with a high proportion of young sample as researchers use University based participant pools. A good example of this is the Morse *et al.* (2011) study that provided the internet attitude scale used in this study, wherein the ages ranged between 18 and 50 yet the average age was 19.07 years old.

The I.T. experience of the sample as rated by the participants is shown in the bar chart below:

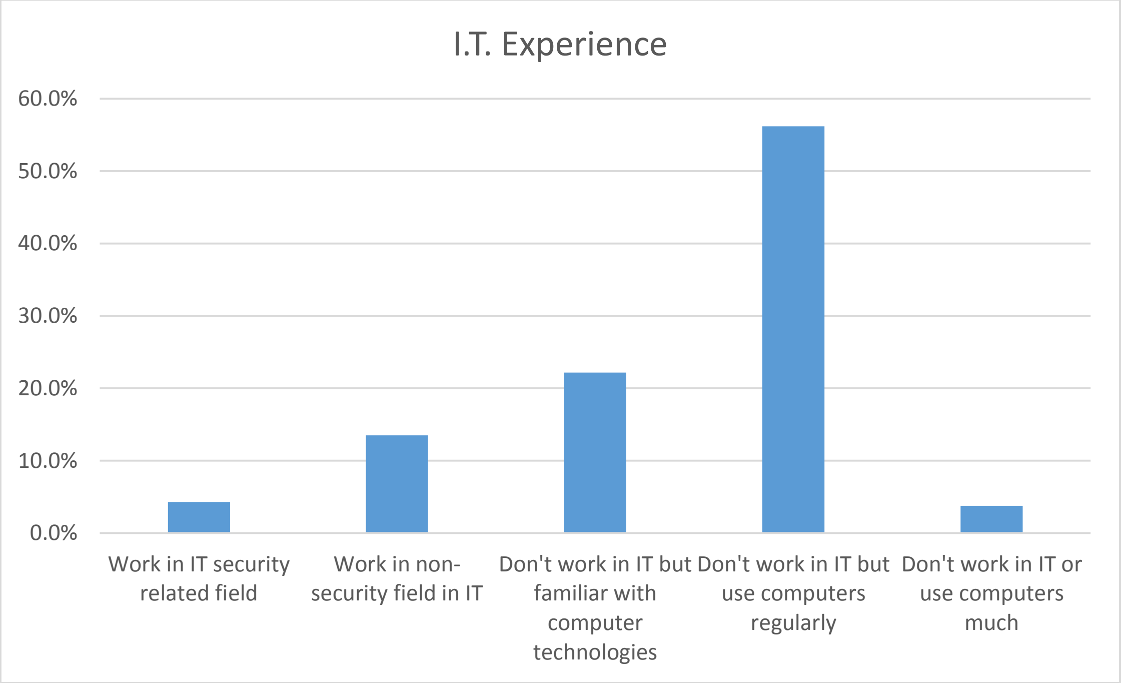


Figure 5-3 I.T. Experience for all Participants in the Cybercrime Survey (Note: Y-axis truncated at 60%)

The majority of participants (56.2%) reported familiarity with computers through regular usage. This indicates that they are unlikely to be familiar with some of the hacking related terminology and so would have benefited from the hyperlinked descriptions. Only a small portion of the sample indicated they don't use computers much, or work in an IT security related field. This is good as these are outlying groups that could impact the results of the survey in such a way that could make them not applicable to the population, through either complete lack of familiarity with any of the concepts for those that don't use computers much, or an over familiarity for those that work in I.T. security.

The pie chart below shows the proportion of the answers to the "Victim of Cybercrime" question:

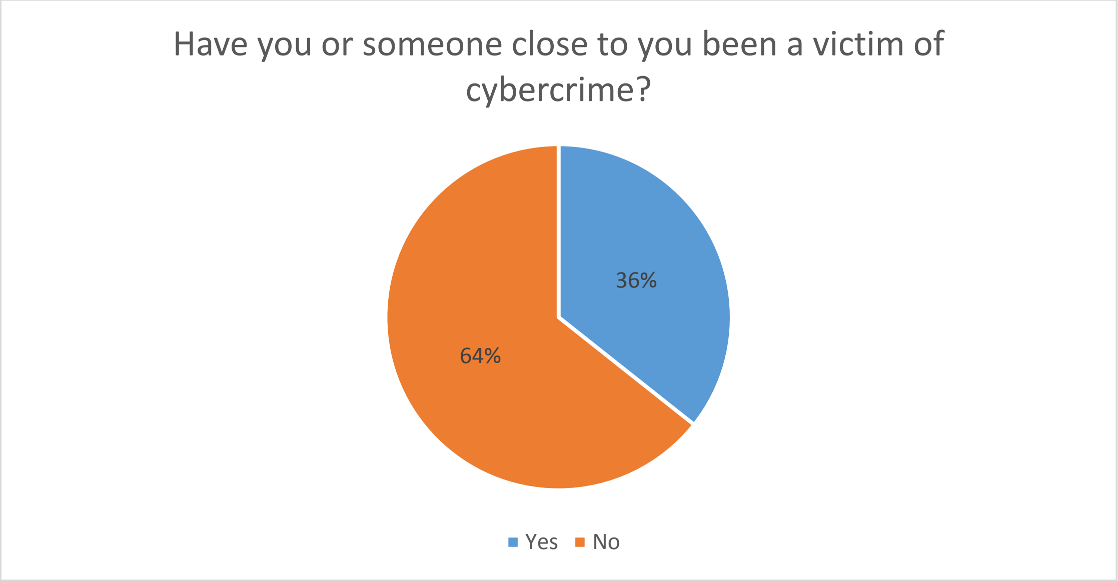


Figure 5-4 Breakdown of Responses to the "Victim of Cybercrime" Question

A considerable proportion of people answered yes to this question. These two subgroups will be compared in the crime perceptions section below in order to determine if it has any impact of the perception of crimes.

Overall the sample is very well-balanced and likely to be representative of the greater population.

5.4 Section A: Lawfulness

The aim of this section was to determine lawfulness of respondents, with regards to their own behaviour, and the behaviour of others. Additional questions were to assess some opinions of the participants on some aspects of the legal system as these measures could potentially impact the sentences they chose for crimes. Questions 1 and 2 asked the participants about lawfulness, a very small difference was observed between the *I Obey Laws* (M = 2.37, SD = 1.466) and the *Others Should Obey Laws* measurements but this difference does not appear to be big enough to be a factor in anything.

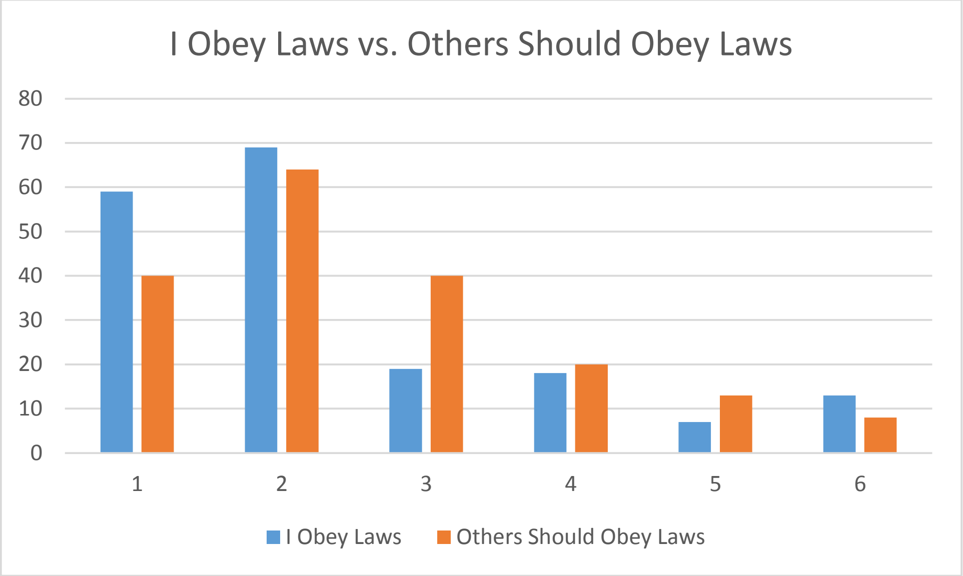


Figure 5-5 I Obey Laws vs. Others Should Obey Laws

The majority of the participants agreed to some extent with the statements; 79.5% for *I Obey Laws* and 77.8% for *Others Should Obey Laws*. Therefore, the majority of participants are generally quite lawful and believe in punishment for crimes.

The means and standard deviations for the remaining *Lawfulness* questions can be seen below.

Statement	Mean	Std. Deviation	Rounded Rating
Prisons Too Soft	3.56	1.75	Neutral
Judges Out of Touch	3.15	1.58	Slightly Agree
Sentences Too Lenient	2.34	1.30	Agree
Prison is the Best Punishment	3.99	1.68	Neutral
Prison is the Best Rehabilitation	4.70	1.59	Slightly Disagree

Table 5-1 Mean and Std. Deviation of Lawfulness Measures

The “Rounded Rating” in the table is the answer option from the Cybercrime Survey corresponding to the nearest whole number to the mean in each case.

5.5 Section B: Internet Attitude Scale

Question 4 consisted of the internet attitude scale. There were 16 items in the internet attitude scale, and they can be broken down into three factors; (1) General Internet Usage, (2) Negative Internet Attitudes, and (3) Task Facilitation. The scale was found to have an overall consistency of $\alpha = .775$, however, this increased to $\alpha = .783$ if the item “*I only feel comfortable using online stores to browse or compare prices*” was removed.

This is a slight improvement on Morse *et al.* (2011) who found α = .74 for the same scale. The internal consistencies of the three subscales were as follows; (1) General Internet Usage α = .736, (2) Negative Internet Attitudes α = .630 (.675 with *"I only feel comfortable using online stores to browse or compare prices"* removed, and (3) Task Facilitation α = .561, compared to .75, .54, and .58 from Morse *et al.* respectively.

The means and standard deviation of the overall scale and the three subscales are shown below.

Scale/Subscale	**Mean**	**Std. Deviation**	**Morse *et al.* Mean**	**Morse *et al.* Std. Deviation**
ATIS (Total Scale)	2.59	0.68	1.77	0.58
General Internet Usage	1.97	0.73	0.85	0.68
Negative Internet Attitudes	3.00	0.86	2.57	0.85
Task Facilitation	2.54	0.98	2.19	1.02

Table 5-2 Mean & Standard Deviation for Current Study & Morse *et al.* (2011) Study

To give the numbers context, the range of possible values is from 1 to 7, and a value of 1 indicates a completely positive result, and a value of 7 indicates a completely negative result. The mean values observed tend towards positive internet associations, with the most negative mean – the negative internet attitude subscale reflecting less of a willingness to disagree with negative statements than there is to agree with positive statements.

There is a small difference between the means when compared to the Morse *et al.* study but there are a few factors that could explain this; (1) Morse *et el.* included two extra statements – *"I feel that the Internet limits my productivity"* (Left out altogether due to recommendation from Morse *et al.*) and *"I only feel comfortable using online stores to browse or compare prices"* (Excluded from statistical analysis as this led to higher Cronbach's alpha) which could influence the mean. (2) The participants in the Morse *et al.* study were all recruited from a psychology participant pool at a large university, with ages ranging between 18 and 50 with an average age of 19.07. This is a fairly skewed sample. The age distribution in the current study is shown in the table below.

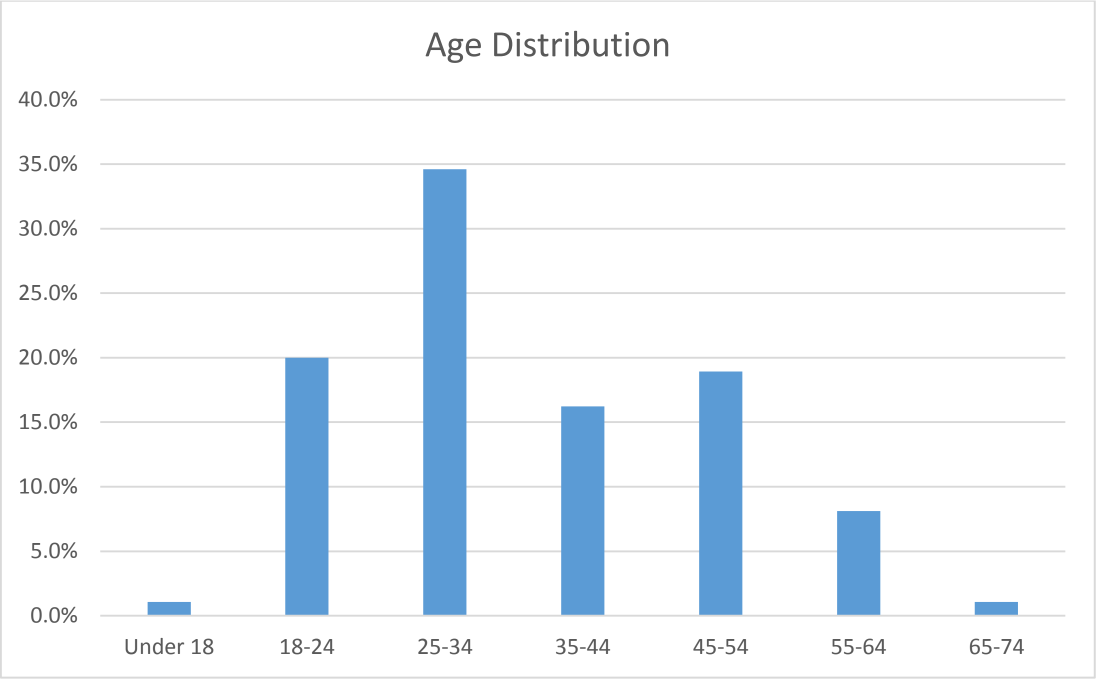


Figure 5-6 Age Distribution of Participants

As the ages were collected within ranges, the exact mean is unknown but it falls somewhere in the 25-44 range. The current status of participants with regards to educational status was not collected, so it is unknown how many of the current sample are students. However, these factors could explain the slight differences in results.

5.6 Section C: Crime Perceptions

5.6.1 Introduction

The crime perceptions assessment was the main purpose of the Cybercrime Survey and aimed to answer the research sub-question "*Are cybercrimes perceived as being less serious than non-cybercrimes?*" This section will walk through the results of the sub-sections within the survey, reporting the results and assessing the implications.

5.6.2 Subsection One: Rankings and Punishments for Brief Descriptions

Question 5 in the first question asked participants to rank the crimes in order of seriousness. The table below shows the overall rank based on the sum of all participants. (Note: These values are reversed, i.e. ranking a crime as number 1 (most serious) gives it 6 points, second gives it 5 points etc.

Ranking	Crime	Total Points
1	Man Assaults Female Partner	983
2	Armed Burglary	882
3	Hackers Steals Credit Card Numbers	658
4	Fraud of €50,000	538
5	Phishing Scam to Steal Images & Passwords	516
6	Hack & Deface Website	308

Table 5-3 Overall Crime Seriousness Rankings

With the exception of "Hacker Steals Credit Cards" ranking higher than "Fraud of €50,000", cybercrimes were rated as being less serious than non-cybercrimes. A slightly deeper look at the responses can be seen in the bar chart below. For each response, crimes that were ranked first or second most serious were placed in the "*High Seriousness*" category, third and fourth most serious in the "*Medium Seriousness*" category, and fifth and sixth in the "*Low Seriousness"* category.

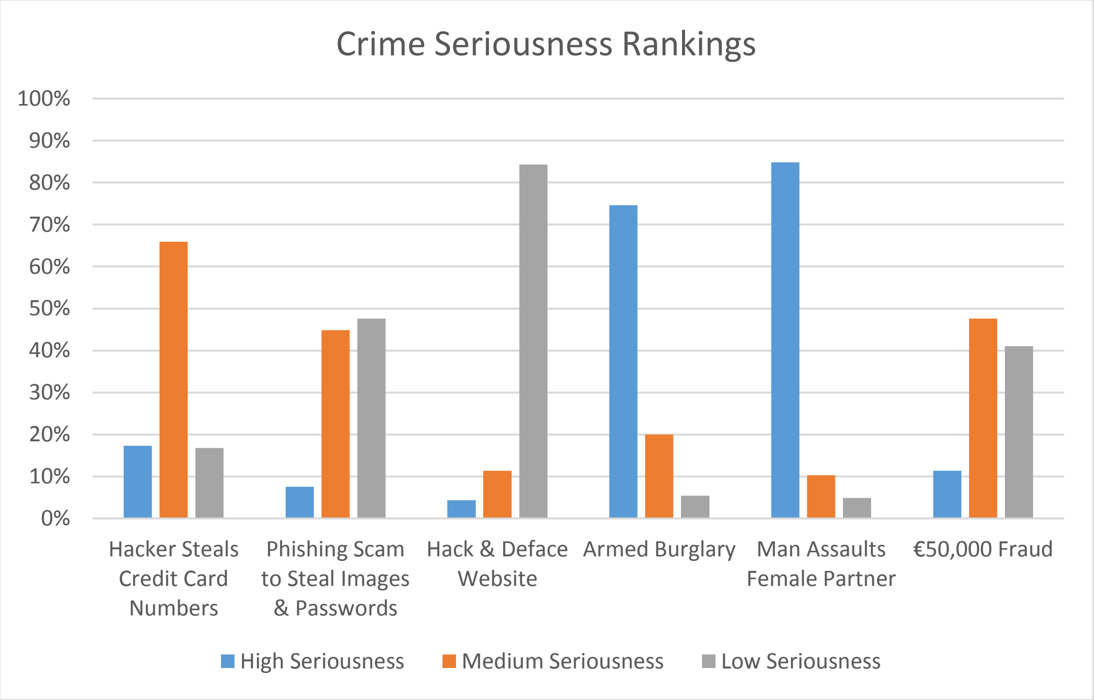


Figure 5-7 Frequencies (%) of rankings per each crime

None of the cybercrimes received very many rankings of high seriousness, while two of the non-cybercrimes received over 80% high seriousness. Additionally, one of the cybercrimes was ranked by over 80% of participants as low seriousness. These results, based on the very brief descriptions of the crimes indicate that the cybercrimes are being perceived as less serious than the non-cybercrimes.

Question 6 asked participants to decide on a sentence for each of the crimes, given the same brief crime descriptions as in the previous question. The answers are summarised in the bar chart below:

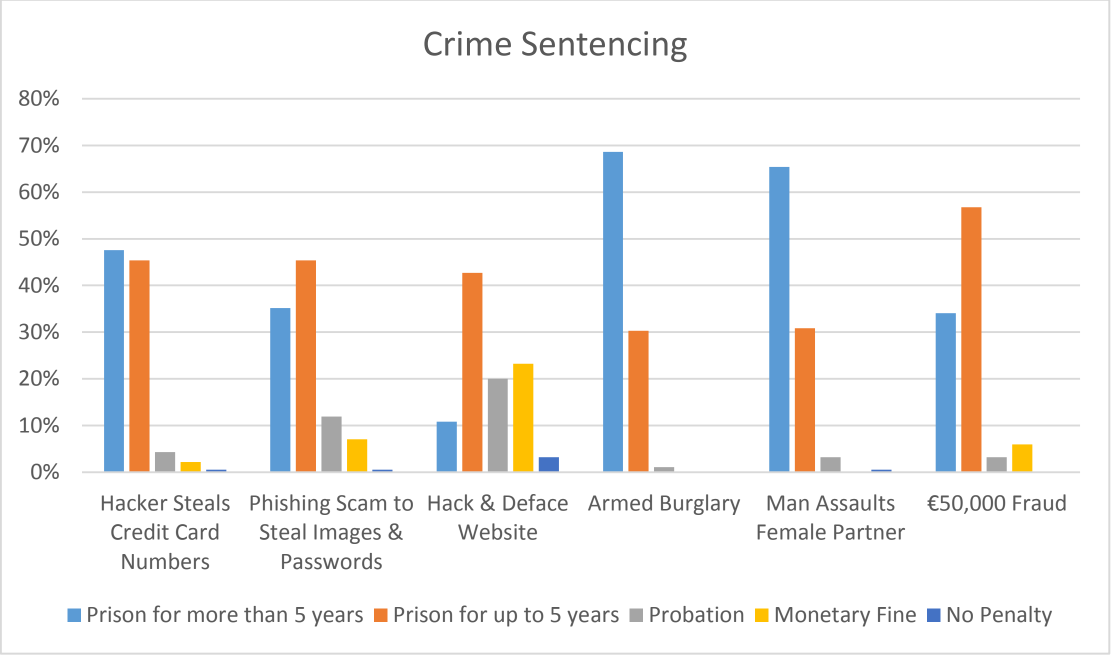


Figure 5-8 Crime sentences for Brief Descriptions (Note: Y-axis truncated at 80%)

For display purposes, the prison sentences have been grouped (Prison for more than 5 years: [Life imprisonment, Prison for more than 10 years, Prison for 5-10 years], Prison for up to 5 years: [Prison for 1-5 years, Prison for less than 1 year]. As with the previous question, there does not appear to be any ambiguity surrounding seriousness or punishments for armed burglary and domestic abuse; over 60% of respondents answered in favour of more than 5 years prison for each of these crimes. Fraud of €50,000 shows surprisingly high counts of prison sentences given that it mostly received rankings of medium and low seriousness in the previous question. Perhaps even more surprisingly, 54% of respondents advocated a prison sentence for hacking and defacing a website in contrast to the 84% that rank it as low seriousness in the previous question. The results from this question suggest that people may be more punitive towards cybercrimes than the relative rankings of seriousness imply, but continue to support the hypothesis that cybercrimes are perceived as being less serious than non-cybercrimes.

5.6.3 Subsection Two: Detailed Crime Scenarios, Verifying Questions & Aims of Sentences

Introduction

In order to go through the results of the questions in this section, the scenarios are paired up; three pairings of a cybercrime and a non-cybercrime. Ideally, they would be paired up with a crime of equivalent seriousness and sentencing, but as that would require a quantification of absolute seriousness, and the selection of cybercrime scenarios were restricted to what was available as having occurred, this was not possible. The phishing scam and fraud of €50,000 were paired together as they both received the lowest sentences in the cyber and non-cyber categories respectively. The website hack and defacement crime was paired with armed burglary as they both received the same sentence (2 years imprisonment). The credit card number theft crime was tricky as it received a sentence that was drastically higher than any of the other crimes. However, it was deemed apt to pair it with domestic abuse as that received the highest ranking in Section 1 of the crime perception section – rank by seriousness based on brief descriptions. It received 100 points more than any other crime and over 300 more than the credit card theft scenario.

The results from participants that selected "Other" in the crime sentencing questions will be discussed in the "Notable Answers" section later in this chapter. A small point of note on punishments is that it is difficult to determine which is the most and least punitive between probation, community service and monetary fine as the impact of each would be dependent on the situation of the person in each case.

Phishing Scam vs Fraud of €50,000

The bar chart below gives an overview of the sentences participants chose for the phishing scam compared to fraud of €50,000:

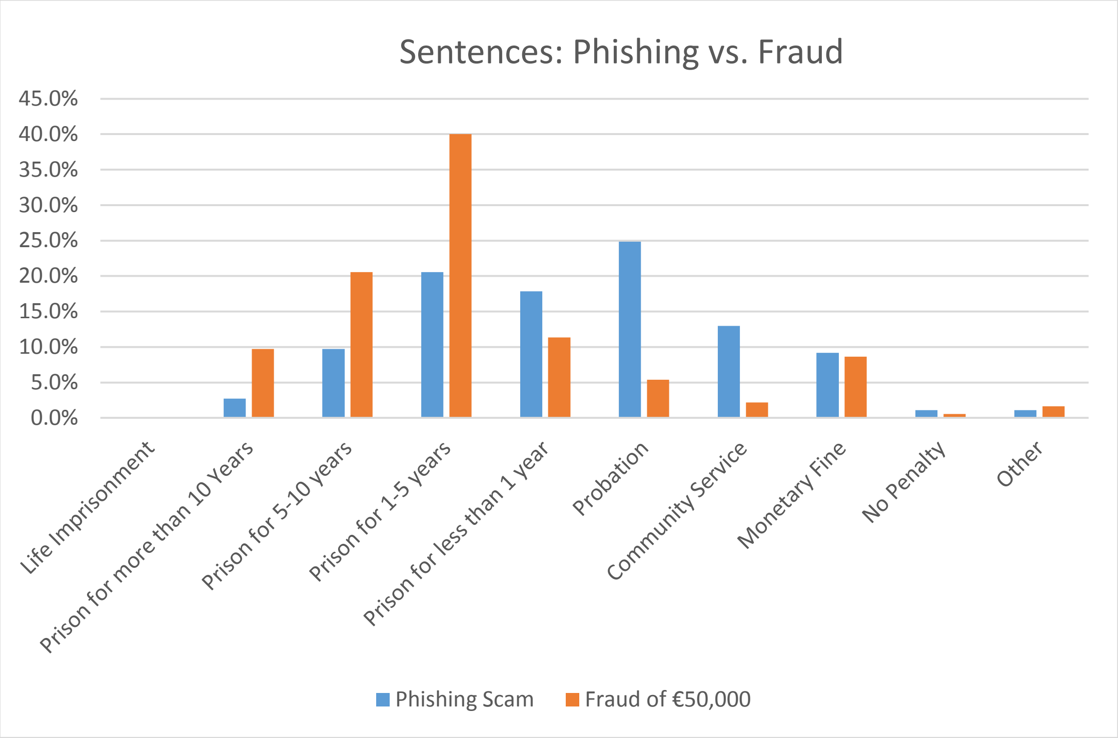


Figure 5-9 Sentences for Phishing Scam vs. Fraud of €50,000 (Note: Y-axis truncated at 45%)

50% of participants chose a prison sentence of some length for the phishing scam, compared to slightly over 80% for fraud. This is a significant difference, particularly when it is taken into account that in actuality the phishing scam received a prison sentence of six months and a $3000 fine, compared to the 150 hours community service that the fraud crime received.

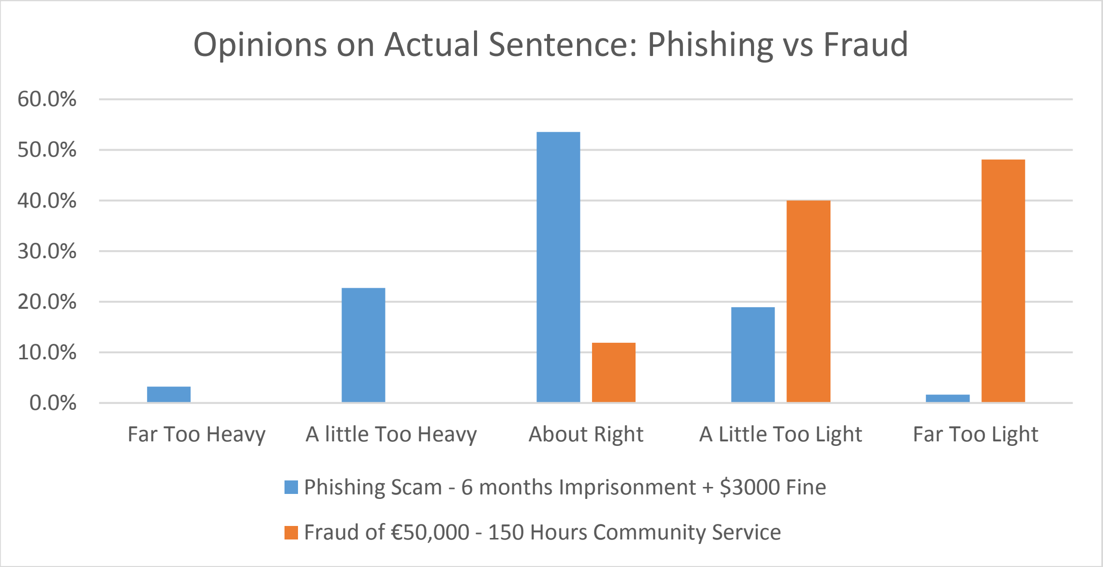


Figure 5-10 Phishing Scam vs. Fraud of €50,000 – Judgement of Sentence (Note: Y-axis truncated at 60%)

The verifying questions confirm the previous results, as only 12% agree that the sentence of 150 hours community service for fraud was about right while the other 88% of participants felt that it was too light. The majority of participants were spread between probation and prison for up to five years for the phishing scam crime, with distribution tapering off at the more extreme ends of the scale, a similar distribution is observed in the verifying question with slightly over 50% agreeing that the punishment of 6 months imprisonment & $3000 fine was about right. The results from this particular comparison are consistent across the questions and indicate that people are less punitive towards cybercrime in this instance, or perhaps that they are more punitive towards non-cybercrime. Identification of the exact nature of the difference goes beyond the scope of this study, so it suffices to say that there is a difference, and it is less for cybercrime than it is for non-cybercrime.

Hack & Deface Website vs. Armed Burglary

The bar chart shown below conveys the sentences that were chosen for the website hack and defacement crime for comparison with armed burglary:

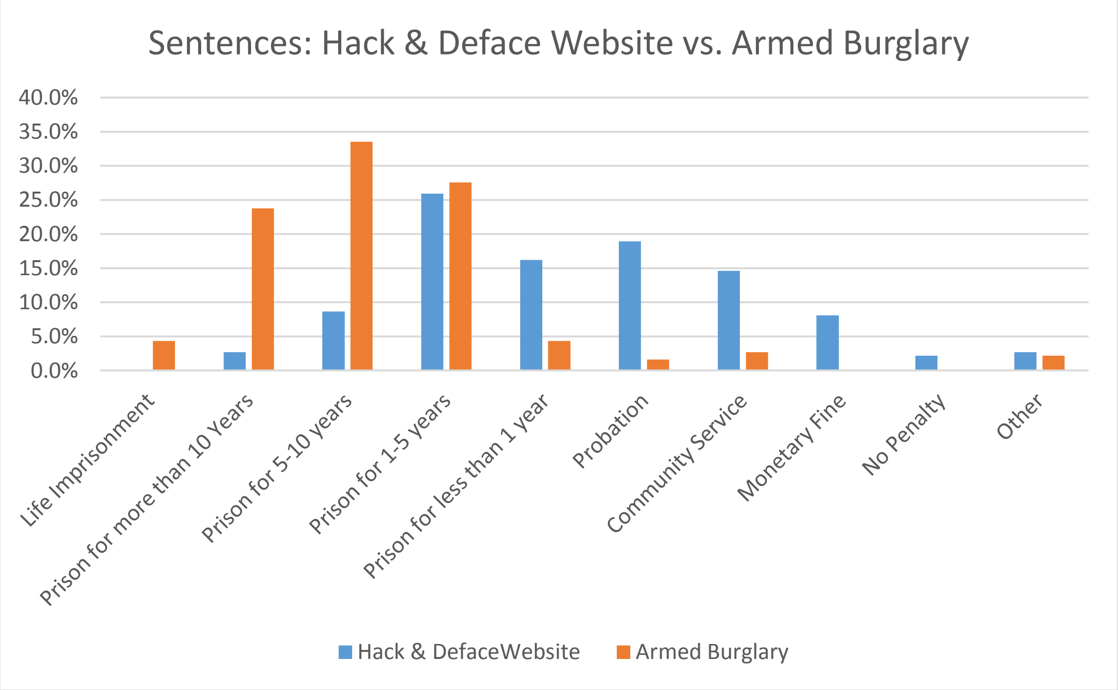


Figure 5-11 Sentences for Hack & Deface Website vs. Armed Burglary (Note: Y-axis truncated at 40%)

Just over 50 % of respondents chose a prison sentence for the website hack and defacement crime, compared to just shy of 90% for armed burglary. The distribution of responses for the website hack and defacement crime is quite similar to that of the phishing scam in the previous pairing. The slight difference between them is consistent with the relative rankings of seriousness based on brief descriptions from part one of the crime perceptions section where phishing was ranked one place above it.

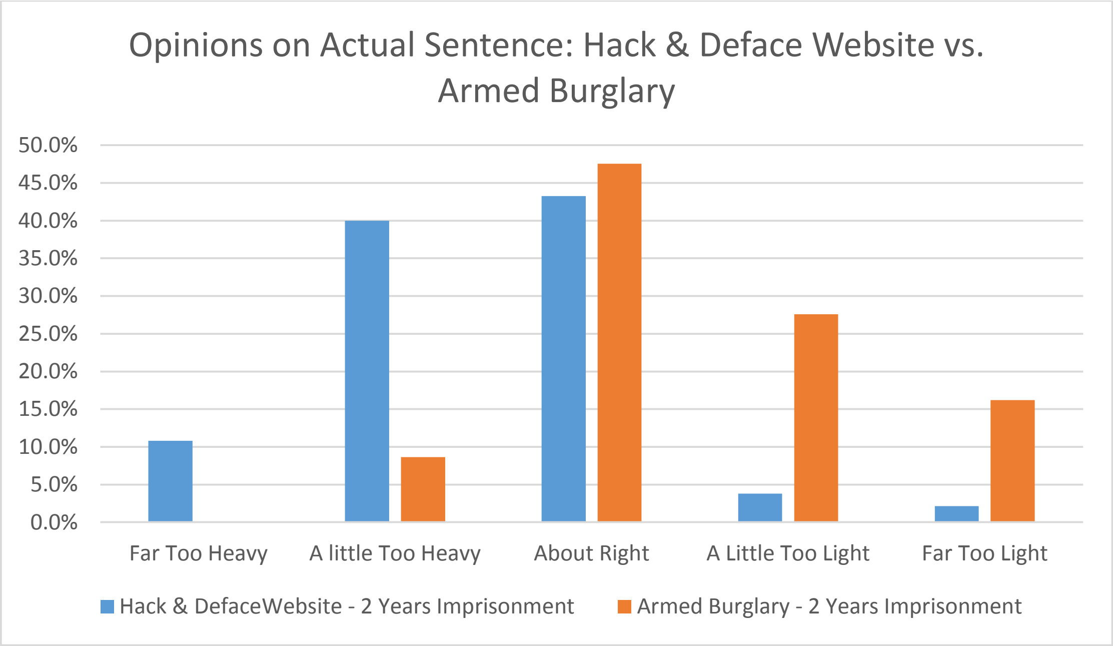


Figure 5-12 Hack & Deface Website vs. Armed Burglary – Judgement of Sentence (Note: Y-Axis truncated at 50%)

The verifying questions support the view that people are less punitive towards cybercrimes. While just over 40% for each crime agree that the sentence is about right, with the exception of less than 10% of cases for each crime, the rest of the participants felt that 2 years for the website hack and defacement crime was too heavy while 2 years for armed burglary was too light. The findings on this pairing are particularly relevant as the actual sentences for the two crimes were the same. As with the previous pairing, the answers across the questions are consistent and support a difference in attitudes towards cybercrime when compared to non-cybercrime, wherein cybercrimes are viewed more lightly.

Hacker Steals Credit Card Numbers vs. Domestic Abuse

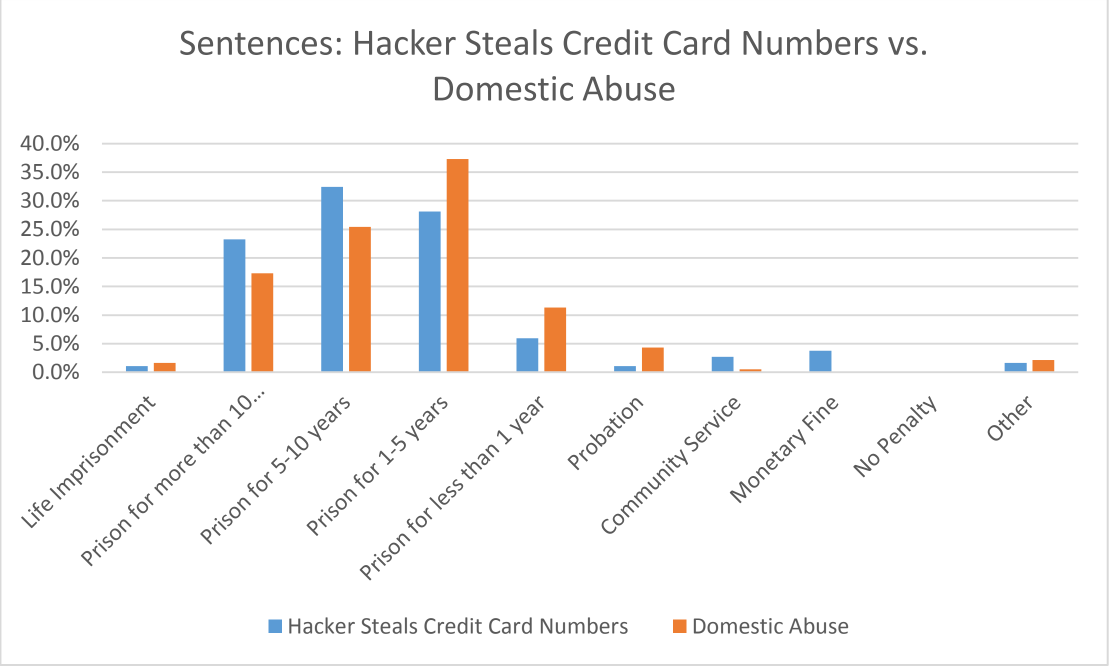


Figure 5-13 Sentences for Hacker Steals Credit Cards vs. Domestic Abuse (Note: Y-axis truncated at 40%)

In both of these cases, a prison sentence was recommended by over 90% of participants and there does not appear to be a huge amount of variation between the overall distributions for the two crimes. This similarity is perhaps one of the most interesting statistics from this study as there is a vast difference between the actual sentences for the two crimes; 27 years for the credit card numbers theft and 6 months' probation for the domestic abuse case. As just over 55% of participants recommended a prison sentence greater than 5 years (24% of these chose over ten years) for the credit card theft case, these numbers do no not differ too greatly with the actual sentence. On the other hand, there is an astounding difference between the distribution of sentencing for domestic abuse and the actual sentence. This data may suggest that the difference in attitudes towards cyber and non-cybercrimes results mostly from more punitive attitudes towards non-cybercrimes. There is likely further difference between violent and non-violent non-cybercrimes and this cannot be stated with certainty without further and deeper statistical analysis that goes beyond the scope of this study.

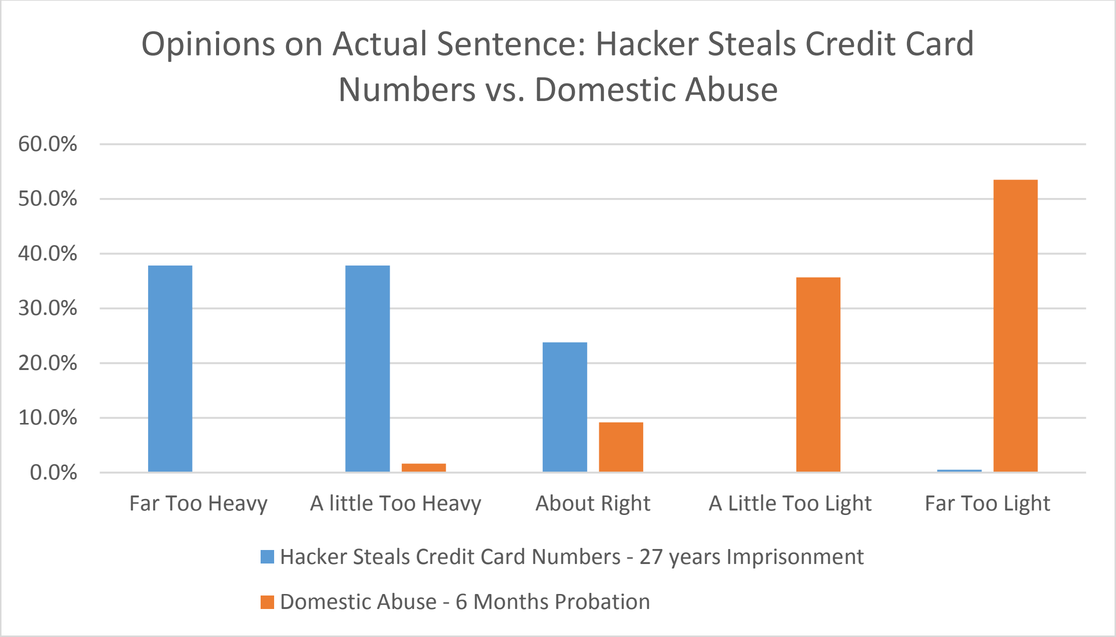


Figure 5-14 Hacker Steals Credit Cards vs. Domestic Abuse - Judgement of Sentence (Note: Y-Axis truncated at 60%)

The verifying questions support the statistics from the initial question for each crime. Just under 25% agree that 27 years for the credit card numbers theft scenario was about right, compared to just under 10% for the domestic abuse scenario which received 6 months' probation. There is a very clear division here with the other 75% believing the 27 year sentence was too heavy, while for domestic abuse, just about 90% decided the sentence of 6 months was too light. The vast difference between the sentences for these scenarios makes any conclusions tentative, but these statistics support the findings from the previous two pairings that people are less punitive towards cybercrimes than they are towards non-cybercrimes.

Aims of Sentences

The bar chart below shows a comparison of the aims of sentencing between cyber and non-cybercrimes. As participants could choose between one and 3 answers, the bar chart represents counts instead of percentages:

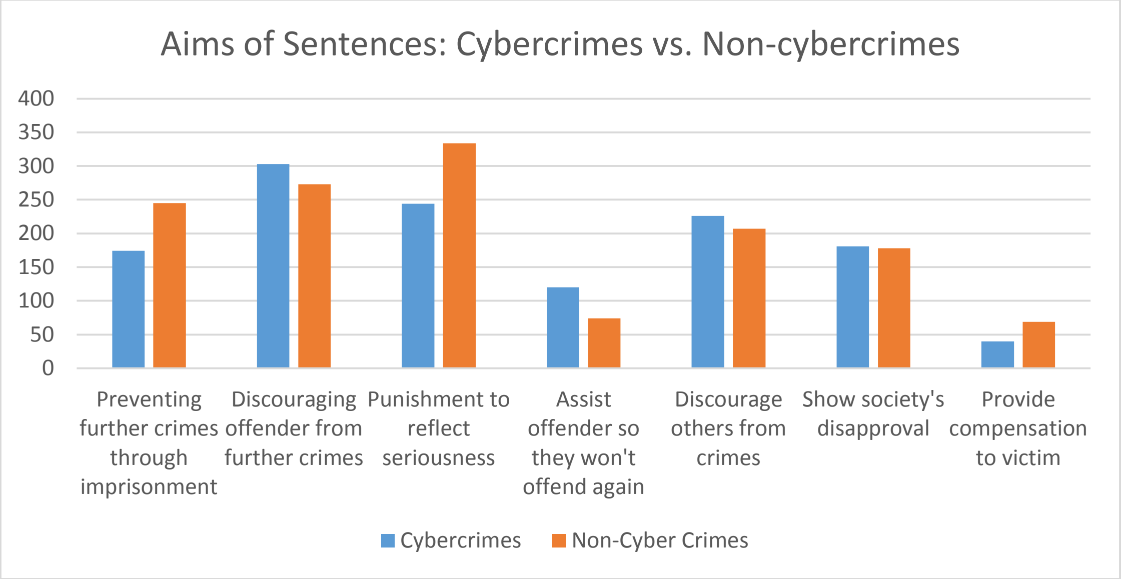


Figure 5-15 Sentence Aims for Cybercrimes and Non-cybercrimes

There does not appear to be a significant difference between the aims for the two crime categories, with a similar pattern of distribution for both. A noteworthy observation is that the second lowest aim in both categories, "Assist offender so they won't offend again", is the category that would represent rehabilitation. It appears that people want to see prevention and discouragement of repeat offence through punishment, rather than rehabilitation. With regards to the research question, the aim of the sentence does not appear to differ between the two crime types and so is unlikely to play a significant factor in differences in sentence choices between the two categories.

Examination of Subgroups

A comparison of some answers was carried out between subgroups identified through demographic measures and the lawfulness questions. This comparison was carried out on the "Hack and Deface Website" and "Armed Burglary" detailed description sentencing questions. These two scenarios were chosen as they were both given the same sentence (2 years imprisonment). The sub groups that were compared were:

- Gender: *Male vs. Female*
- Primary Country of Residence: *Ireland vs. Other*
- IT Familiarity: *"IT savvy"* (Work in security related field in IT, work in non-security field in IT, don't work in IT but familiar with computer related technologies) *vs. rest*
- (You or Someone Close to You) Victim of Cybercrime: *Yes vs. No*
- Other People Should obey Laws and be Punished: *Agree vs. Disagree*

- Prison is the Best Method of Punishment for a Crime: *Agree vs. Neutral vs. Disagree*
- Prison is the Best Method of Rehabilitation for a Crime: *Agree vs. Neutral vs. Disagree*
- Total Internet Attitude: *Positive vs. Negative*

Surprisingly, the answers were generally consistent across the groups. This is illustrated by the two bar charts below depicting the comparison across the "Victim of Cybercrime" category.

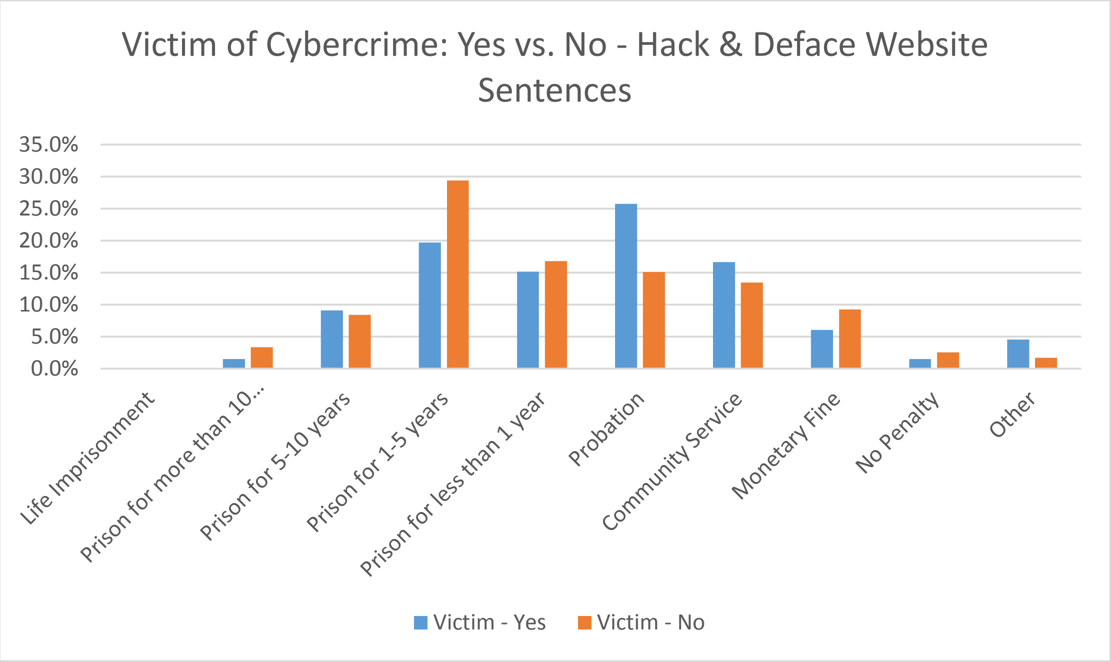


Figure 5-16 Comparison of Sentences across Victim of Cybercrime Yes vs. No for Hack and Deface Website Crime Description (Note: Y-axis truncated at 35%)

As can be seen, the distributions are very similar for the "Hack & Deface Website" scenario, the only notable slight inequalities are the differences between "Prison for 1-5 years" and "Probation". This is unusual though as the "Victim – No" group is higher in the prison category while the "Victim – Yes" group is higher in the probation category. This is the opposite of what might have been expected. It is possible that this could be as a result of sample size and may even out with a larger sample. Possibly, past encounters with cybercrime do not have an influence here as the rest of the distribution suggests and this discrepancy is simply an arbitrary difference. There was no particular differences for the armed burglary crime scenario as can be seen below.

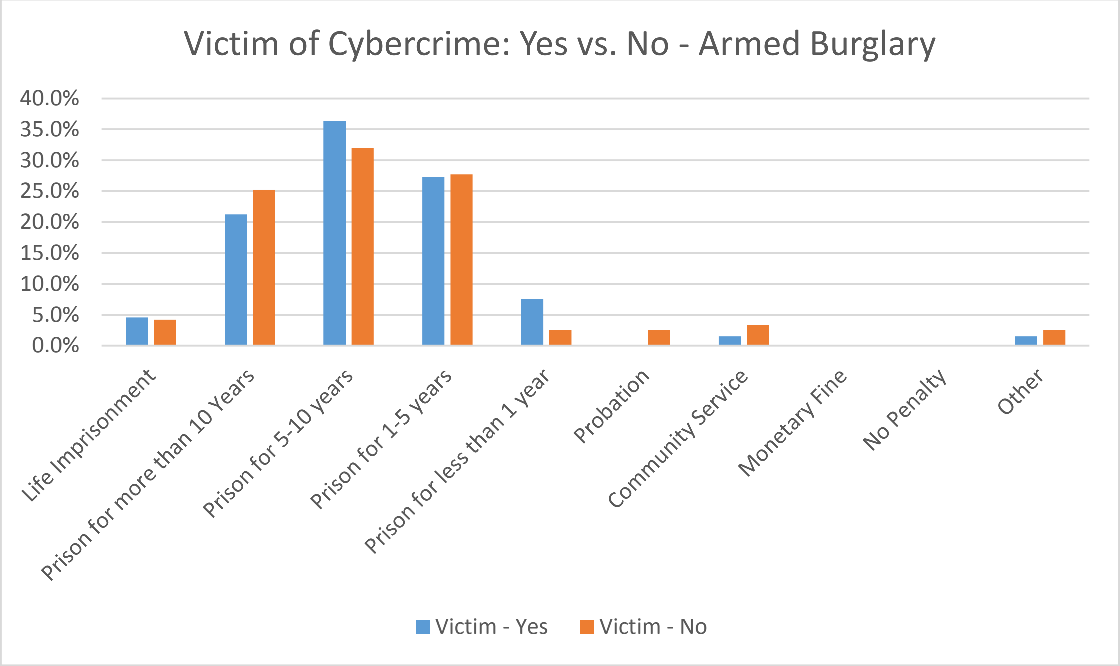


Figure 5-17 Comparison of Sentences across Victim of Cybercrime Yes vs. No for Armed Burglary Crime Description (Note: Y-axis truncated at 40%)

The general consistency across all of the subgroups indicates that the questions in the Cybercrime Survey were well formed and unambiguous. The bar charts for all the subgroups compared can be found in Appendix B.

One grouping that did show slight differences, albeit still with the same general distribution is the “Prison is the Best Punishment” subgroups, shown in the bar charts below.

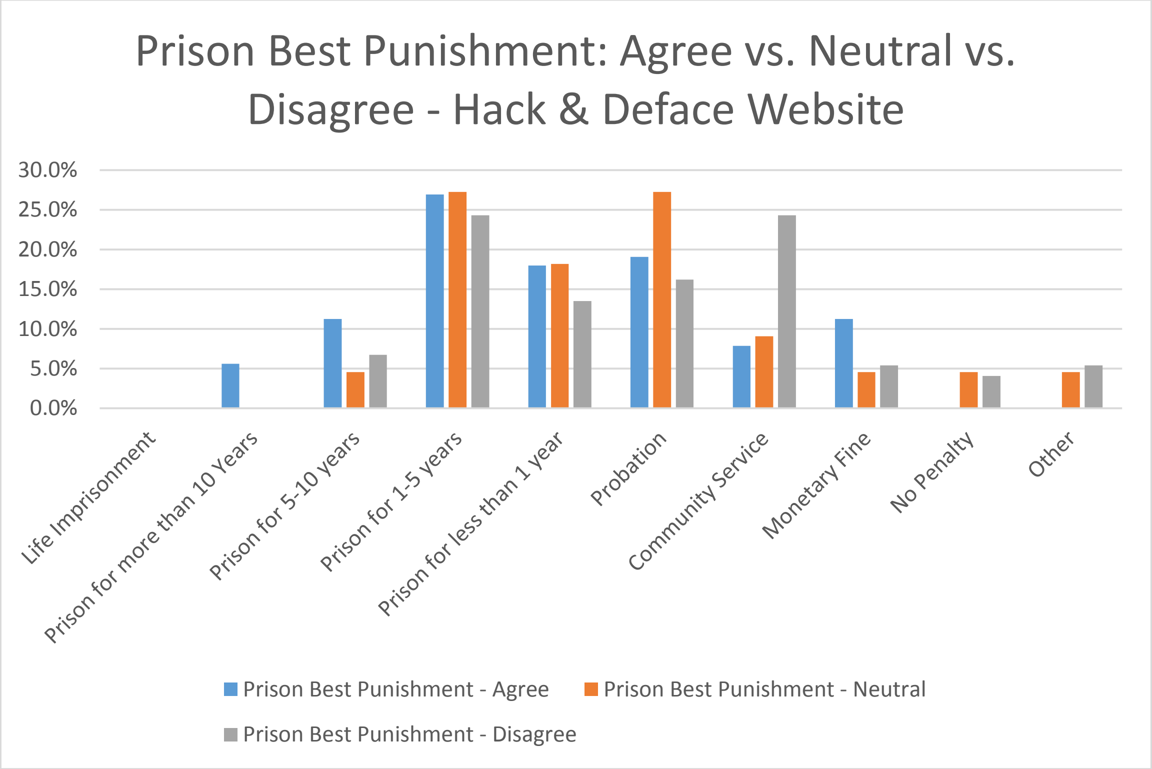


Figure 5-18 Comparison of Subgroups across Agree, Neutral & Disagree with "Prison is the Best Method of Punishment for a Crime" for Hack & Deface Website Crime Scenario (Note: Y-axis is truncated at 30%)

The results align somewhat with what might be expected, although possibly to a lesser degree than one might expect, There is a higher tendency towards prison sentences in the "Agree" category, and a spike in the "Probation" and "Community Service" sentences for the "Neutral" and "Disagree" categories respectively. However, almost 45% of those in the "Disagree" category chose a prison sentence as the sentence for the Hack & Deface Website scenario. This pales in comparison to the sizable proportion of 86.5% of those that disagreed with the statement "Prison is the Best Method of Punishment for a Crime", and 100% of those that claimed neutrality to it recommending a prison sentence as the best punishment for armed burglary as can be seen in the bar chart below. This difference supports all other findings within this study that indicate people are less punitive towards cybercrime/more punitive towards non-cybercrimes but also adds to another observation that people do not feel that prison sentences are a good solution, but do not have any alternatives to offer. This is also discussed in the "Notable Answers" section below.

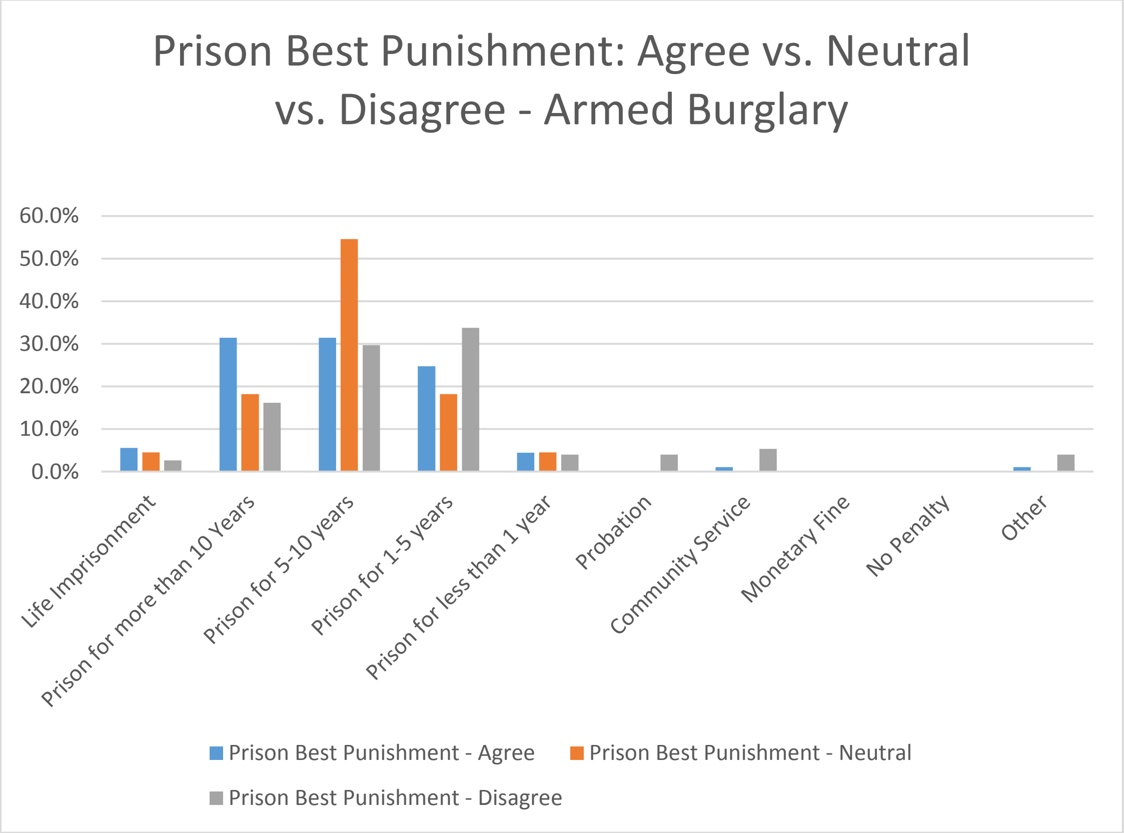


Figure 5-19 Comparison of Subgroups across Agree, Neutral & Disagree with "Prison is the Best Method of Punishment for a Crime" for Armed Burglary Crime Scenario (Note: Y-axis is truncated at 60%)

Notable Answers

The "Other" answer option with a text box for elaboration is a useful source of information in a survey. While it does not fit well with statistical analysis, it can allow people to provide answers that might help to highlight issues with a survey, or provide interesting insights. In the Cybercrime Survey, an answer in the text box was required if the "Other" option was selected.

We will now discuss some of these answers from the six "Sentencing for detailed description of crimes" questions. With the exception of grammatical corrections, no changes have been made to any of the answers quoted.

There are two main categories that these answers fall into. The first is that a number of the answers consisted of combinations of answer options that were available as individual options, e.g. "*Prison for less than a year, probation and community service*". 10 of the 20 "Other" answers across the 6 questions were of this nature. This highlights a potential shortcoming with the survey; it was not possible to select more than one sentence. This was in conflict with some of the survey content as one of the crime scenarios received a combined sentence (Phishing: Imprisonment & Fine), an option that respondents were not able to select when they were determining sentences. It is possible that this may have impacted the results on a per item basis, however, as this limitation applied to all the questions, i.e. both cybercrime and non-cybercrime questions, then it is unlikely to have an impact on findings related to the research question as they were all answered under the same conditions.

Answers in the second category are those that suggest a dissatisfaction with the options available in the legal system. Some suggest alternatives, however, a few answers simply convey the message "*Something else but I don't know what*". Some examples of the answers that offer alternatives are:

- Armed Burglary
  - "*Find Paul a job so he won't have to steal"*
- Hack & Deface Website
  - "*Get Jane to fix the breach in the system + probation*"
- Phishing Scam
  - "*Psychiatric evaluation and treatment*"

One particular participant, Respondent 133, at first glance looked like a peculiar outlier, e.g. four "No Sentence" answers out of six in the sentencing for brief descriptions question. However, once the "Other" answers were reviewed (participant gave them for 5 of the 6 detailed description questions), it is apparent that Respondent 133 simply was not satisfied with any of the options. The answers offered reflect very definite opinions that are quite insightful:

- Armed Burglary
  - *"Indentured military service of an undefined term reviewed every 3 months (N.B. * prison solves nothing, put them to work or put them to death)"*
- Hack & Deface Website
  - "*Anonymous or promoting her online identity... pick one. Jane is a civilly minded citizen, highlighting the wilful negligence of a hack-able public service system is not a crime... it's a service.*"
- Domestic Abuse
  - "*Peter is mentally unstable, Peter needs indefinite support from the health services. They decide when he is no longer a danger to others.*"

- Theft of Credit Card Numbers
    - *"It's a money crime... so take his money away. All of it if you have to."*
- Fraud of €50,000
    - *"It's a money crime, take her assets and money including future earnings to make the client whole... include punitive damages."*

The "Hack and Deface Website" answer highlights a potential source of confusion for some participants; if they were not familiar with the hacktivist collective Anonymous, or if they were confused or unfamiliar with the concept of hackers having online identities under which may seek notoriety or glory for online while keeping their actual identities hidden, then the question could potentially have seemed like it contained a contradiction. However, as mentioned in the "Examination of Subgroups" section, there is a consistency of answering across all groups which suggests that this did not have a significant negative impact on the data.

This answer also provides an interesting approach to the legal response to hacking – suggesting that the onus is on the owners of any public system, such as a website, to ensure that it is not hackable and the accountability does not lie with the hacker. However, it is questionable what protection this approach offers to users of the internet. All of Respondent 133's answers are linked with the idea that prison is a poor method for rehabilitation, and not the best solution as a punishment either. This has also been suggested by the data from all participants, albeit not particularly strongly, in the "Lawfulness" section – the mean answer for "Prison is the Best Method of Punishment" was "Neutral" and for "Prison is the Best Method of Rehabilitation" is "Slightly Disagree". This may suggest, as was also mentioned in the "Examination of Subgroups" section (comparison of those who answered in agreement, neutrality, and disagreement with "Prison is the Best Method of Punishment") that while people do not appear to agree with prison as a solution, they are reluctant to actively disagree with it as they do not have an alternative solution.

5.7 Section D: Hacking Resources Awareness & Opinions

5.7.1 Introduction

The aim of the questions in this section was to answer the research sub-question "*Are people aware of the type of hacking resources that are available online?*" and this was done through presenting participants with some of the information derived from the assessment of these resources. The results of this will be presented below, first the tools, and then the courses.

5.7.2 Hacking Tool Awareness

Participants were reasonably accurate in making the distinction between real and fake tools, as can be seen in the bar chart below:

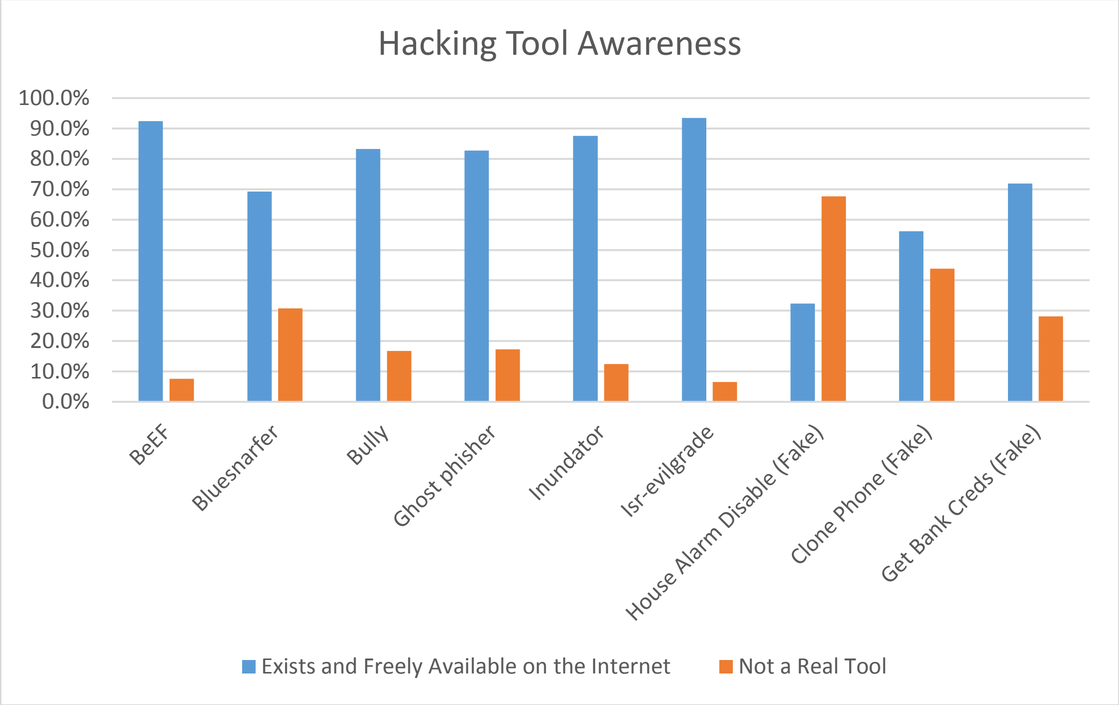


Figure 5-20 Hacking Tools Awareness

For all of the tools except the fake “Clone Phone” tool (clones phone AND all data on it by placing it next to it for 2-3 minutes) and the fake “Get Bank Creds” tool (Steals internet history over Wi-Fi and uses this to access bank accounts previously accessed in the browser), the majority of participants in each case accurately distinguished between real and fake tools. This suggests an awareness of some of the different ways that people can be targeted by malicious hackers, but also indicates that there is possibly a slightly fearful attitude as a result of an impression that “anything is possible”. As will be discussed again later in the “Results Meta-Analysis” chapter, films or TV shows may be responsible for the belief that phones can be cloned easily. The 72% that believe the “Get Bank Creds” tool is real however this may also be partially as a result of some technicalities around the fake tool descriptions that will be discussed further in the

"Results Meta-Analysis" chapter. In spite of this, the general awareness levels of the type of tools available on the internet indicate that this awareness likely also applies to potential script kiddies, even before they set out on the "script kiddie path". This availability of tools with these capabilities combined with the awareness of their availability could be a significant factor in setting them on this path.

5.7.3 Hacking Course Availability Opinions

This section focused on opinions about the availability of the courses rather than awareness as potential users are likely to discover them as they seek help to figure out how and when to use the tools that are available. The results are displayed in the two bar charts below which were separated into two purely for display purposes.

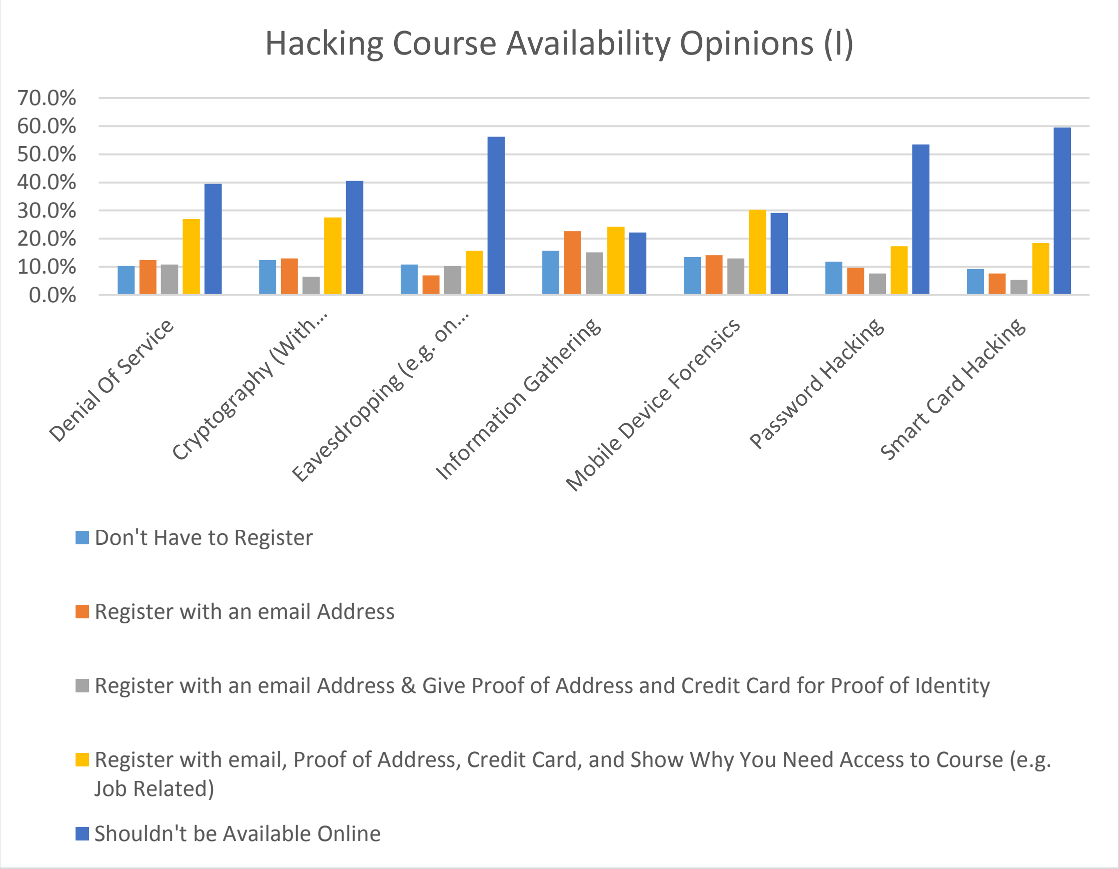


Figure 5-21 Hacking Course Availability Opinions Part 1 (Note: Y-Axis truncated at 70%)

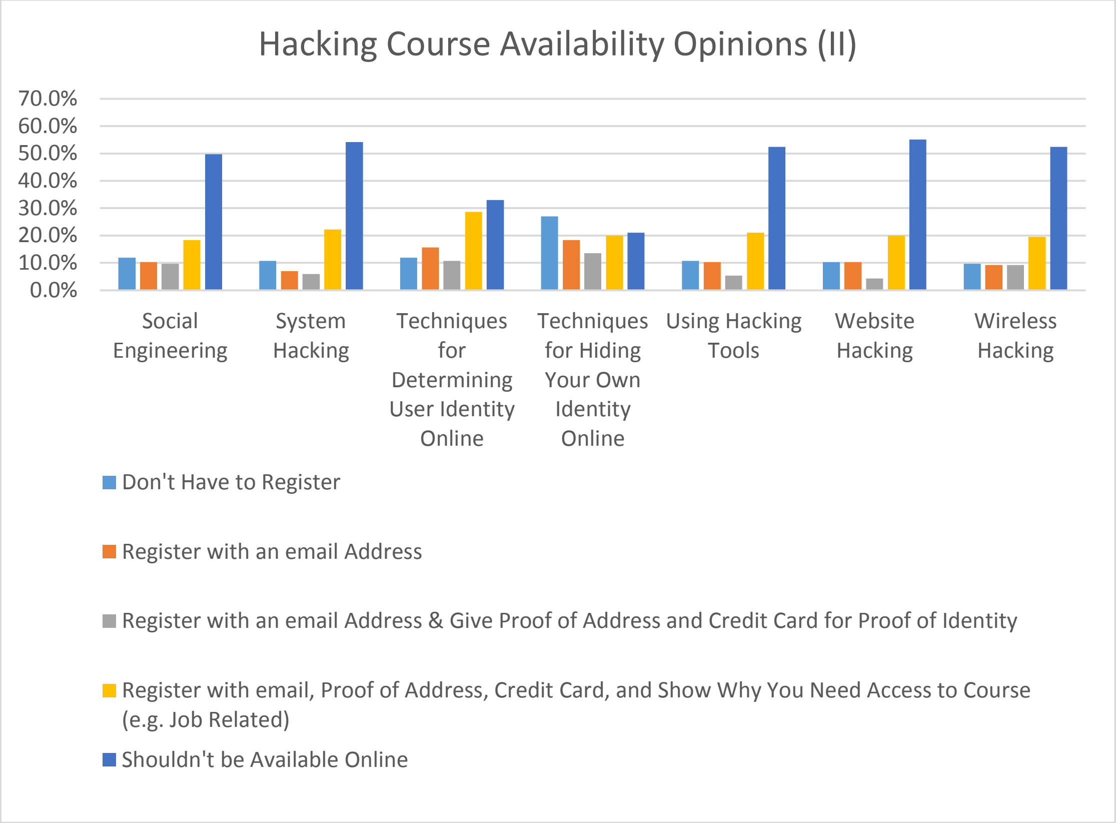


Figure 5-22 Hacking Course Availability Opinions Part 2 (Note: Y-Axis truncated at 70%)

With the exception of just four of the course topics, a clear majority of participants voted that the courses for that topic should not be available online, overwhelmingly in some of the cases with margins as big as 40% (Smart Card Hacking & Eavesdropping). Unsurprisingly, the four topics that had a more even distribution were for techniques that do not involve attacks, or potentially illegal activities; Information Gathering, Mobile Device Forensics, Techniques for Determining User Identity Online, and Techniques for Hiding Your Own User Identity Online. An interesting subgroup to investigate is those that work in IT security. This group was found to display a tendency towards the opposite opinion; all courses should be available without having to register. However, as this group only consisted of 8 people, the sample is too small to be of statistical use.

5.8 Key Findings

From this analysis some of the key take-away points are:

- There is a difference in attitudes towards cybercrimes and non-cybercrimes, where there is generally a more punitive attitude towards non-cybercrimes.
- It appears that past encounters with cybercrime do not have an influence on attitude to cybercrimes
- People do not feel that prison sentences are a good solution, but do not have any alternatives to offer.
- The aims of sentences that people provide are quite similar across cybercrimes and non-cybercrimes and are generally more punitive than rehabilitative.
- People are generally accurately aware of the types of hacking tools that are available online.
- There appears to be a general consensus that any courses that teach any form of hacking attack should not be available online

5.9 Conclusions

In this chapter the results of the Cybercrime Survey were presented and analysed. First the demographics were presented, indicating that the Cybercrime Survey sample was a well distributed sample and a good representative of the population. The findings from the lawfulness section indicated that the participants were generally quite lawful and believed in punishment for crimes, but were not overly satisfied with prison as a solution. The internet attitudes scale results suggested that people generally have quite positive attitudes towards the internet, with the most negative answers reflecting a disinclination to disagree with negative statements that generally referenced security indicating that security concerns could be the main issue that people associate with the internet. The crime perceptions section found that people do view cybercrimes as being less serious than non-cybercrimes and are generally more punitive towards non-cybercrimes than cybercrimes. In the hacking resources section people were generally accurate in identifying the real hacking tools, but the majority of the sample showed two false positives on the fake tools. A general agreement was identified among participants that hacking courses teaching offensive methods should not be available online.

The findings from the literature review confirmed the first research sub-question; people are more likely to engage in illicit activities online then they are in the physical world, and these findings suggest that the second and third research sub-questions can also be answered affirmatively. This will be discussed further in the “Conclusions and Future Work” chapter.

6 CYBERCRIME SURVEY RESULTS: META-ANALYSIS BY EXPERTS

6.1 Introduction

After the analysis had been carried out on the responses to the Cybercrime Survey, some of the results were combined into a presentation that was given to some security experts in order to help validate the Cybercrime Survey and the findings. This was done in order to confirm the findings with individuals who are very familiar with the topics. Feedback from an expert was particularly relevant for the hacking resources section as it allowed the questions to be assessed by people who understood all of the concepts extremely well, and also allowed for some educated insights.

This chapter will present that information in the following way, first the design of the exercise will be explained, followed by the feedback for the crime perceptions section and the hacking tools and courses section. Implications of the feedback will also be discussed.

6.2 Design & Participants

The expert review process was designed to provide the experts with the essential information that was uncovered based on the results of the survey process. It was felt that if all of the results were presented to the experts, this would be very time consuming for them, and counter-productive to the research. Instead, prior to the presentation of the slideshow, the participants were shown a preview version of the survey (a function offered by www.smartsurvey.co.uk that allows the user to view an identical version of the survey without needing to answer the questions before moving on to another page). The sections that were chosen to analyse were Section 1 of the Crime perceptions section, i.e. rankings and sentences for brief crime descriptions, and the hacking resources section. This amounted to four questions in total, although the two hacking resources questions have a considerable amount of content in each.

The three security experts that participated in the exercise had combined experience of over 10 years in the IT security industry in addition to experience in non-security areas of the industry also. The full set of slides that were used for this presentation can be viewed in Appendix C. The general pattern is that a screenshot of each question was shown followed by one or two slides showing the results of the question. When each question was displayed, the intention behind the question was explained. While the results were shown, the security experts were asked questions on the findings. The answers to these questions were recorded. The participants will be referred to as Expert A, Expert B and Expert C.

6.3 Feedback

This section will go through the feedback received from the three cybersecurity experts on the crime perceptions, hacking tools, and hacking courses results, and additionally some closing questions.

6.3.1 Crime Perceptions

The answers provided will now be discussed as we step through the questions. For both of the crime perception question results, they were asked:

- *Do you agree with the findings?*
- *Do you have any other comments regarding the findings or the question?*

Both Expert A and Expert C felt that fraud of €50,000 was a worse crime than credit card number theft, with Expert A clarifying that it is the market for credit card numbers that needs to be cracked down on and that these crimes will continue to occur unless something is done about the market for buying and selling credit card numbers. Expert A and Expert B felt that phishing (5th overall) should have been ranked higher, although both indicated that further context is important for that decision, e.g. using a phishing scam to steal celebrity pictures and release them to the public is worse than stealing anybody's pictures just for private use. Expert B raised the opinion that media coverage has a considerable impact on crime perceptions as people are used to hearing about trials for non-cybercrimes but very little is heard in the news about trials of cyber criminals. Expert C commented that hacking and defacing a website is not a very serious crime but could merit a custodial sentence if it were a part of a hate crime. Expert B expressed the general opinion that the ranking and sentencing results would look a little bit different if all of the participants surveyed were "info sec savvy". All three agreed that the questions were well formed to obtain the information they were seeking.

6.3.2 Hacking Tool Awareness

For the hacking tools awareness question, participants were asked the following questions:

- *Are you surprised with any of the results?*
- *Do you think the tools were described in a way that conveyed their function clearly to the participants?*
- *Would you have done anything differently? E.g. choose different tools, describe them differently, etc.*

The feedback for the descriptions of tools was very positive here, Expert A raised some potential issues with two of the fake tool descriptions, and Expert C highlighted a potential confusion with the description of one of the real tools. These will be discussed further in the "Cybercrime Survey Feedback Discussion" section below.

Expert B expressed surprise at the amount of people that still considered Bluetooth a secure option (30% of people thought Bluesnarfer (A tool that steals data over a Bluetooth connection) was a fake tool). Other than that there was not many other comments, all 3 were not surprised by the results and felt that the question and descriptions were well formed for their aim.

6.3.3 Hacking Courses Opinions

The three participants were asked the following questions when viewing the results on the hacking course opinions question:

- *Are you surprised with any of the results?*
- *Would you have asked the question any differently?*
- *Do you have any other thoughts/comments on this question?*

All 3 of the experts expressed surprise that the top answer for every category wasn't "Don't Have to Register". They discussed the matter that freely available resources on this kind of information enable people to defend themselves, and that without these kind of resources, the fight against cyber criminals would be more difficult and more frivolous.

6.3.4 Closing Questions

The participants were then asked 3 closing questions:

- *Do you think that people perceive cybercrime to be less serious than other crime (violent and non-violent)?*
- *Do you think cybercrimes deserve the same punishment as violent and non-violent crimes?*
- *Do you think the abundance of resources that are available for ethical hackers enable malicious actors to engage in cybercrimes?*

There was a general agreement for the answers of all three of these questions; all agreed that cybercrime was perceived as being less serious and Expert A also commented that "Breaking and entering isn't the same as opening an unlocked door online into someone's infrastructure". This is a similar opinion to that expressed by Respondent 133 as discussed in the "Notable Answers" section of the "Cybercrime Survey: Results" chapter, wherein the onus is on the owner to ensure the infrastructure is secure against attacks. All three experts agreed that cybercrimes are quite contextual and judgements on the seriousness and prosecution of them should really be taken on a case by case basis. All three also agreed that the hacking resources that are available online are enabling malicious actors, however, the removal of said resources could potentially be a massive blow to the fight against cybercrime; these resources are needed in order to educate the defence.

6.4 Cybercrime Survey Feedback Discussion

The overall feedback from the security experts was that the Cybercrime Survey was well constructed in order to obtain the information that the study was seeking. As mentioned above, there were some potential issues raised about a few of the tool descriptions. On first glance at the tools, Expert A claimed that the "House Alarm Disable" tool and the "Get Bank Creds" tools were real, and Expert C claimed there could be some potential confusion around the description for the Inundator tool.

"House Alarm Disable - A tool that plants malicious software on your phone that will disable your house alarm once you connect to your home Wi-Fi". The intention behind this description was that the attacker using the tool did not need to be nearby, and that the malicious software could be planted at any time or anywhere and once the phone connected to a network that also had a house alarm connected, the house alarm would be rendered useless for future uses. Expert A referred to a Wired article (Wired, 2014) that discusses how attackers can place themselves close to the house and intercept

transmissions from the sensors back to the control panel in order to prevent the alarm from triggering. The other two experts were aware of this technique and identified the fake tool as being a different concept, but it is possible that some survey participants could come to the same conclusion as Expert A. However, this tool was the only one in the list for which the majority of participants voted (correctly) that it was not a real tool, so it is unlikely that this was the case.

"*Get Bank Creds - A tool that steals a phone's browser history over Wi-Fi and uses this to gain access to online banking accounts previously accessed on the phone"*. The intention behind this description was that through some vulnerability the tool could extract the browser history from a device and use this to access any online banking accounts that were previously accessed at any time using the browser. Expert A at a first glance misinterpreted this as being similar to a sniffing attack where passwords posted over HTTP can be interpreted in plain text by an attacker on the same network, or the hijacking of the session. Given the high number of people that thought this was a real tool (just over 70%), it is possible that some users had this same misconception.

"Inundator - A tool that floods a system with "fake" attacks so they can slip in a real attack that might get through unnoticed/unstopped". Expert C claimed that the description seemed a bit vague given the use of the term "system", and that it would have been a bit clearer if the term "firewall" was used in its' place. This is definitely a valid point, and for anyone who knows what a firewall is, it would make the description clearer. However, the design of the Cybercrime Survey aimed to make the survey as accessible as possible to those who are not familiar with the technologies, and so all unnecessary uses of terms were omitted where possible. This was one of those cases where it was deemed not absolutely necessary for the understanding of the function of the tool to include the term so system was used in its' place.

6.5 Conclusions

The survey and a subset of results regarding cybercrime perceptions and the hacking resources section were presented to three cybersecurity experts. The experts were asked a number of questions on each of the result sets presented to them as well as some additional questions at the end. There was a general agreement that the results appeared to be an accurate representation of the general public's opinions and knowledge, but the results might be different if the survey participants all worked in I.T. security. There were no major issues found with the survey itself and the few minor issues that were raised had been justified by the study, or were deemed not to have a significant impact on results. All three cybersecurity experts agreed that there was a difference in the perception of cybercrime compared to non-cybercrime, and that malicious actors were likely to be using hacking resources intended for use only in white hat hacking.

7 CONCLUSIONS AND FUTURE WORK

7.1 Overview of Research, Results & Conclusions

There were multiple streams to the research in this dissertation that combined to answer the research question:

> *Does the nature of behaviour online and the landscape of the world-wide web combined with current attitudes towards cybercrime, create an environment that encourages people to more readily engage in criminal activities online?*

In order to best approach the research question, it was broken down into three research sub-questions:

1. *Are people more likely to engage in illicit activities online compared to in the physical world?*
2. *Are cybercrimes perceived as being less serious than non-cybercrimes?*
3. *Are people aware of the type of free hacking resources that are available online?*

7.2 Conclusions of Each Research Sub-Question

7.2.1 Addressing Research Sub-Question One: Are People More Likely to Engage in Illicit Activities Online Compared to in the Physical World?

The first research question was addressed through the literature review. Existing research into behaviour online was reviewed and assessed to determine if people are more likely to engage in illicit behaviour online. Suler's (2004) *online disinhibition effect* is a notable theory in this field dictating the lowering of behavioural inhibitions online. Both benign and toxic disinhibition can occur as a result of a number of factors (toxic disinhibition being the phenomenon that would lead to increased likelihood to engage in illicit activities). They are not exclusive, i.e. displaying benign disinhibition does not prevent a person from also displaying toxic disinhibition. There are a number of factors and theories of behaviour that can contribute to this toxic disinhibition such as the interaction between the internet, and social influence, containment theory, and deterrence theory (Fishbein & Ajzen, 1975; Reckless, 1961; Wu, Lin, & Shih, 2017). It has also been concluded through research that there in insufficient deterrence in cyberspace which is conducive to cybercrime (Carlin, 2015; Goldman & McCoy, 2016; Wilson, Sobesto, & Cukier, 2015). These findings allow the conclusion of an affirmative answer to the first research sub-question; People are more likely to engage in illicit activities online than they are in the physical world.

7.2.2 Addressing Research Sub-Question Two: Are Cybercrimes Perceived as Being Less Serious than Non-Cybercrimes?

While some research into perceptions of crime has been carried out, there has been very little research on perceptions of cybercrime. A survey was created based upon previous research carried out by Paulin *et al.* (2003) on perceptions of crime. The previous research had not contained any cybercrimes, so three of the six crime scenarios used in the research were discarded and replaced with three real cybercrime scenarios. The Cybercrime Survey asked participants to decide on rankings and sentences for the six crime scenarios, and then to make a judgement on the actual sentence the crime received to allow verification of the initial responses. The results were assessed by pairing up a cybercrime and a non-cybercrime of best equivalence and comparing the results. The crimes lined up reasonably well with the exception of the credit card theft scenario (27 years) and the domestic abuse scenario (6 months' probation), however, it was deemed acceptable to pair these for comparison given that domestic abuse had been ranked by participants as the more serious crime by a considerable margin. All pairings and results were consistent with an affirmative answer to the research question: Cybercrimes are perceived as being less serious than non-cybercrimes.

7.2.3 Addressing Research Sub-Question Three: Are People Aware of the Type of Free Hacking Resources that are Available Online?

In order to address this question, a selection of free hacking tools, and hacking courses were assessed based on a number of factors. This assessment confirmed the presence of such resources, and provided information about them to contribute to the survey. The confirmation of the presence of the resources by itself is a factor for usage by malicious actors, however, the research sub-question was defined to look at awareness of these resources, as the likelihood of usage by malicious actors, particularly those of the script kiddie variation, increases if they are generally aware of the existence of such resources, rather than merely happening across them online by chance, i.e. it's a lot easier to find something if you know what you are looking for and you know it exists.

The results of the Cybercrime Survey with regards to this stream of research indicates that people are generally aware of the type of tools that are available. The majority of the sample gave a false positive response to two of the fake tools which could be as a result of one of two factors;

(1) As discussed in the previous chapter, it is possible that some participants misinterpreted the tool descriptions, or

(2) Some participants may simply be of the opinion that "Anything is possible" when it comes to cybercrime. This could be as a result of a lack of familiarity with computer related technologies and would be consistent with the considerable proportion of survey participants that placed themselves in any of the categories less than "I don't work in IT but am familiar with computer related technologies" (i.e. less 'tech savvy').

The question on the availability of hacking courses online indicated that people are of the opinion that these courses should not be available online, the matter of which will be discussed further in the "Future Work" section below. The results and conclusions from the hacking resources assessment and survey section indicate an affirmative answer to the research sub-question; People are aware of the type of hacking resources that are available online.

7.3 Conclusions of Main Research Question

The results from the research into the three research sub-questions indicate that the main research question can also be answered affirmatively; the nature of behaviour online and the landscape of the world-wide web combined with current attitudes towards cybercrime create an environment that encourages people to more readily engage in criminal activities online.

An observation during research for the survey that is particularly relevant to this conclusion is a quote from Andrew Helton – the perpetrator behind the phishing scam scenario that was used in the Cybercrime Survey:

> *"There was no expertise involved. All I did was essentially copy and paste. "*
>
> *- Andrew Helton (LA Times, 2016)*

This highlights exactly the type of scenario that this research is mainly focused on – it is now possible for individuals of low technical skill to engage in cybercrime through the use of freely available tools.

It would be easy to place the blame in this situation with the growth of ethical hacking as this is the direct cause of the propagation of free hacking resources online. However, this industry developed and expanded in response to the increasing rate of cybercrime occurrence, out of a need to increase the knowledge and preparedness of organisations required to defend themselves against such attacks. There is an ethos of open-ness and sharing of information in the ethical hacking community exemplified by the well-known not-for–profit organisation OWASP, wherein their goal is to make software security visible through the sharing of tools and information (OWASP, n.d.). As mentioned by all of the cybersecurity experts consulted in this research, these resources are central to the continued improved performance of ethical hackers, and without them, it is possible that this could cause a considerable decline in the performance of the ethical hacking industry overall, resulting in a further increase in cybercrime rates.

7.4 Future Work

Further research into this area is recommended. One possible avenue of research could focus on empirical research around behaviour online. This is an important aspect of the problem and further research is required. Survey research on this matter would not be sufficient as people are less likely to be honest, or sometimes aware of it, if they are asked about their propensities or past activities in relation to illicit behaviour. This research also focused only on free resources. There are undoubtedly also paid resources that are used by malicious actors. These could be assessed as they were not addressed at all within the current study.

7.4.1 Recommendations for Hacking Resources

With the regards to the usage of hacking resources there are a number of possible suggestions:

- Companies such as Offensive Security (Kali Linux) that distribute free hacking software should add features for future distribution that tracks who downloads and installs it, through requiring registration for download and the recording of IP addresses.

- Another possible feature that could be added to the distribution of software is that people are asked to provide the IP addresses of targets the tools will be used to attack. Confirmation will be required from the target. Any recorded attempts to attack targets not disclosed will be treated as an illegal attack and could result in legal action.
- Online hacking courses should be treated like locksmith courses, with established regulations and legislation that require that people provide ID in order to take the courses.

These solutions might help to reduce the malicious usage of hacking resources.

7.4.2 Recommendations for Attitudes to Cybercrime

There are also some possible solutions around dealing with cybercrime and attitudes to it:

- There should be government developed awareness programmes, including TV, radio, internet ads, etc. on the impact of cybercrime which could include testimonials from victims and short case studies that outline some high profile cases.
- Parents need to be made aware of how easily their children can become script kiddies, and generally parents need to educate their children that their activities online have real consequences for real people. E.g. similar to cyberbullying campaigns.
- As suggested by some of the survey responses and the feedback from the cybersecurity experts, an increased onus on the owner of public systems and infrastructures to ensure their security could reduce the general levels of vulnerability to cybercrime. E.g. if organisations were also punished (in addition to the attacker being punished) for failing to secure their systems, they might be more proactive about patching which would make it less likely that script kiddies would be able to find vulnerable targets.
- Alternative penalties could be introduced for cybercrime, such as banning them from using computers, or making them work for free for the victims of their crimes.

7.4.3 Recommendations for Future Research

With the regards to new research directions there are a number of possible suggestions:

- The survey could be redeployed, but systematically only selecting distinct audiences, e.g. a group could do the survey who are I.T. professionals with a lot of experience with computer security issues, and a group of solicitors and judges, and a group of secondary school students aged 12-17. The contrast in answers might be informative
- An exploration of the legislation and legal precedents that exist in the area of cybercrime in Ireland might be very instructive in terms of how it differs from legislation and legal precedents that concern non-cybercrime.
- A different survey that compared the cyber and the real world in a different way could provide some useful results, i.e. a survey that didn’t look at cybercrime and non-cybercrime, but instead looked at on-line shopping and non-on-line shopping, or on-line banking and non-on-line banking, or on-line dating and non-on-line dating.

7.5 Final Thoughts

This research has highlighted that behaviour on the internet and the current landscape of the internet combined with attitudes towards cybercrime create an environment conducive to an increased likelihood to engage in criminal activities online. A number of possible features/solutions have been recommended that could contribute to the reduction in this matter. Nonetheless, this research has highlighted that further research and/or action is required on this matter.

8 BIBLIOGRAPHY

Abraham, S., & Chengular-Smith, I. (2010). An Overview of Social Engineering Malware: Trends, Tactics and Implications. *Technology in Society*, 183-196.

Aiken, M., McMahon, C., Haughton, C., O'Neill, L., & O'Carroll, E. (2015). A Consideration of the Social Impact of Cybercrime: Examples from Hacking, Piracy and Child Abuse Material Online. *Contemporary Social Science*.

Al Shehhi, A., Oudah, M., & Aung, Z. (2014). Investigating Factors Behind Choosing a Cryptocurrency. *IEEE International Conference on Industrial Engineering and Engineering Management* (pp. 1443-1447). IEEE.

Ali, A., Murthy, R., & Kohun, F. (2016). Recovering From the Nightmare of Ransomware - How Savvy Users Get Hit with Viruses and Malware: A Personal Case Study. *Issues in Information Systems*, 58-69.

Alonzon, M., & Aiken, M. (2004). Flaming in Electronic Communications. *Decision Support Systems*, 205-213.

ARS Technica. (2017). *An NSA Derived Ransomware Worm is Shutting Down Computers Worldwide*. Retrieved June 30, 2017, from ARS Technica: https://arstechnica.com/security/2017/05/an-nsa-derived-ransomware-worm-is-shutting-down-computers-worldwide/?comments=1

Banu, N., & Banu, S. M. (2013). A Comprehensive Study of Phishing Attacks. *International Journal of Computer Science and Information Technologies*, 783-786.

Berkowitz, A. D. (2004). *An Overview of the Social Norms Approach.* Cresskill, NJ: Hampton Press.

Bjerg, O. (2015). How is Bitcoin Money? *Theory, Culture and Society*, 53-72.

BlockGeeks. (2017). *What is Cryptocurrency: Everything You Need to Know [Ultimate Guide]*. Retrieved from BlockGeeks: https://blockgeeks.com/guides/what-is-cryptocurrency/

Brodsky, S. L., & O'Neal Smitherman, H. (1983). *Handbook Of Scales for Research in Crime and Delinquacy.* New York: Plenum.

Carlin, J. P. (2015). Detect, Disrupt, Deter: A Whole-Government Approach to National Security Cyber Threats. *Hav. Nat'l Sec. J. 7*, 391.

Chandrika, V. (2014). Ethical Hacking:Types of Ethical Hackers. *Internation Journal of Emerging Technology in Computer Science and Electronics (IJETSCE)*, 44-48.

Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M., & Weimann, G. (2008). Uncovering the Dark Web: A Case Study of Jihad on the Web. *Journal of the American Society for Information Sciences and Technology*, 1347-1359.

Chesney, T., Coyne, I., B., L., & Madden, N. (2009). Griefing in Virtual Worlds: Causes, Casualties and Coping Strategies. *Information Systems Journal*, 525-548.

Cole, J. (2016). Dark Web 101. *Air Force Air Command and Staff College Maxwell AFB United States*.

Curbelo, A. M., & Cruz, A. (2013). Faculty Attitudes Towards Teaching Ethical Hacking to Computer and Information Systems Undergraduate Students. *Proceedings of the Eleventh LACCEI Latin American and Caribbean Conference for Engineering and Technology*. 2013.

CyberScoop. (2017). *Leaked NSA Tools, Now Infecting Over 200,000 Machines, Will be Weaponized for Years*. Retrieved June 30, 2017, from CyberScoop: https://www.cyberscoop.com/leaked-nsa-tools-now-infecting-over-200000-machines-will-be-weaponized-for-years/

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why Phishing Works. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 581-590). ACM.

Diamond, B., & Bachmann, M. (2015). Out of the Beta Phase: Obstacles, Challenges, and Promising Paths in the Study of Cyber Criminology. *International Journal of Cyber Criminology*, 24-34.

Dimkov, T., Pieters, W., & Hartel, P. (2011). Training Students to Steal: A Practical Assignment in Computer Security Education. *Proceedings of the 42nd ACM Technical Symposium on Computer Science Education* (pp. 21-26). ACM.

Dodd, D. K. (1985). Robbers in the Classroom: A Deindividuation Exercise. *Teaching of Psychology*, 89-91.

Douglas, D., Santanna, J. J., de Oliveira Schmidt, R., Granville, L. Z., & Pras, A. (2017). Booters: Can Anything Justify Distributed Denial Of Service (DDos) Attacks for Hire? *Journal of Information, Communication and Ethics in Society*, 90-104.

edgescan™. (2016). *2106 Vulnerability Statistics Report.* edgescan™.

Ekawade, S., & Mule Snehal, P. U. (2016). Phishing Attacks and it's Preventions. *Imperial Journal of Interdiscliplinary Research*, 1766-1769.

Engadget. (2017). *'Shadow Brokers' Dump of NSA Tools Includes New Windows Exploits (Updated)*. Retrieved June 30, 2017, from Engadget:

https://www.engadget.com/2017/04/14/shadow-brokers-dump-windows-zero-day/

FIRST. (n.d.). *Common Vulnerability Scoring System v3.0: Specification Document*. Retrieved June 25, 2017, from https://www.first.org/cvss/specification-document

Fishbein, M., & Ajzen, I. (1975). *Belief Attitude, Intention and Behaviour.* Reading MA: Addison-Wesley.

Fuchs, C. (2014). Hacktivism and Contemporary Politics. In C. Fuchs, *Social Media, Policitics adn the State: Protests, Revolutions, Riots, Crime and Policing in the Age of Facebook, Twitter and Youtube* (pp. 88-106). New York.

Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the Security Perceptions of Personal Internet Users. *Computers & Security*, 410-417.

Garera, S., Provos, N., Chew, M., & Rubin, A. D. (2007). A Framework for Detection and Measurement of Phishing Attacks. *Proceedings of the 2007 ACM Workshop on Recurring Malcode* (pp. 1-8). ACM.

Gibbons, D. C., Jones, J. F., & Garabedian, P. G. (1972). Gauging Public Opinion about the Crime Problem. *Crime and Delinquency*, 134-146.

Goldman, Z. K., & McCoy, D. (2016). Economic Espionage: Deterring Financially Motivated Cybercrime. *J. Nat'l Security L. & Pol'y*, 595-621.

Gordon, S., & Ford, R. (2006). On the Definition and Classification of Cybercrime. *Journal in Computer Virology*, 13-20.

Graphic News. (2017). *Global Impact of WannaCry Cyber Attack.* Retrieved May 26, 2017, from https://www.graphicnews.com/en/pages/35387/CRIME-Global-impact-of-WannaCry-cyber-attack

Hampson, N. (2012). Hacktivism, Anonymous & a New Breed of Protest in a Networked World. *Boston College International and Comparative Law Review*, 511-542.

Haney, C., Banks, C., & Zimbardo, P. (1972). Interpersonal Dynamics in a Simulated Prison. *Stanford University CA Dept of Psychology*.

Hendrick, T. A., Fischer, A. R., Tobi, H., & Frewer, L. J. (2013). Self-reported Attitude Scales: Current Practice in Adequate Assessment of Reliability, Valididty and Dimensionality. *Journal of Applied Social Psychology*, 1538-1552.

Hoerger, M. (2010). Participant Dropout as a Function of Survey Length in Internet-Mediated University Studies: Implications for Study Design and Voluntary

Participation in Pyschological Research. *CyberPsychology, Behaviour and Social Networking*, 697-700.

Hollenbaugh, E. E., & Everett, M. K. (2013). The Effects of Anonymity on Self-Disclosure in Blogs: An Application of the Online Disinhibition Effect. *Journal of Computer-Mediated Communication*, 283-302.

Holtfreter, K., van Slyke, S., Bratton, J., & Gertz, M. (2008). Public Perceptions of White Collar Crime and Punishment. *Journal of Criminal Justice*, 50-60.

IC3. (2003). *IC3 2003 Internet Fraud Report.* IC3.

IC3. (2016). *2016 Internet Crime Report.* IC3.

InfoSec Institute. (2011, October 24). *A History of Anonymous*. Retrieved from InfoSec Institute: http://resources.infosecinstitute.com/a-history-of-anonymous/#gref

Interpol. (n.d.). *Cybercrime*. Retrieved May 15, 2017, from https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

Jaishankar, K. (2008). Space Transition Theory. In F. Schmallager, & P. M. (Eds.), *Crimes of the Internet* (pp. 283-301). Upper Saddle River, NJ: Prentice Hall.

Jamil, D., & Khan, M. N. (2011). Is Ethical Hacking Ethical. *International Journal of Engineering Science and Technology*, 3758-3763.

Joinson, A. N. (2007). Disinhibition and the Internet. In J. Gackenbach, *Psychology and the Internet: Interpersonal, Interpersonal and Transpersonal Implications, 2nd ed* (pp. 75-92). San Diego CA: Academic Press.

Kiesler, S., & Sproull, L. (1992). Group Decision Making and Communication Technology. *Organizational Behaviour and Human Decision Processes*, 96-123.

Krebs, B. (2014, September 06). *Dread Pirate Sunk by Leaky CAPTCHA.* Retrieved from Krebs On Security: https://krebsonsecurity.com/2014/09/dread-pirate-sunk-by-leaky-captcha/

Krebs, B. (2017, April 04). *Dual Use Software Criminal Case Not so Novel*. Retrieved from Krebs On Security: https://krebsonsecurity.com/2017/04/dual-use-software-criminal-case-not-so-novel/

LA Times. (2016). *Man gets Six Months in Prison for Hacking Hundreds of email Accounts, Including Those of Celebrities*. Retrieved June 30, 2017, from Los Angeles Times: http://www.latimes.com/local/lanow/la-me-ln-hacking-prison-sentence-celebrities-email-20160721-snap-story.html

Lacson, W., & Jones, B. (2016). The 21st Century DarkNet Market: Lessons from the Fall of Silk Road. *Internation Journal of Cyber Criminology*, 40-61.

Landreth, B. (1985). Out of the Inner Circle: A Hacker's Guide to Computer Security. *Microsoft Press*.

Lapidot-Lefler, N., & Barak, A. (2012). Effects of Anonymity, Invisibility and Lack of Eye Contact on Online Disinhibition. *Computers in Human Behaviour*, 434-443.

Le Bon, G. (1896). *The Crowd: A Study of the Popular Mind.* New York: MacMillan & Co.

Leukfeldt, R., Veenstra, S., & Stol, W. (2013). High Volume Cyber Crime and the Organization of the Police: The Results of Two Empirical Studies in the Netherlands. *Internation Journal of Cyber Criminology*, 1-17.

Liaw, S.-S. (2002). An Internet Survey for Perceptions of Computers and the World Wide Web: Relationship, Prediction and Difference. *Computers in Human Behaviour*, 17-35.

Livermore, J. (2007). What are Faculty Attitudes Toward Teaching Ethical Hacking and Penetration Testing. *Proceedings of the 11th Colloquium for Information Systems Security Education,* (pp. 111-116). Boston.

Logan, P., & Clarkson, A. (2004). Is it Safe? Information Security Education: Are We Teaching a Dangerous Subject? *Proceedings of the 8th Colloquium for Information Systems Security Education*, (pp. 65-70). West Point, NY.

Logan, P., & Clarkson, A. (2005). Teaching Students to Hack: Curriculum Issues in Information Security. *ACM SIGCSE Bulletin, 37*(1), pp. 157-161.

Meinert, M. C. (2016). Social Engineering: The Art of Human Hacking. *ABA Banking Journal*.

Meyers, C., Powers, S., & Faissol, D. (2009). *Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches.* Lawrence Livermore National Laboratory.

Michel, C. (2016). Violent Street Crime versus Harmful White Collar Crime: A Comparison of Perceived Seriousness and Punitiveness. *Critical Criminology*, 127-143.

Milgram, S. (1963). Behavioural Study of Obedience. *The Journal of Abnormal and Social Psychology*, 371.

Morse, B. J., Gullekson, N. L., Moris, S. A., & Popovich, P. M. (2011). The Development of a General Internet Attitudes Scale. *Computers in Humnan Behaviour*, 480-489.

Mukhopadhyay, U., Skjellum, A., Hambolu, O., Oakley, J., Yu, L., & Brooks, R. (2016). A Brief Survey of Cryptocurrency Systems. *14th Annual Conference on Privacy, Security and Trust (PST)* (pp. 745-752). IEEE.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer Electronic Cash System.

Ngafeeson, M. (2010). Cybercrime Classification: A Motivational Model. *Proceedings of Southwest Decision Sciences Institute Conference.*

Ngo, F., & Jaishankar, K. (2017). Commemorating a Decade in the Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship of Cyber Crime. *International Journal of Cyber Criminology*.

Nguyen, Q. K. (2016). Blockchain - A Financial Technology for Future Sustainable Development. *2016 3rd International Conference on Green Technology and Sustainable Development (GTSD)* (pp. 51-54). IEEE.

Olsen, P. (2013). *We Are Anonymous.* Random House.

OWASP. (n.d.). *Welcome to OWASP*. Retrieved June 30, 2017, from OWASP: https://www.owasp.org/index.php/Main_Page

Palmer, C. C. (2001). Ethical Hacking. *IBM Systems Journal*, 769-780.

Pashel, B. A. (2006). Teaching Students to Hack: Ethical Implications in Teaching Students to Hack at the University Level. *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development* (pp. 197-200). ACM.

Pathak, P. B. (2016). A Dangerous Trend of Cybercrime: Ransomware Growing Challenge. *International Journal of Avanced Research in Computer Engineering & Technology*, 372-373.

Paulin, J., Searle, W., & Knaggs, T. (2003). *Attitudes to Crime and Punishment.* Wellington, New Zealand: Ministry of Justice.

Poonia, A. S. (2014). CyberCrime: Challenges and Classification. *International Journal of Emerging Trends & Technology in Computer Science*, 119-121.

Postmes, T. (1998). Deindividuation and Antinormative Behaviour. *Psychological Bulletin*, 238-259.

Poteat, V. E. (2005). Classroom Ethics: Hacking and Cracking. *Journal of Computing Sciences in Colleges*, 225-231.

Pras, A., Speretto, A., Moura, G., Drago, I., Barbosa, R., Sadre, R., . . . Hofstede, R. (2010). Attacks by “Anonymous” WikiLeaks Proponents Not Anonymous. *University of Twente, Centre for Telematics and Information Technology (CTIT).*

Prendergrass, W. S. (2013). What is Anonymous? A Case Study of an Information Systems Hacker Activist Collective Movement. *Diss. Robert Morris University*.

Prewitt, M. F., & Callahan, M. W. (2017). Jurisdiction in the Information Age. In I. I. Education, *Intellectual Property Law 2017 Edition* (pp. 16-1 - 16-25).

PWC. (2016). *Global Economic Crime Survey 2016.* PWC.

Raconteur. (2017). *WannaCry: The Biggest Ransomware Attack in History*. Retrieved May 25, 2017, from https://www.raconteur.net/infographics/wannacry-the-biggest-ransomware-attack-in-history

RAND Corporation. (2016). *The Role of the 'Dark Web' in the Trade of Illicit Drugs.* Retrieved April 28, 2017, from http://www.rand.org/pubs/research_briefs/RB9925.html

Raymond, E. (1996). *The New Hacker's Dictionary.* MIT Press.

Reckless, W. C. (1961). A New Theory of Delinquency and Crime. *Federal Probation*, 42-46.

Reckless, W. C. (1973). *The Crime Problem, 5th Ed.* Englewood Cliffs, NJ: Prentice-Hall.

Reicher, S. D., Spears, R., & Postmes, T. (1995). A Social Idenetity Model of Deindividuation. *European Review of Social Psychology*, 161-198.

Reinig, B. A., Briggs, R. O., & Nunamaker, J. F. (1998). Flaming in the Electronic Classroom. *Journal of Personlity and Social Psychology*, 45-59.

Richardson, R., & North, M. (2017). Ransomware: Evolution, Mitigation and Prevention. *International Management Review*, 11-21.

Rogers, M. K. (2006). A Two Dimensional Circumplex Approach to the Development of a Hacker Taxonomy. *Digital Investigation*, 97-102.

Rogers, M. K. (2011). The Psyche of Cybercriminals: A Psycho-Social Perspective. *Cybercrimes: A Mutlidisciplinary Analysis* (pp. 217-235). Berlin Heidelberg: Springer .

Rossi, P. H., Waite, E., Bose, C. E., & Berk, R. E. (1974). The Seriousness of Crimes: Normative Structure and Individual Differences. *American Sociological Review*, 224-237.

Sagargholap101. (2014, April 28). *Introduction to 'Deep Web'*. Retrieved June 22, 2016, from GetSoftwareHelp24X7: https://getsoftwarehelp24x7.wordpress.com/2014/04/28/introduction-to-deep-web/

Saleem, S. A. (2006). Ethical Hacking as a Risk Management Technique. *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development* (pp. 201-203). ACM.

Salvi, H. U., & Kerkar, R. V. (2016). Ransomware: A Cyber Extortion. *Asian Journal of Convergence in Technology*.

Scaife, N., Carter, H., Traynor, P., & Butler, K. R. (2016). CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. *IEEE 36th Internation Conference on Distributed Computing Systems* (pp. 303-312). IEEE.

Seebruck, R. (2015). A Typology of Hackers: Classifying Cyber Malfeasance Using a Weighted Arc Circumplex Model. *Digital Investigation*, 36-45.

Serracino-Inglott, P. (2013). Is it OK to be an Anonyomous? *Ethics & Global Politics*.

Sherman, R. C., & Dowdle, M. D. (1974). The Perception of Crime and Punishment: A Multidimensional Scaling Analysis. *Social Science Research*, 109-126.

Silke, A. (2003). Deindividuation, Anonymity and Violence: Findings from Northern Ireland. *The Journal of Social Psychology*, 493-499.

Simmonds, A., Sandilands, P., & van Ekert, L. (2004). An Ontology for Network Security Attacks. *Asian Applied Computing Conference* (pp. 317-323). Springer Berline Heidelberg.

Spears, R., Lea, M., Corneliussen, R.-A., Postmes, T., & Haar, W. T. (2002). Computer-Mediated Communication as a Channel for Social Resistance: The Strategic Side of SIDE. *Small Group Research*, 555-574.

Stajano, F., & Paul, W. (2011). Understanding Scam Victims: Seven Principles for Systems Security. *Communications of the ACM*, 70-75.

Staub, E. (1996). Cultural-Societal Roots of Violence: The Examples of Genocidal Violence and of Contemporary Youth Violence in the United States. *American Psychologist*, 117.

Stryker, C. (2011). *Epic Win for Anonymous: How 4chan's Army Conquered the Web.* The Overlook Press.

Suler, J. (2004). The Online Disinhibition Effect. *Cyberpsychology and Behaviour*, 321-326.

The Daily Beast. (2017, March 31). *FBI Arrests Hacker who Hacked No One*. Retrieved May 2, 2017, from http://www.thedailybeast.com/fbi-arrests-hacker-who-hacked-no-one

The Daily Mail. (2015). *ISIS dismiss Anonymous hackers as 'idiots' for threatening to shut down their Twitter accounts… when they can just open new ones*. Retrieved May 23, 2017, from http://www.dailymail.co.uk/news/article-3326912/ISIS-dismiss-Anonymous-hackers-idiots-threatening-shut-Twitter-accounts-just-open-new-ones.html

The Jargon File (4.4.7). (2003). *The Jargon File (4.4.7)*. Retrieved April 15, 2017, from http://www.catb.org/jargon/html/index.html

The New York Times. (2016, 2016). *'Shadow Brokers' Leak Raises Alarming Question: Was the NSA Hacked?* Retrieved June 30, 2017, from The New York Times: https://www.nytimes.com/2016/08/17/us/shadow-brokers-leak-raises-alarming-question-was-the-nsa-hacked.html

The United States Department of Justice. (2016). *Oregon Man Sentenced to Prison for Hacking into Hundreds of E-Mail Accounts and Stealing Personal Photos Belonging to Victims*. Retrieved May 5, 2017, from https://www.justice.gov/usao-cdca/pr/oregon-man-sentenced-prison-hacking-hundreds-e-mail-accounts-and-stealing-personal

The United States Department of Justice. (2017a). *Winchester Man Sentenced To 24 Months For Illegally Hacking Into Website And Lying To Federal Agents*. Retrieved May 5, 2017, from https://www.justice.gov/usao-edky/pr/winchester-man-sentenced-24-months-illegally-hacking-website-and-lying-federal-agents

The United States Department of Justice. (2017b). *Russian Cyber-Criminal Sentenced to 27 Years in Prison for Hacking and Credit Card Fraud Scheme*. Retrieved May 5, 2017, from https://www.justice.gov/opa/pr/russian-cyber-criminal-sentenced-27-years-prison-hacking-and-credit-card-fraud-scheme

Thompson, W. E., & Dodder, R. A. (1983). Juvenile Delinquency Explained? A Test of Containment Theory. *Youth & Society*, 171-194.

Tsai, C.-C., Lin, S. S., & Tsai, M.-J. (2001). Developing an Internet Attitude Scale for High School Students. *Computers and Education*, 41-51.

Udris, R. (2014). Cyberbullying Among High School Students in Japan: Development and Validation of the Online Disinhibition Scale. *Computers in Human Behaviour*, 253-261.

United States of America v. Taylor Huddleston. (2017). Retrieved from Krebs on Security: https://krebsonsecurity.com/wp-content/uploads/2017/04/W.D.Ark_._null_null_0.pdf van der Walt, C. (2017). The Impact of Nation-State Hacking on Commercial Cybersecurity. *Computer Fraud & Security*, 5-10.

Verizon. (2016). *Data Breach Digest.* Verizon.

Vogt, S. D. (2017). The Digital Underworld: Combating Crime on the Dark Web in the Modern Era. *Santa Clara Journal of International Law*, 105-124.

Wilson, T. M., Sobesto, B., & Cukier, M. (2015). The Effect of a Surveillance Banner in an Attacked Computer System: Additional Evidence for the Relevance of Restrictive Deterrence in Cyberspace. *Journal of Research in Crime and Delinquency*, 829-855.

Wired. (2014). *How Thieves Can Hack and Disable Your Home Alarm System*. Retrieved June 15, 2017, from Wired: https://www.wired.com/2014/07/hacking-home-alarms/

Wired. (2017). *A Scary New Ransomware Outbreak Uses WannaCry's Old Tricks*. Retrieved June 30, 2017, from Wired: https://www.wired.com/story/petya-ransomware-outbreak-eternal-blue/

World Economic Forum. (2016). *All You Need to Know About Blockchain, Explained Simply.* Retrieved May 20, 2017, from https://www.weforum.org/agenda/2016/06/blockchain-explained-simply/

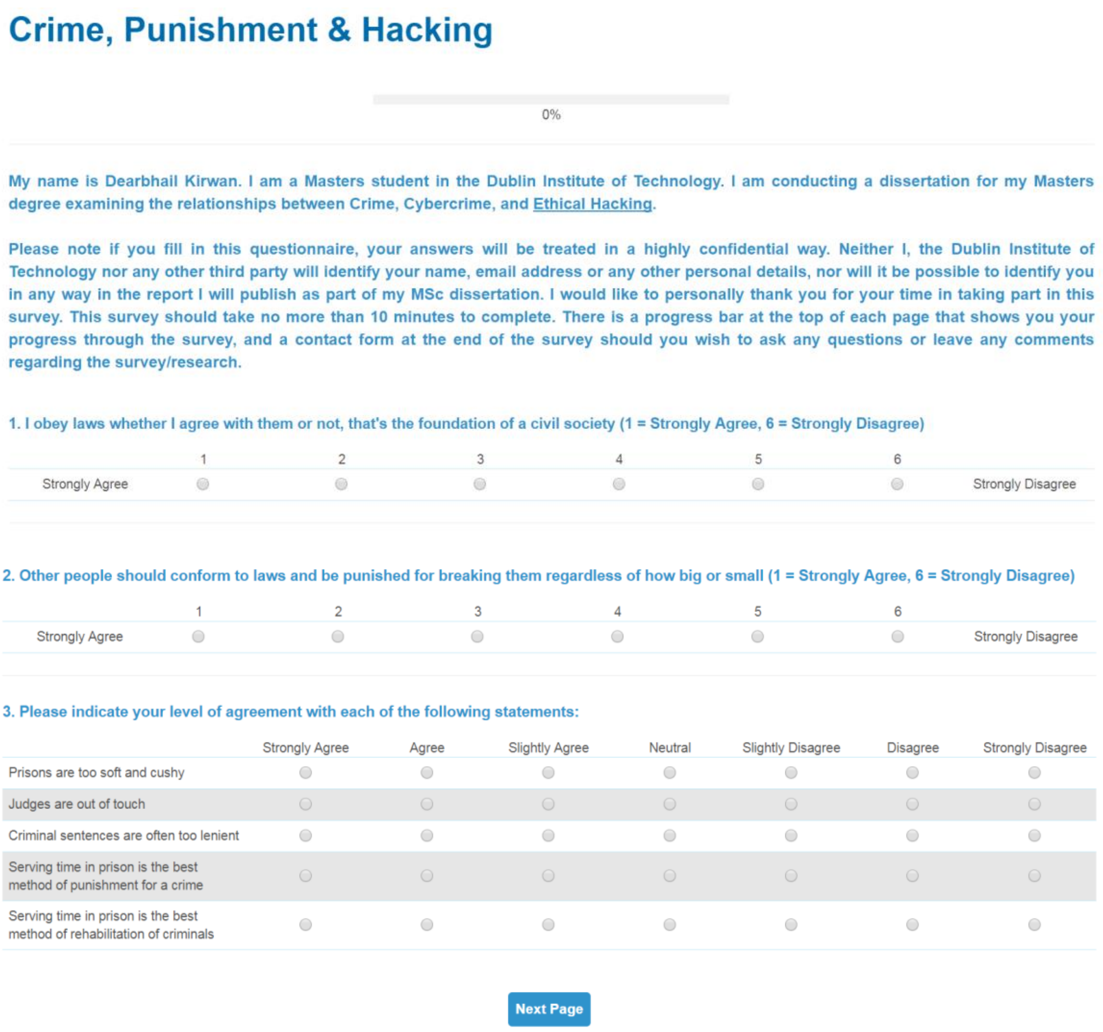
Wu, S., Lin, T.-C., & Shih, J.-F. (2017). Examining the Antecedents of Online Disinhibition . *Information Technology & People*, 189-209.

ZD Net. (2017). *Six Quick Facts to Know About the Petya Global Ransomware Attack*. Retrieved June 30, 2017, from ZD Net: http://www.zdnet.com/article/six-quick-facts-june-global-ransomware-cyberattack/

Zimbardo, P. G. (1969). The Human Choice: Individuation, Reason and Order Versus Deindividuation, Impulse and Chaos. *Nebraska Symposium on Motivation.* University of Nebraska Press.

Zlomislic, V., Fertalj, K., & Sruk, V. (2014). Denial of Service Attacks: An Overview. *Information Systems and Technologies (CISTI)*, 1-6.

APPENDIX A



Crime, Punishment & Hacking

0%

My name is Dearbhail Kirwan. I am a Masters student in the Dublin Institute of Technology. I am conducting a dissertation for my Masters degree examining the relationships between Crime, Cybercrime, and Ethical Hacking.

Please note if you fill in this questionnaire, your answers will be treated in a highly confidential way. Neither I, the Dublin Institute of Technology nor any other third party will identify your name, email address or any other personal details, nor will it be possible to identify you in any way in the report I will publish as part of my MSc dissertation. I would like to personally thank you for your time in taking part in this survey. This survey should take no more than 10 minutes to complete. There is a progress bar at the top of each page that shows you your progress through the survey, and a contact form at the end of the survey should you wish to ask any questions or leave any comments regarding the survey/research.

1. I obey laws whether I agree with them or not, that's the foundation of a civil society (1 = Strongly Agree, 6 = Strongly Disagree)

	1	2	3	4	5	6	
Strongly Agree	○	○	○	○	○	○	Strongly Disagree

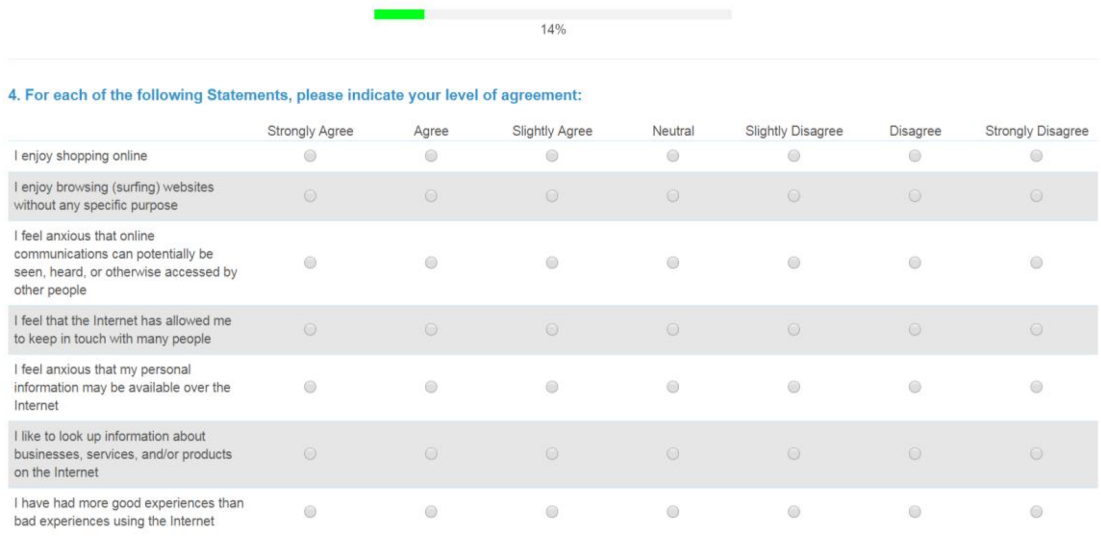
2. Other people should conform to laws and be punished for breaking them regardless of how big or small (1 = Strongly Agree, 6 = Strongly Disagree)

	1	2	3	4	5	6	
Strongly Agree	○	○	○	○	○	○	Strongly Disagree

3. Please indicate your level of agreement with each of the following statements:

	Strongly Agree	Agree	Slightly Agree	Neutral	Slightly Disagree	Disagree	Strongly Disagree
Prisons are too soft and cushy	○	○	○	○	○	○	○
Judges are out of touch	○	○	○	○	○	○	○
Criminal sentences are often too lenient	○	○	○	○	○	○	○
Serving time in prison is the best method of punishment for a crime	○	○	○	○	○	○	○
Serving time in prison is the best method of rehabilitation of criminals	○	○	○	○	○	○	○

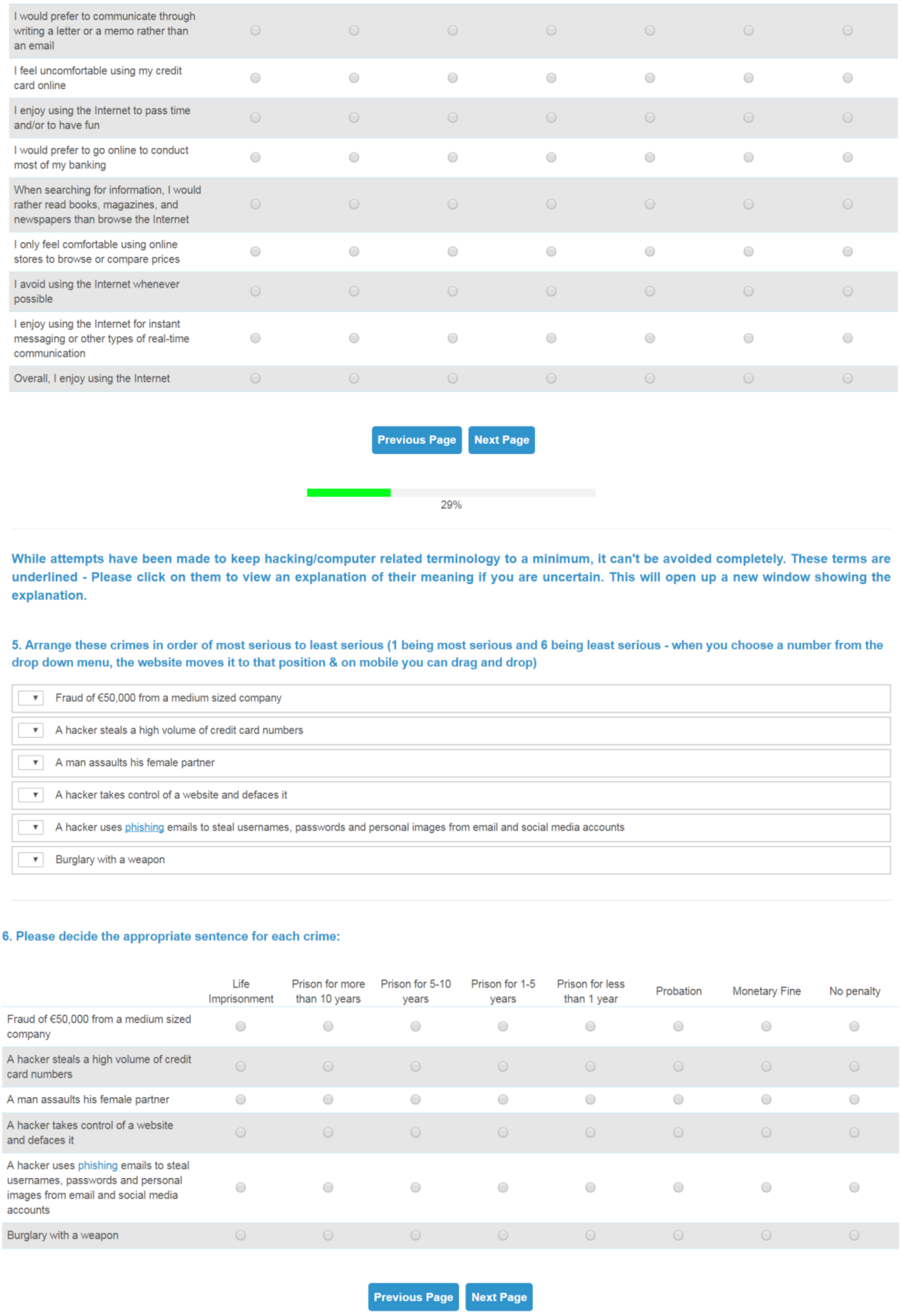
Next Page



14%

4. For each of the following Statements, please indicate your level of agreement:

	Strongly Agree	Agree	Slightly Agree	Neutral	Slightly Disagree	Disagree	Strongly Disagree
I enjoy shopping online	○	○	○	○	○	○	○
I enjoy browsing (surfing) websites without any specific purpose	○	○	○	○	○	○	○
I feel anxious that online communications can potentially be seen, heard, or otherwise accessed by other people	○	○	○	○	○	○	○
I feel that the Internet has allowed me to keep in touch with many people	○	○	○	○	○	○	○
I feel anxious that my personal information may be available over the Internet	○	○	○	○	○	○	○
I like to look up information about businesses, services, and/or products on the Internet	○	○	○	○	○	○	○
I have had more good experiences than bad experiences using the Internet	○	○	○	○	○	○	○



I would prefer to communicate through writing a letter or a memo rather than an email	○	○	○	○	○	○	○
I feel uncomfortable using my credit card online	○	○	○	○	○	○	○
I enjoy using the Internet to pass time and/or to have fun	○	○	○	○	○	○	○
I would prefer to go online to conduct most of my banking	○	○	○	○	○	○	○
When searching for information, I would rather read books, magazines, and newspapers than browse the Internet	○	○	○	○	○	○	○
I only feel comfortable using online stores to browse or compare prices	○	○	○	○	○	○	○
I avoid using the Internet whenever possible	○	○	○	○	○	○	○
I enjoy using the Internet for instant messaging or other types of real-time communication	○	○	○	○	○	○	○
Overall, I enjoy using the Internet	○	○	○	○	○	○	○

While attempts have been made to keep hacking/computer related terminology to a minimum, it can't be avoided completely. These terms are underlined - Please click on them to view an explanation of their meaning if you are uncertain. This will open up a new window showing the explanation.

5. Arrange these crimes in order of most serious to least serious (1 being most serious and 6 being least serious - when you choose a number from the drop down menu, the website moves it to that position & on mobile you can drag and drop)

▾ Fraud of €50,000 from a medium sized company

▾ A hacker steals a high volume of credit card numbers

▾ A man assaults his female partner

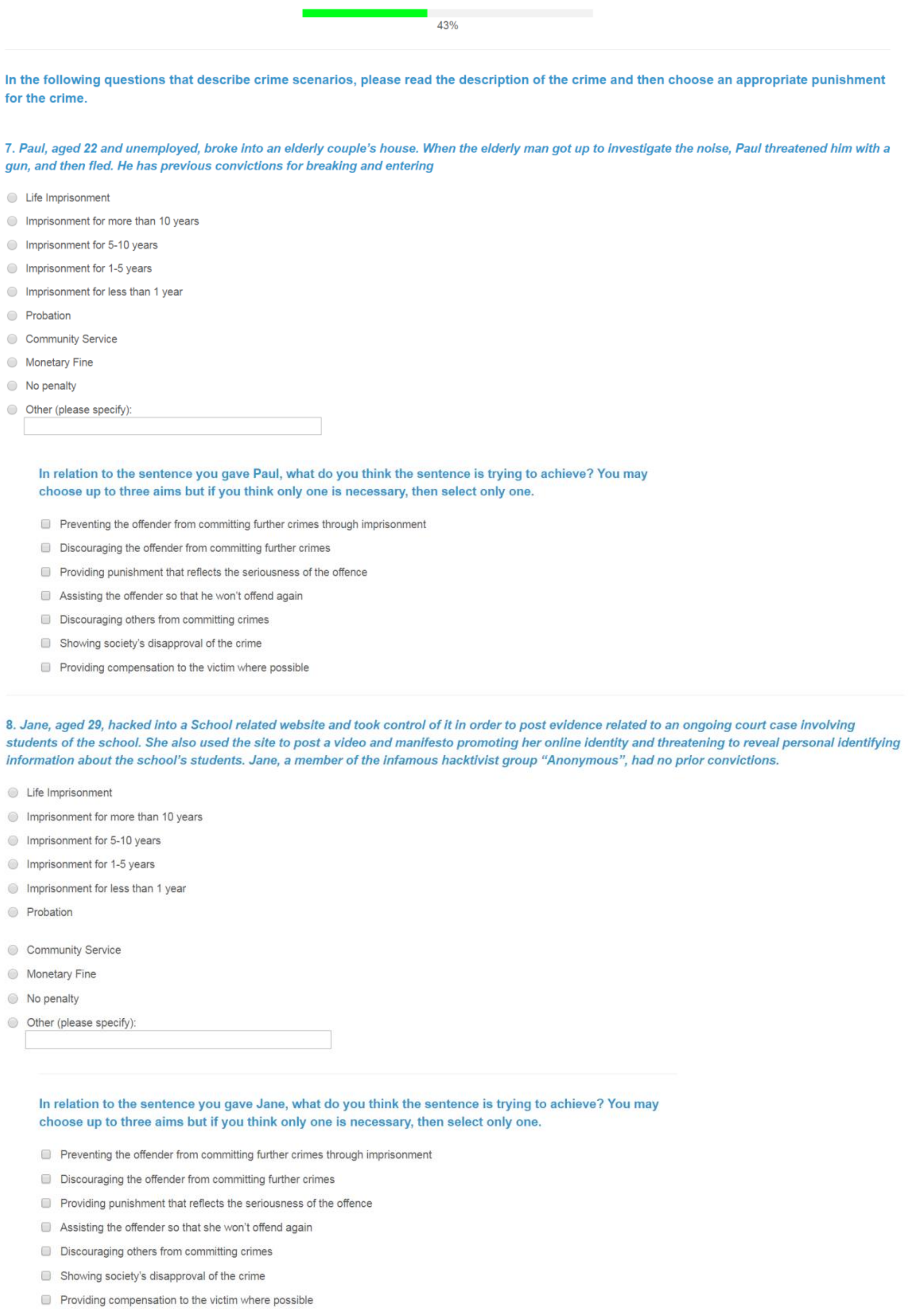
▾ A hacker takes control of a website and defaces it

▾ A hacker uses phishing emails to steal usernames, passwords and personal images from email and social media accounts

▾ Burglary with a weapon

6. Please decide the appropriate sentence for each crime:

	Life Imprisonment	Prison for more than 10 years	Prison for 5-10 years	Prison for 1-5 years	Prison for less than 1 year	Probation	Monetary Fine	No penalty
Fraud of €50,000 from a medium sized company	○	○	○	○	○	○	○	○
A hacker steals a high volume of credit card numbers	○	○	○	○	○	○	○	○
A man assaults his female partner	○	○	○	○	○	○	○	○
A hacker takes control of a website and defaces it	○	○	○	○	○	○	○	○
A hacker uses phishing emails to steal usernames, passwords and personal images from email and social media accounts	○	○	○	○	○	○	○	○
Burglary with a weapon	○	○	○	○	○	○	○	○



43%

In the following questions that describe crime scenarios, please read the description of the crime and then choose an appropriate punishment for the crime.

7. ***Paul, aged 22 and unemployed, broke into an elderly couple's house. When the elderly man got up to investigate the noise, Paul threatened him with a gun, and then fled. He has previous convictions for breaking and entering***

○ Life Imprisonment

○ Imprisonment for more than 10 years

○ Imprisonment for 5-10 years

○ Imprisonment for 1-5 years

○ Imprisonment for less than 1 year

○ Probation

○ Community Service

○ Monetary Fine

○ No penalty

○ Other (please specify):

In relation to the sentence you gave Paul, what do you think the sentence is trying to achieve? You may choose up to three aims but if you think only one is necessary, then select only one.

□ Preventing the offender from committing further crimes through imprisonment

□ Discouraging the offender from committing further crimes

□ Providing punishment that reflects the seriousness of the offence

□ Assisting the offender so that he won't offend again

□ Discouraging others from committing crimes

□ Showing society's disapproval of the crime

□ Providing compensation to the victim where possible

8. ***Jane, aged 29, hacked into a School related website and took control of it in order to post evidence related to an ongoing court case involving students of the school. She also used the site to post a video and manifesto promoting her online identity and threatening to reveal personal identifying information about the school's students. Jane, a member of the infamous hacktivist group "Anonymous", had no prior convictions.***

○ Life Imprisonment

○ Imprisonment for more than 10 years

○ Imprisonment for 5-10 years

○ Imprisonment for 1-5 years

○ Imprisonment for less than 1 year

○ Probation

○ Community Service

○ Monetary Fine

○ No penalty

○ Other (please specify):

In relation to the sentence you gave Jane, what do you think the sentence is trying to achieve? You may choose up to three aims but if you think only one is necessary, then select only one.

□ Preventing the offender from committing further crimes through imprisonment

□ Discouraging the offender from committing further crimes

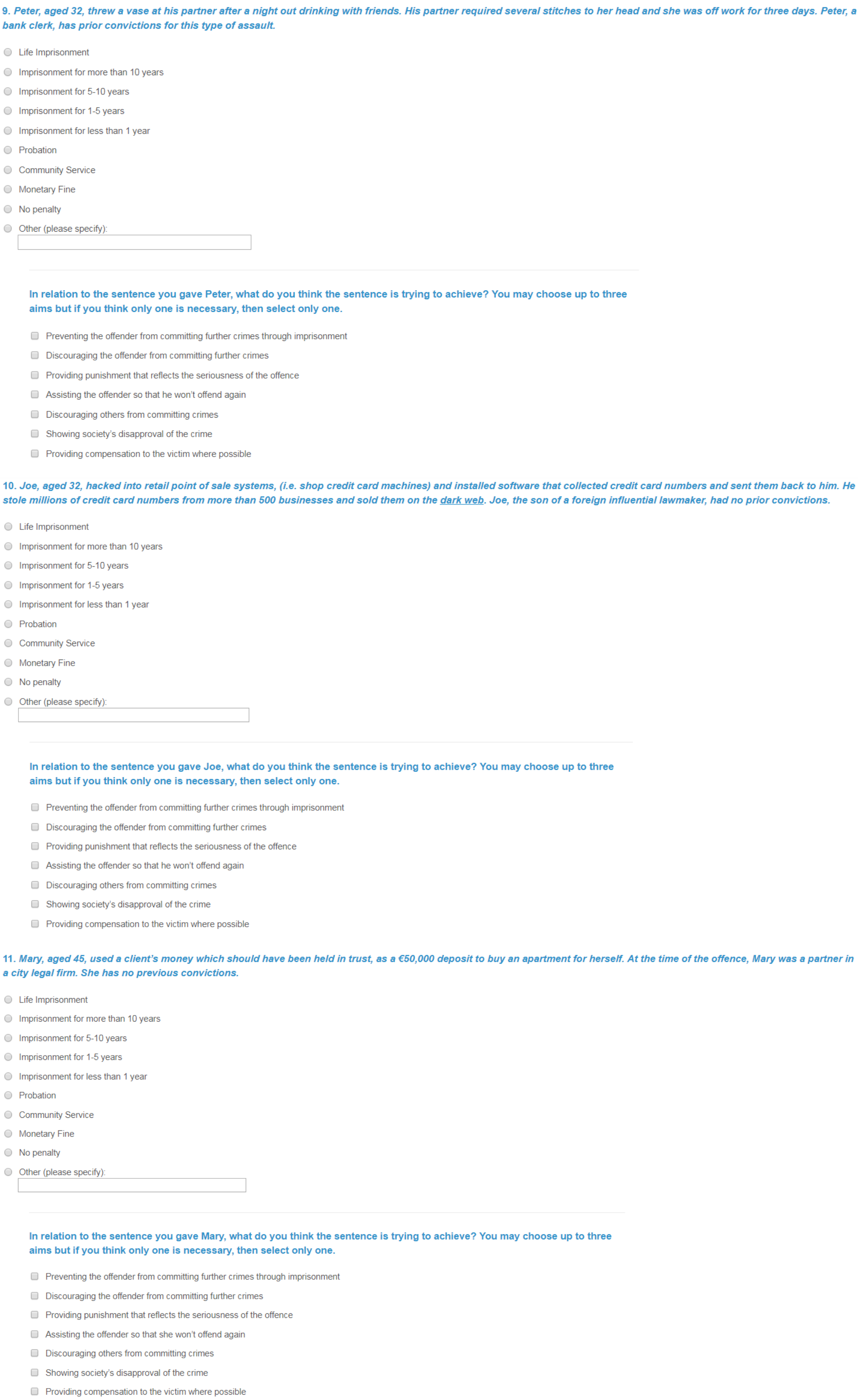
□ Providing punishment that reflects the seriousness of the offence

□ Assisting the offender so that she won't offend again

□ Discouraging others from committing crimes

□ Showing society's disapproval of the crime

□ Providing compensation to the victim where possible



9. Peter, aged 32, threw a vase at his partner after a night out drinking with friends. His partner required several stitches to her head and she was off work for three days. Peter, a bank clerk, has prior convictions for this type of assault.

○ Life Imprisonment
○ Imprisonment for more than 10 years
○ Imprisonment for 5-10 years
○ Imprisonment for 1-5 years
○ Imprisonment for less than 1 year
○ Probation
○ Community Service
○ Monetary Fine
○ No penalty
○ Other (please specify):

In relation to the sentence you gave Peter, what do you think the sentence is trying to achieve? You may choose up to three aims but if you think only one is necessary, then select only one.

□ Preventing the offender from committing further crimes through imprisonment
□ Discouraging the offender from committing further crimes
□ Providing punishment that reflects the seriousness of the offence
□ Assisting the offender so that he won't offend again
□ Discouraging others from committing crimes
□ Showing society's disapproval of the crime
□ Providing compensation to the victim where possible

10. Joe, aged 32, hacked into retail point of sale systems, (i.e. shop credit card machines) and installed software that collected credit card numbers and sent them back to him. He stole millions of credit card numbers from more than 500 businesses and sold them on the dark web. Joe, the son of a foreign influential lawmaker, had no prior convictions.

○ Life Imprisonment
○ Imprisonment for more than 10 years
○ Imprisonment for 5-10 years
○ Imprisonment for 1-5 years
○ Imprisonment for less than 1 year
○ Probation
○ Community Service
○ Monetary Fine
○ No penalty
○ Other (please specify):

In relation to the sentence you gave Joe, what do you think the sentence is trying to achieve? You may choose up to three aims but if you think only one is necessary, then select only one.

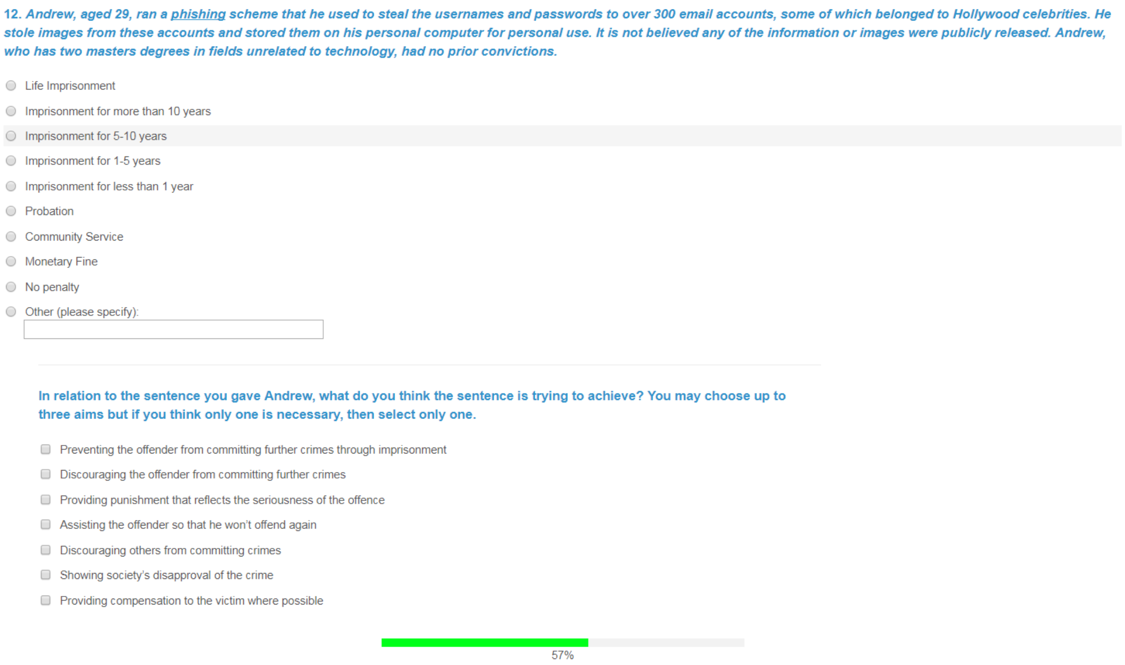
□ Preventing the offender from committing further crimes through imprisonment
□ Discouraging the offender from committing further crimes
□ Providing punishment that reflects the seriousness of the offence
□ Assisting the offender so that he won't offend again
□ Discouraging others from committing crimes
□ Showing society's disapproval of the crime
□ Providing compensation to the victim where possible

11. Mary, aged 45, used a client's money which should have been held in trust, as a €50,000 deposit to buy an apartment for herself. At the time of the offence, Mary was a partner in a city legal firm. She has no previous convictions.

○ Life Imprisonment
○ Imprisonment for more than 10 years
○ Imprisonment for 5-10 years
○ Imprisonment for 1-5 years
○ Imprisonment for less than 1 year
○ Probation
○ Community Service
○ Monetary Fine
○ No penalty
○ Other (please specify):

In relation to the sentence you gave Mary, what do you think the sentence is trying to achieve? You may choose up to three aims but if you think only one is necessary, then select only one.

□ Preventing the offender from committing further crimes through imprisonment
□ Discouraging the offender from committing further crimes
□ Providing punishment that reflects the seriousness of the offence
□ Assisting the offender so that she won't offend again
□ Discouraging others from committing crimes
□ Showing society's disapproval of the crime
□ Providing compensation to the victim where possible



12. Andrew, aged 29, ran a phishing scheme that he used to steal the usernames and passwords to over 300 email accounts, some of which belonged to Hollywood celebrities. He stole images from these accounts and stored them on his personal computer for personal use. It is not believed any of the information or images were publicly released. Andrew, who has two masters degrees in fields unrelated to technology, had no prior convictions.

○ Life Imprisonment

○ Imprisonment for more than 10 years

○ Imprisonment for 5-10 years

○ Imprisonment for 1-5 years

○ Imprisonment for less than 1 year

○ Probation

○ Community Service

○ Monetary Fine

○ No penalty

○ Other (please specify):

In relation to the sentence you gave Andrew, what do you think the sentence is trying to achieve? You may choose up to three aims but if you think only one is necessary, then select only one.

□ Preventing the offender from committing further crimes through imprisonment

□ Discouraging the offender from committing further crimes

□ Providing punishment that reflects the seriousness of the offence

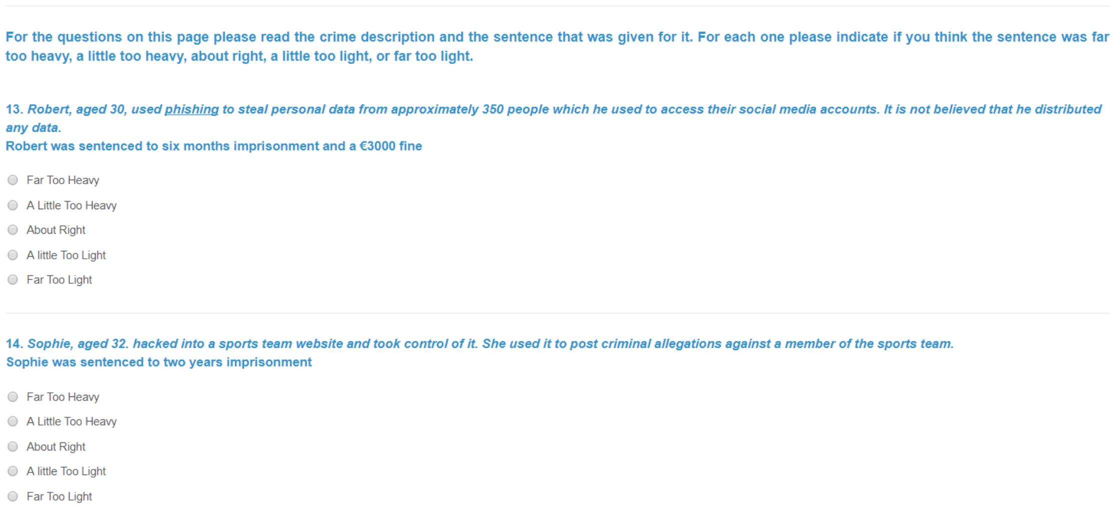
□ Assisting the offender so that he won't offend again

□ Discouraging others from committing crimes

□ Showing society's disapproval of the crime

□ Providing compensation to the victim where possible

57%



For the questions on this page please read the crime description and the sentence that was given for it. For each one please indicate if you think the sentence was far too heavy, a little too heavy, about right, a little too light, or far too light.

13. Robert, aged 30, used phishing to steal personal data from approximately 350 people which he used to access their social media accounts. It is not believed that he distributed any data.
Robert was sentenced to six months imprisonment and a €3000 fine

○ Far Too Heavy

○ A Little Too Heavy

○ About Right

○ A little Too Light

○ Far Too Light

14. Sophie, aged 32. hacked into a sports team website and took control of it. She used it to post criminal allegations against a member of the sports team.
Sophie was sentenced to two years imprisonment

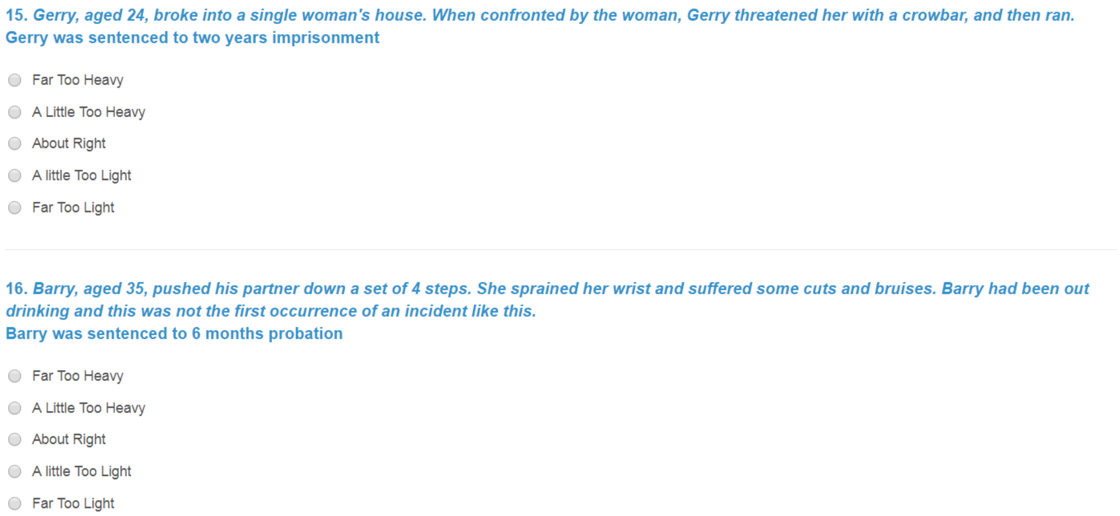
○ Far Too Heavy

○ A Little Too Heavy

○ About Right

○ A little Too Light

○ Far Too Light



15. Gerry, aged 24, broke into a single woman's house. When confronted by the woman, Gerry threatened her with a crowbar, and then ran.
Gerry was sentenced to two years imprisonment

○ Far Too Heavy

○ A Little Too Heavy

○ About Right

○ A little Too Light

○ Far Too Light

16. Barry, aged 35, pushed his partner down a set of 4 steps. She sprained her wrist and suffered some cuts and bruises. Barry had been out drinking and this was not the first occurrence of an incident like this.
Barry was sentenced to 6 months probation

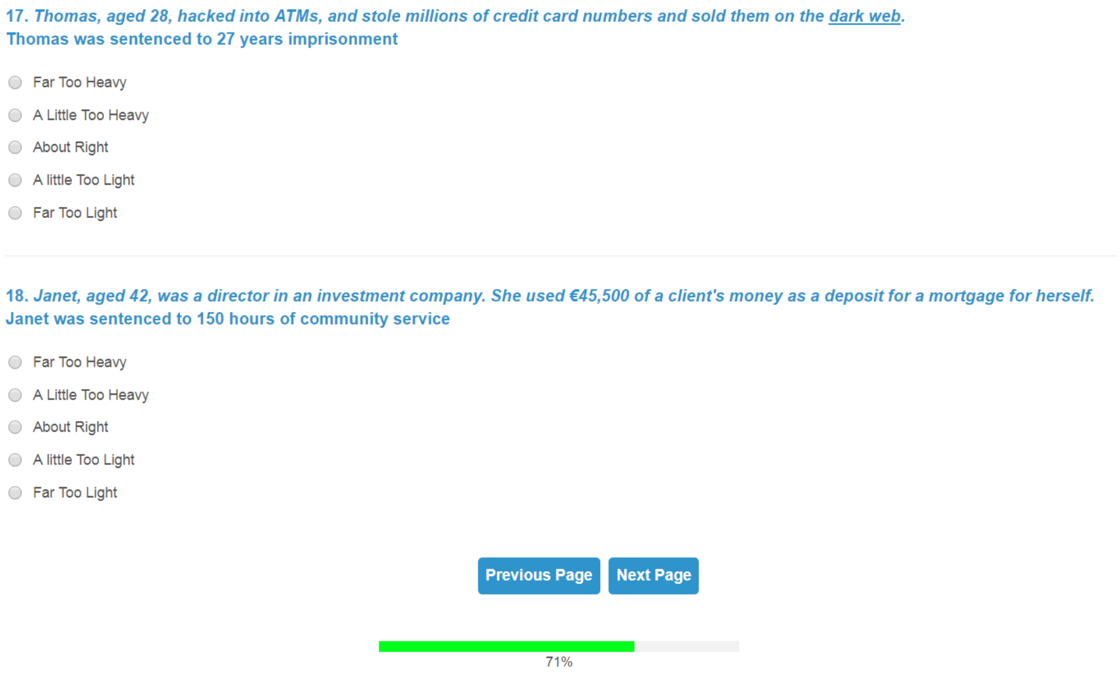
○ Far Too Heavy

○ A Little Too Heavy

○ About Right

○ A little Too Light

○ Far Too Light



17. ***Thomas, aged 28, hacked into ATMs, and stole millions of credit card numbers and sold them on the dark web.***
Thomas was sentenced to 27 years imprisonment

○ Far Too Heavy

○ A Little Too Heavy

○ About Right

○ A little Too Light

○ Far Too Light

18. ***Janet, aged 42, was a director in an investment company. She used €45,500 of a client's money as a deposit for a mortgage for herself.***
Janet was sentenced to 150 hours of community service

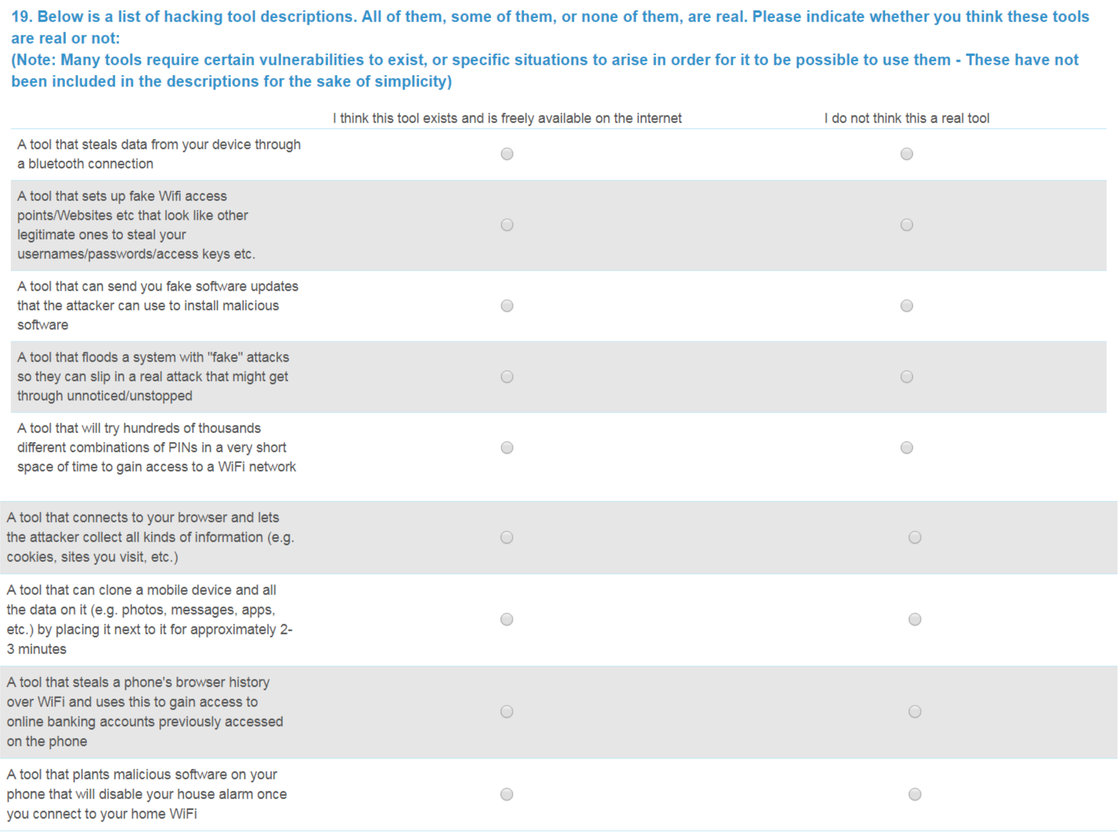
○ Far Too Heavy

○ A Little Too Heavy

○ About Right

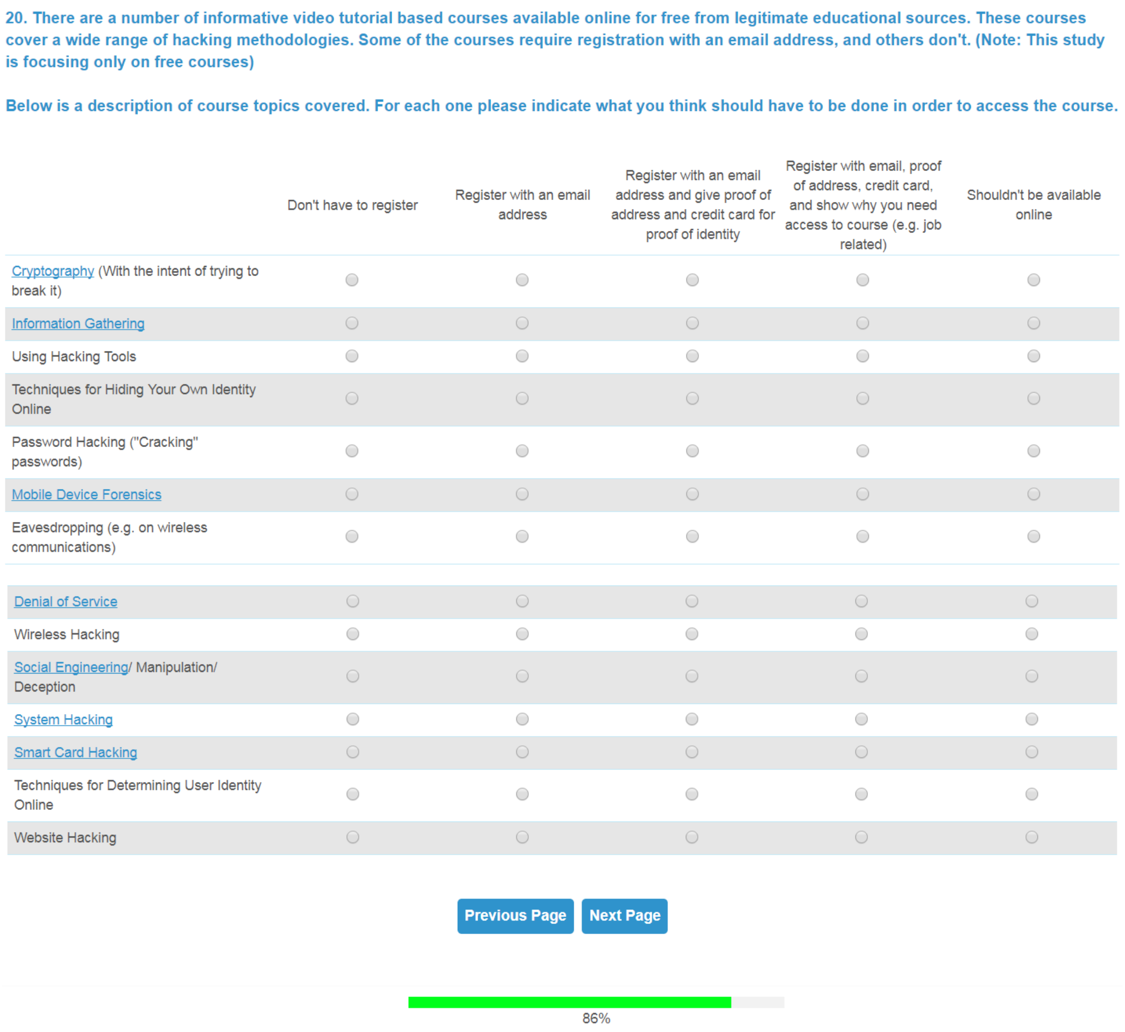
○ A little Too Light

○ Far Too Light



19. Below is a list of hacking tool descriptions. All of them, some of them, or none of them, are real. Please indicate whether you think these tools are real or not:
(Note: Many tools require certain vulnerabilities to exist, or specific situations to arise in order for it to be possible to use them - These have not been included in the descriptions for the sake of simplicity)

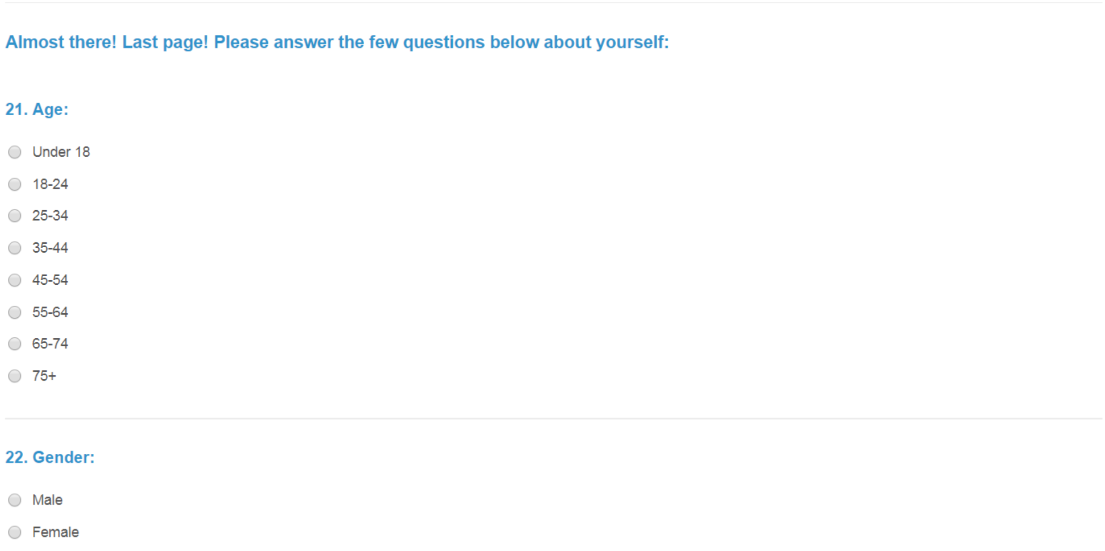
	I think this tool exists and is freely available on the internet	I do not think this a real tool
A tool that steals data from your device through a bluetooth connection	○	○
A tool that sets up fake Wifi access points/Websites etc that look like other legitimate ones to steal your usernames/passwords/access keys etc.	○	○
A tool that can send you fake software updates that the attacker can use to install malicious software	○	○
A tool that floods a system with "fake" attacks so they can slip in a real attack that might get through unnoticed/unstopped	○	○
A tool that will try hundreds of thousands different combinations of PINs in a very short space of time to gain access to a WiFi network	○	○
A tool that connects to your browser and lets the attacker collect all kinds of information (e.g. cookies, sites you visit, etc.)	○	○
A tool that can clone a mobile device and all the data on it (e.g. photos, messages, apps, etc.) by placing it next to it for approximately 2-3 minutes	○	○
A tool that steals a phone's browser history over WiFi and uses this to gain access to online banking accounts previously accessed on the phone	○	○
A tool that plants malicious software on your phone that will disable your house alarm once you connect to your home WiFi	○	○



20. There are a number of informative video tutorial based courses available online for free from legitimate educational sources. These courses cover a wide range of hacking methodologies. Some of the courses require registration with an email address, and others don't. (Note: This study is focusing only on free courses)

Below is a description of course topics covered. For each one please indicate what you think should have to be done in order to access the course.

	Don't have to register	Register with an email address	Register with an email address and give proof of address and credit card for proof of identity	Register with email, proof of address, credit card, and show why you need access to course (e.g. job related)	Shouldn't be available online
Cryptography (With the intent of trying to break it)	○	○	○	○	○
Information Gathering	○	○	○	○	○
Using Hacking Tools	○	○	○	○	○
Techniques for Hiding Your Own Identity Online	○	○	○	○	○
Password Hacking ("Cracking" passwords)	○	○	○	○	○
Mobile Device Forensics	○	○	○	○	○
Eavesdropping (e.g. on wireless communications)	○	○	○	○	○
Denial of Service	○	○	○	○	○
Wireless Hacking	○	○	○	○	○
Social Engineering/ Manipulation/ Deception	○	○	○	○	○
System Hacking	○	○	○	○	○
Smart Card Hacking	○	○	○	○	○
Techniques for Determining User Identity Online	○	○	○	○	○
Website Hacking	○	○	○	○	○



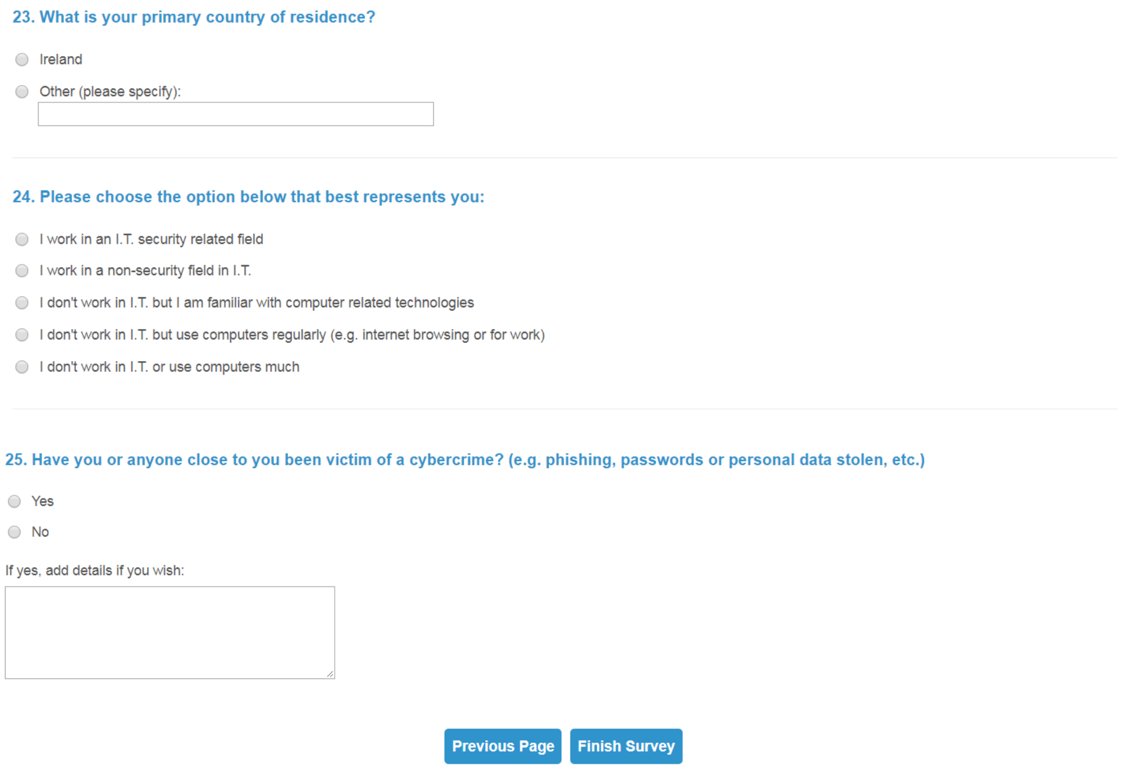
Almost there! Last page! Please answer the few questions below about yourself:

21. Age:

○ Under 18
○ 18-24
○ 25-34
○ 35-44
○ 45-54
○ 55-64
○ 65-74
○ 75+

22. Gender:

○ Male
○ Female



23. What is your primary country of residence?

○ Ireland

○ Other (please specify):

24. Please choose the option below that best represents you:

○ I work in an I.T. security related field

○ I work in a non-security field in I.T.

○ I don't work in I.T. but I am familiar with computer related technologies

○ I don't work in I.T. but use computers regularly (e.g. internet browsing or for work)

○ I don't work in I.T. or use computers much

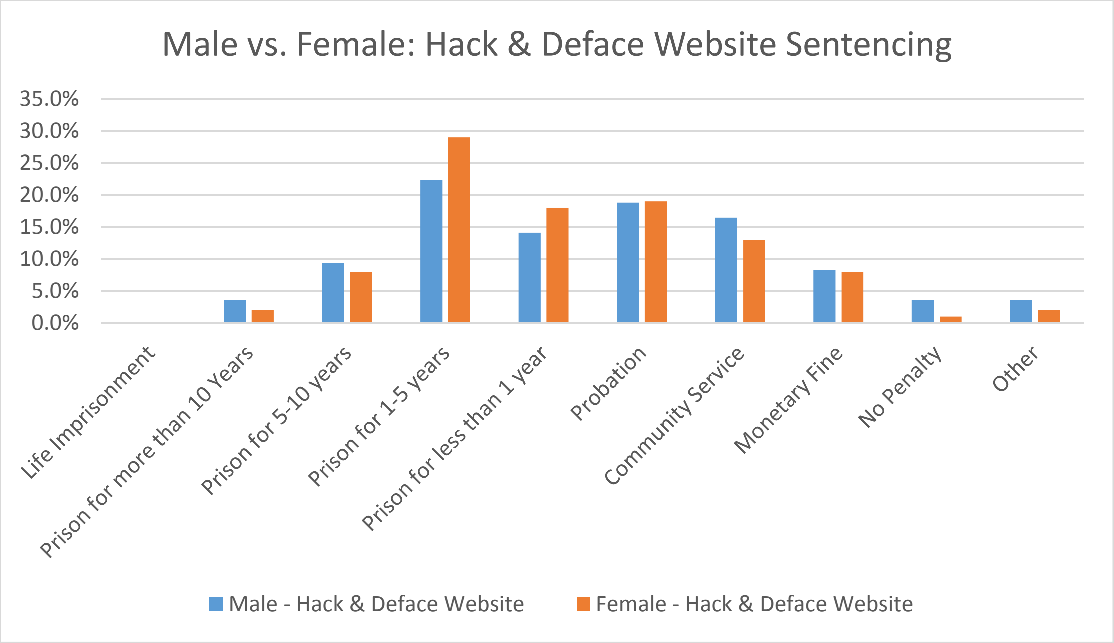
25. Have you or anyone close to you been victim of a cybercrime? (e.g. phishing, passwords or personal data stolen, etc.)

○ Yes

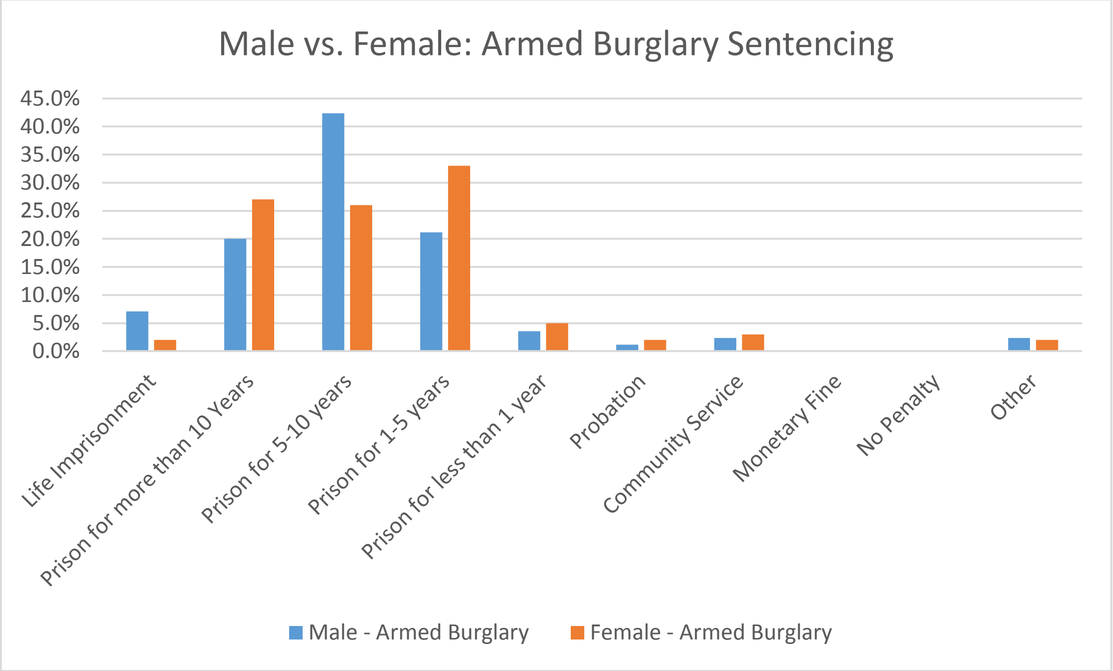
○ No

If yes, add details if you wish:

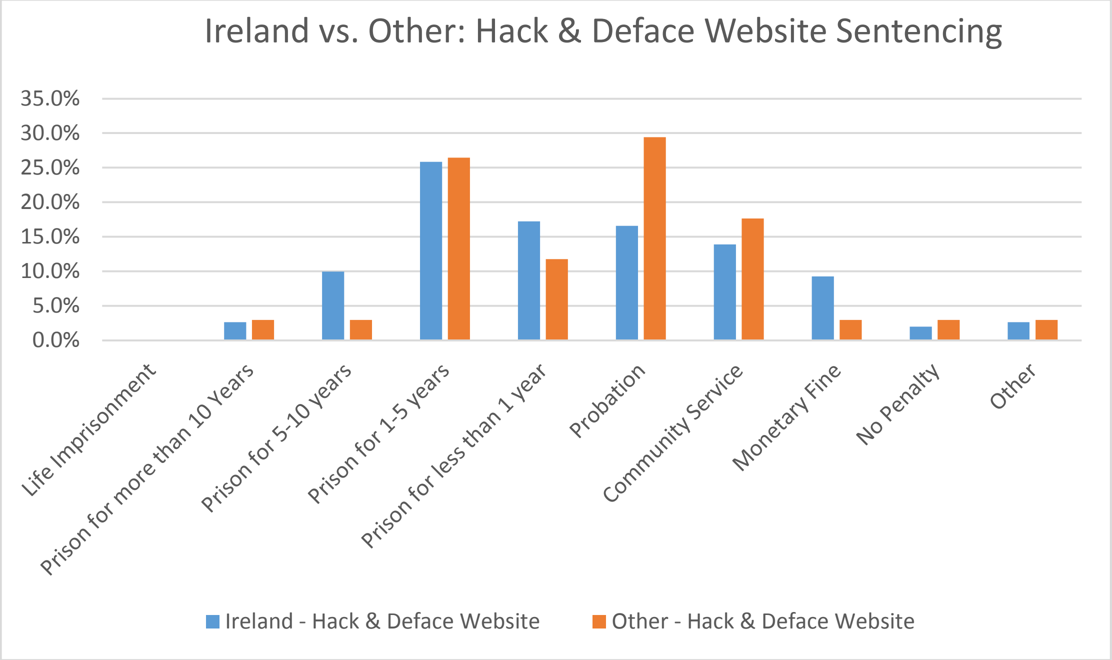
APPENDIX B

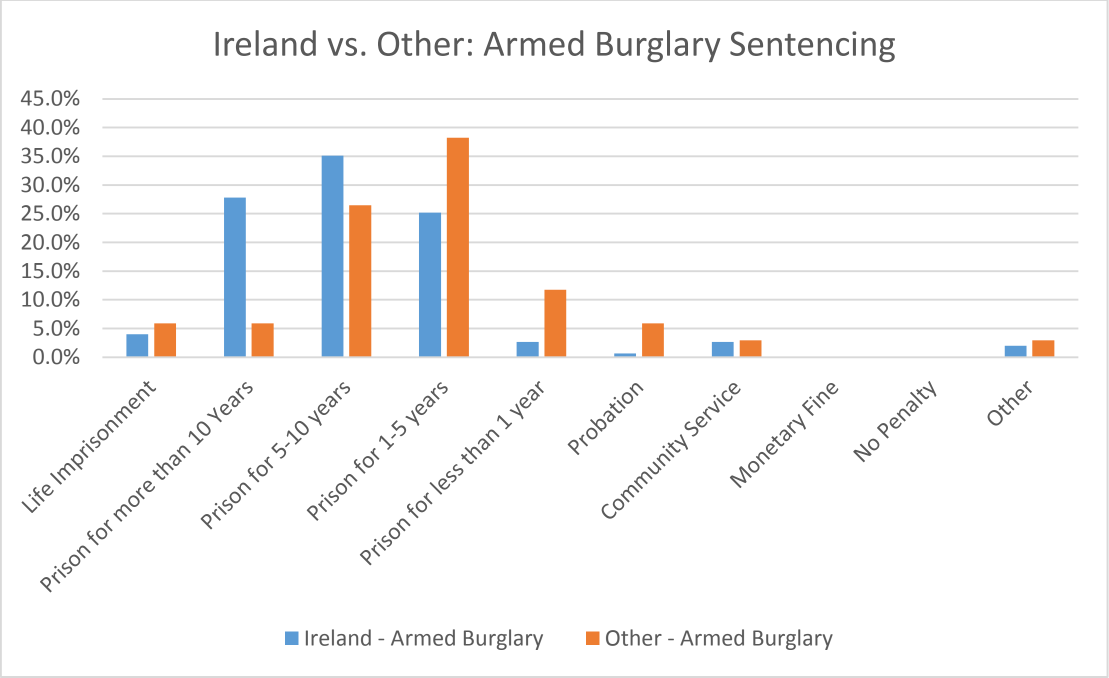


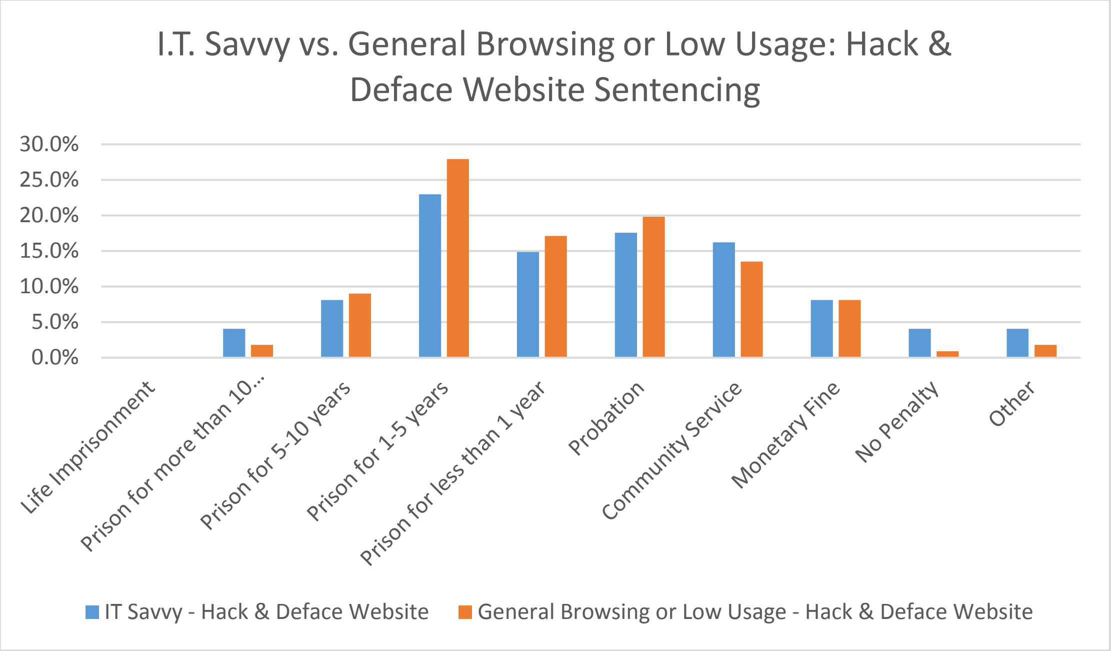
Male vs. Female: Hack & Deface Website Sentencing
35.0%
30.0%
25.0%
20.0%
15.0%
10.0%
5.0%
0.0%
Life Imprisonment
Prison for more than 10 Years
Prison for 5-10 years
Prison for 1-5 years
Prison for less than 1 year
Probation
Community Service
Monetary Fine
No Penalty
Other
Male - Hack & Deface Website
Female - Hack & Deface Website

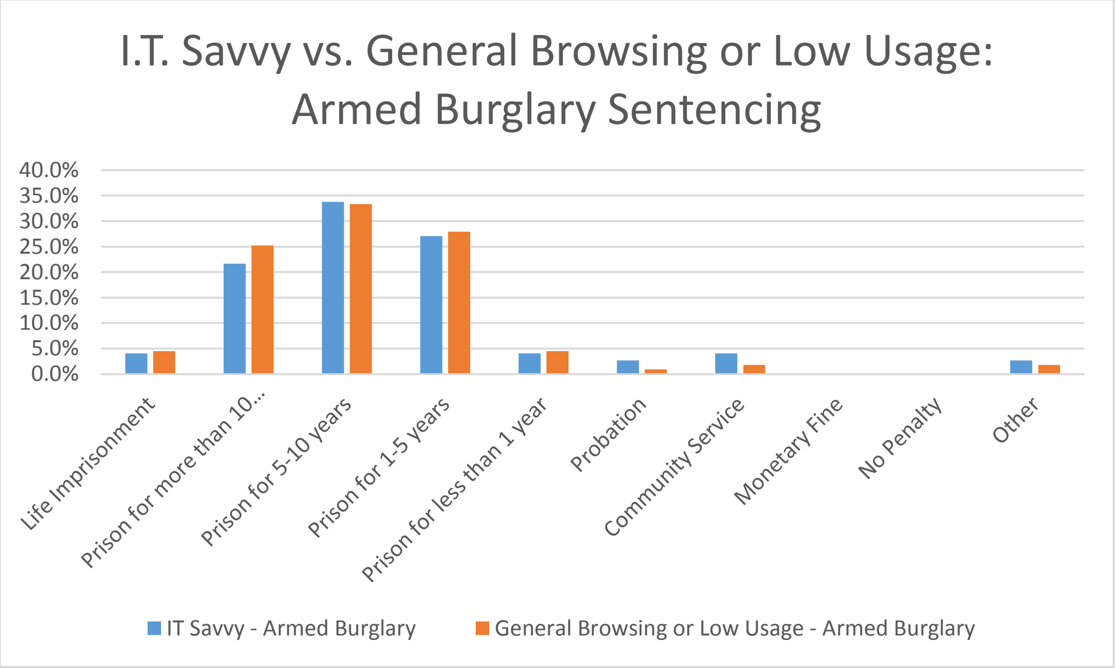


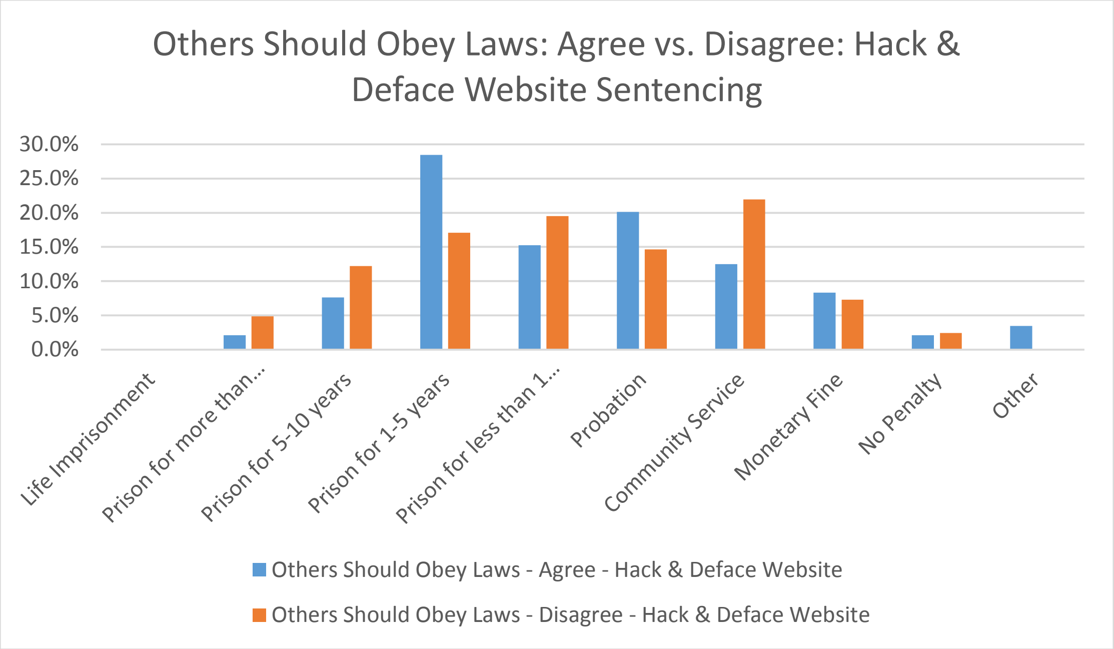
Male vs. Female: Armed Burglary Sentencing
45.0%
40.0%
35.0%
30.0%
25.0%
20.0%
15.0%
10.0%
5.0%
0.0%
Life Imprisonment
Prison for more than 10 Years
Prison for 5-10 years
Prison for 1-5 years
Prison for less than 1 year
Probation
Community Service
Monetary Fine
No Penalty
Other
Male - Armed Burglary
Female - Armed Burglary

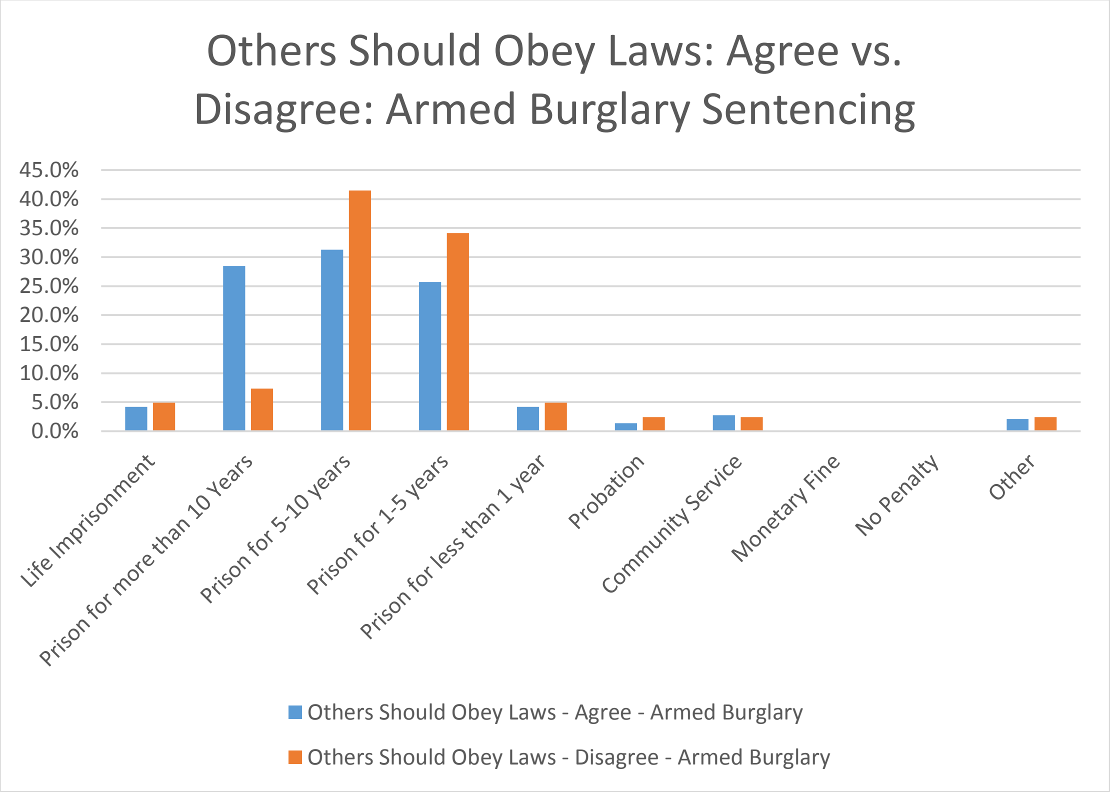

Ireland vs. Other: Hack & Deface Website Sentencing
35.0%
30.0%
25.0%
20.0%
15.0%
10.0%
5.0%
0.0%
Life Imprisonment
Prison for more than 10 Years
Prison for 5-10 years
Prison for 1-5 years
Prison for less than 1 year
Probation
Community Service
Monetary Fine
No Penalty
Other
Ireland - Hack & Deface Website
Other - Hack & Deface Website

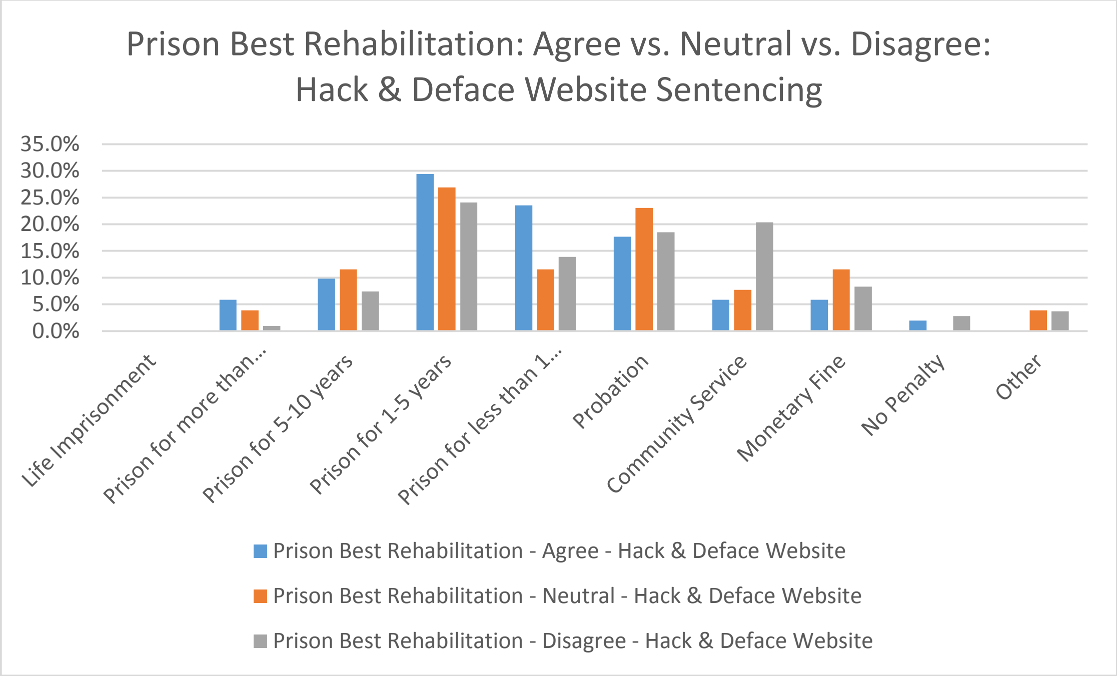

Ireland vs. Other: Armed Burglary Sentencing
45.0%
40.0%
35.0%
30.0%
25.0%
20.0%
15.0%
10.0%
5.0%
0.0%
Life Imprisonment
Prison for more than 10 Years
Prison for 5-10 years
Prison for 1-5 years
Prison for less than 1 year
Probation
Community Service
Monetary Fine
No Penalty
Other
Ireland - Armed Burglary
Other - Armed Burglary

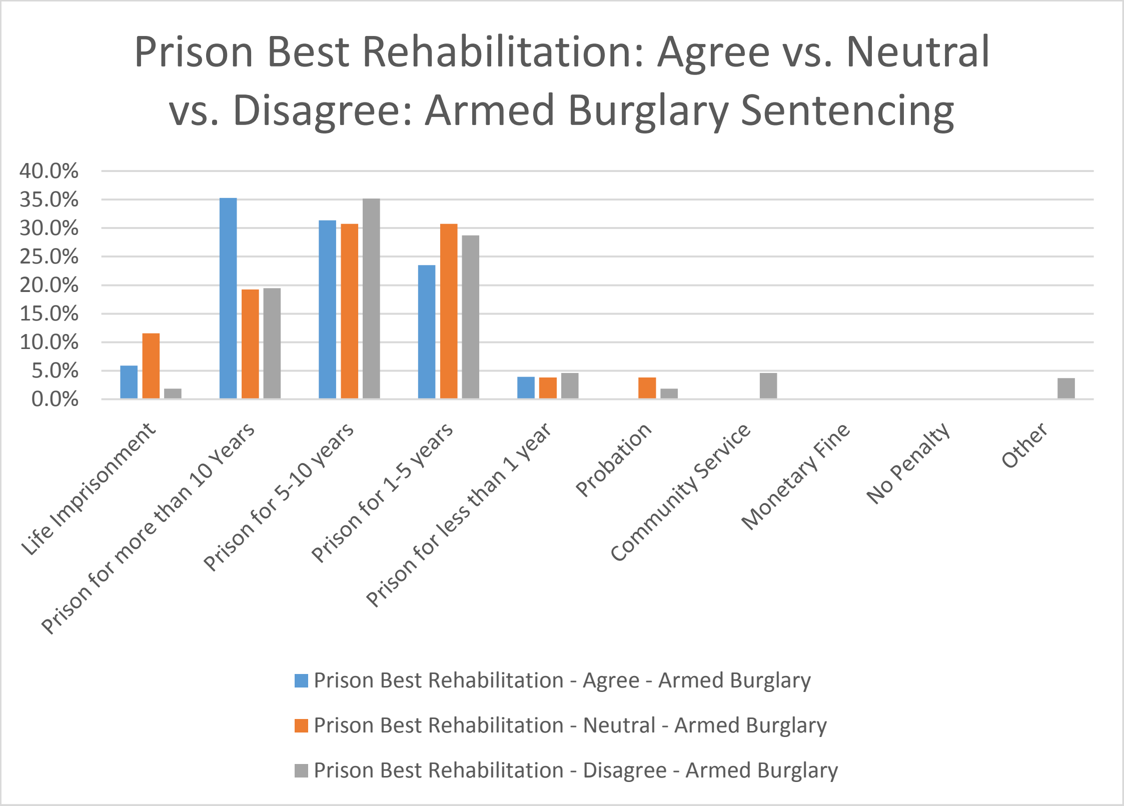

I.T. Savvy vs. General Browsing or Low Usage: Hack & Deface Website Sentencing
30.0%
25.0%
20.0%
15.0%
10.0%
5.0%
0.0%
Life Imprisonment
Prison for more than 10...
Prison for 5-10 years
Prison for 1-5 years
Prison for less than 1 year
Probation
Community Service
Monetary Fine
No Penalty
Other
IT Savvy - Hack & Deface Website
General Browsing or Low Usage - Hack & Deface Website

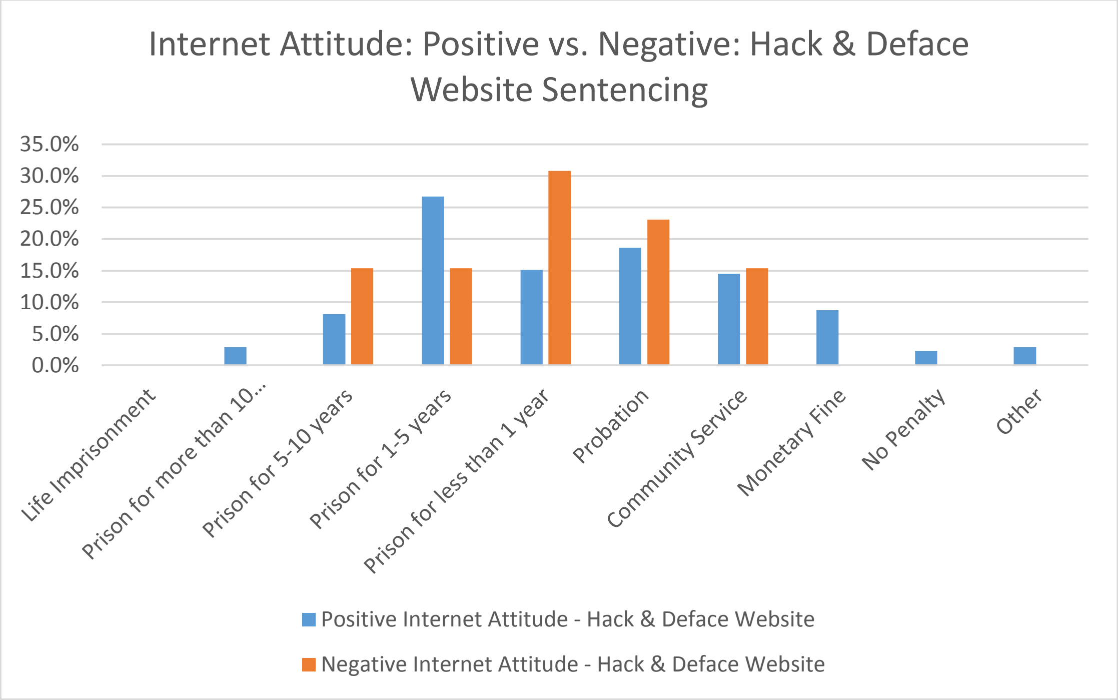

I.T. Savvy vs. General Browsing or Low Usage: Armed Burglary Sentencing
40.0%
35.0%
30.0%
25.0%
20.0%
15.0%
10.0%
5.0%
0.0%
Life Imprisonment
Prison for more than 10...
Prison for 5-10 years
Prison for 1-5 years
Prison for less than 1 year
Probation
Community Service
Monetary Fine
No Penalty
Other
IT Savvy - Armed Burglary
General Browsing or Low Usage - Armed Burglary

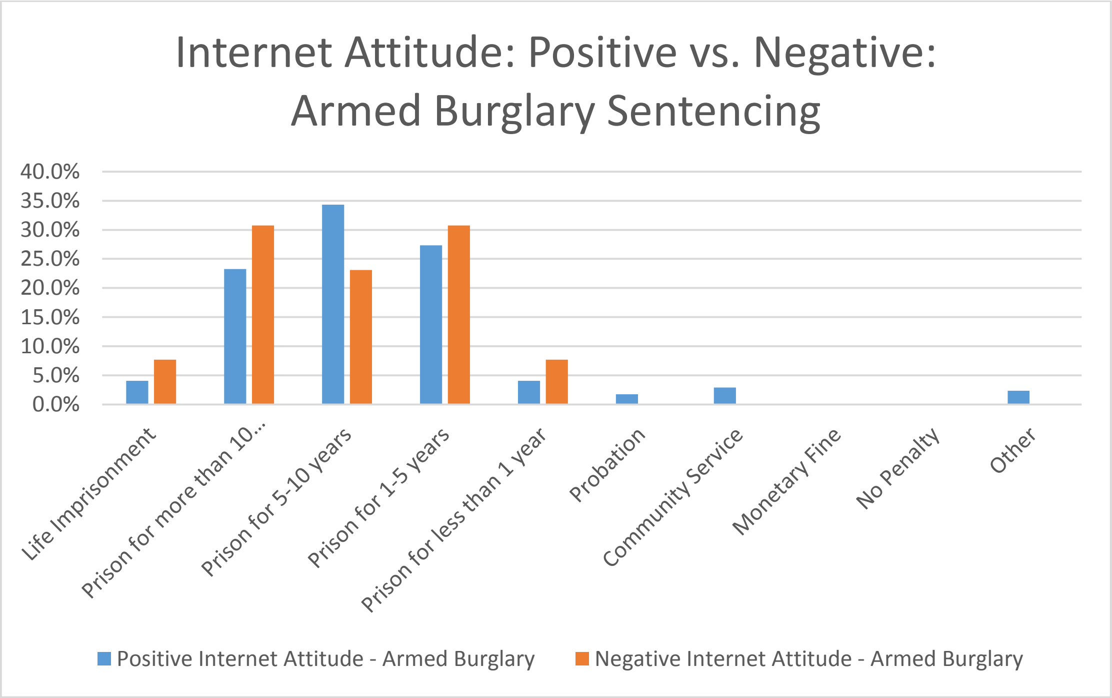

Others Should Obey Laws: Agree vs. Disagree: Hack & Deface Website Sentencing
30.0%
25.0%
20.0%
15.0%
10.0%
5.0%
0.0%
Life Imprisonment
Prison for more than...
Prison for 5-10 years
Prison for 1-5 years
Prison for less than 1...
Probation
Community Service
Monetary Fine
No Penalty
Other
Others Should Obey Laws - Agree - Hack & Deface Website
Others Should Obey Laws - Disagree - Hack & Deface Website


Others Should Obey Laws: Agree vs. Disagree: Armed Burglary Sentencing
45.0%
40.0%
35.0%
30.0%
25.0%
20.0%
15.0%
10.0%
5.0%
0.0%
Life Imprisonment
Prison for more than 10 Years
Prison for 5-10 years
Prison for 1-5 years
Prison for less than 1 year
Probation
Community Service
Monetary Fine
No Penalty
Other
Others Should Obey Laws - Agree - Armed Burglary
Others Should Obey Laws - Disagree - Armed Burglary


Prison Best Rehabilitation: Agree vs. Neutral vs. Disagree: Hack & Deface Website Sentencing
35.0%
30.0%
25.0%
20.0%
15.0%
10.0%
5.0%
0.0%
Life Imprisonment
Prison for more than...
Prison for 5-10 years
Prison for 1-5 years
Prison for less than 1...
Probation
Community Service
Monetary Fine
No Penalty
Other
Prison Best Rehabilitation - Agree - Hack & Deface Website
Prison Best Rehabilitation - Neutral - Hack & Deface Website
Prison Best Rehabilitation - Disagree - Hack & Deface Website

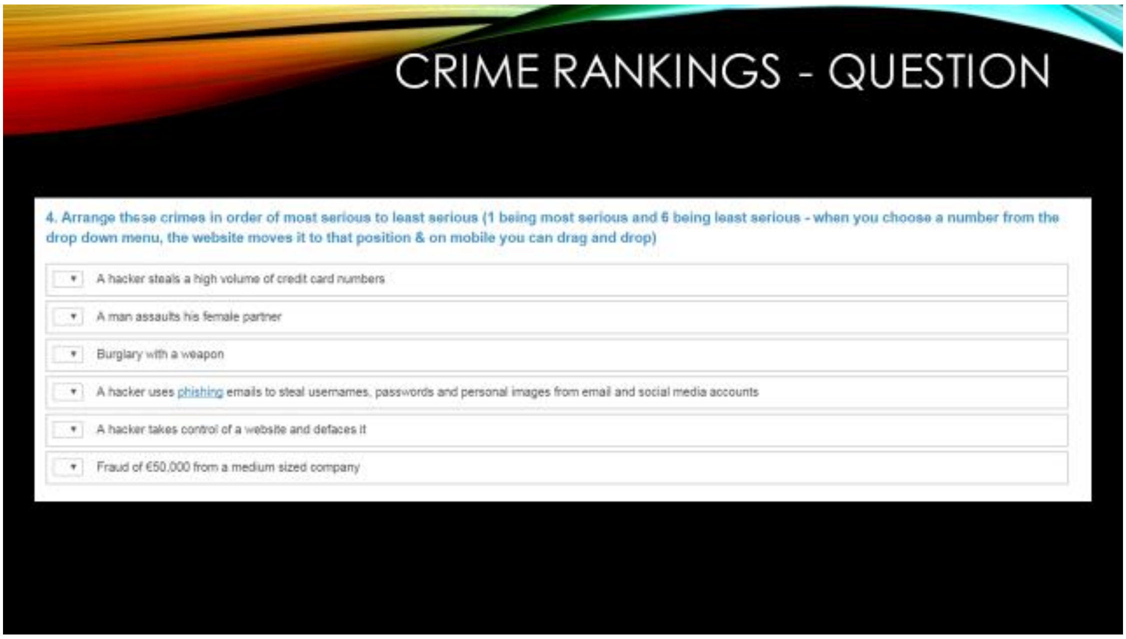

Prison Best Rehabilitation: Agree vs. Neutral vs. Disagree: Armed Burglary Sentencing
40.0%
35.0%
30.0%
25.0%
20.0%
15.0%
10.0%
5.0%
0.0%
Life Imprisonment
Prison for more than 10 Years
Prison for 5-10 years
Prison for 1-5 years
Prison for less than 1 year
Probation
Community Service
Monetary Fine
No Penalty
Other
Prison Best Rehabilitation - Agree - Armed Burglary
Prison Best Rehabilitation - Neutral - Armed Burglary
Prison Best Rehabilitation - Disagree - Armed Burglary


Internet Attitude: Positive vs. Negative: Hack & Deface Website Sentencing
35.0%
30.0%
25.0%
20.0%
15.0%
10.0%
5.0%
0.0%
Life Imprisonment
Prison for more than 10…
Prison for 5-10 years
Prison for 1-5 years
Prison for less than 1 year
Probation
Community Service
Monetary Fine
No Penalty
Other
Positive Internet Attitude - Hack & Deface Website
Negative Internet Attitude - Hack & Deface Website


Internet Attitude: Positive vs. Negative: Armed Burglary Sentencing
40.0%
35.0%
30.0%
25.0%
20.0%
15.0%
10.0%
5.0%
0.0%
Life Imprisonment
Prison for more than 10…
Prison for 5-10 years
Prison for 1-5 years
Prison for less than 1 year
Probation
Community Service
Monetary Fine
No Penalty
Other
Positive Internet Attitude - Armed Burglary
Negative Internet Attitude - Armed Burglary

APPENDIX C

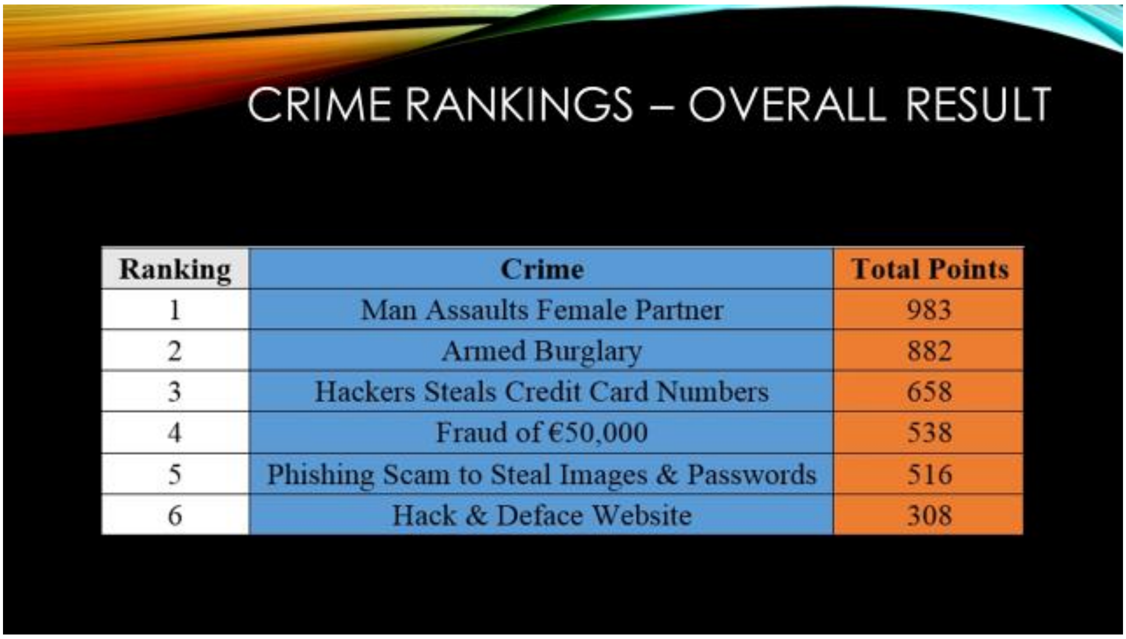
CYBERCRIME SURVEY – EXPERT OPINION ON RESULTS



CRIME RANKINGS - QUESTION

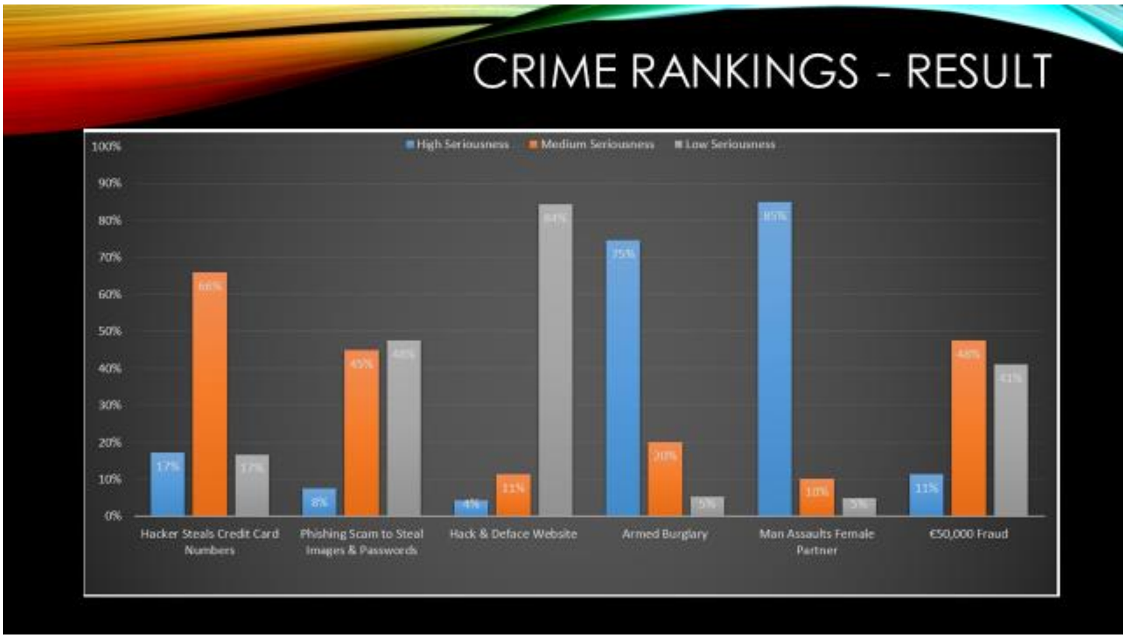
4. Arrange these crimes in order of most serious to least serious (1 being most serious and 6 being least serious - when you choose a number from the drop down menu, the website moves it to that position & on mobile you can drag and drop)

- ▾ A hacker steals a high volume of credit card numbers
- ▾ A man assaults his female partner
- ▾ Burglary with a weapon
- ▾ A hacker uses phishing emails to steal usernames, passwords and personal images from email and social media accounts
- ▾ A hacker takes control of a website and defaces it
- ▾ Fraud of €50,000 from a medium sized company

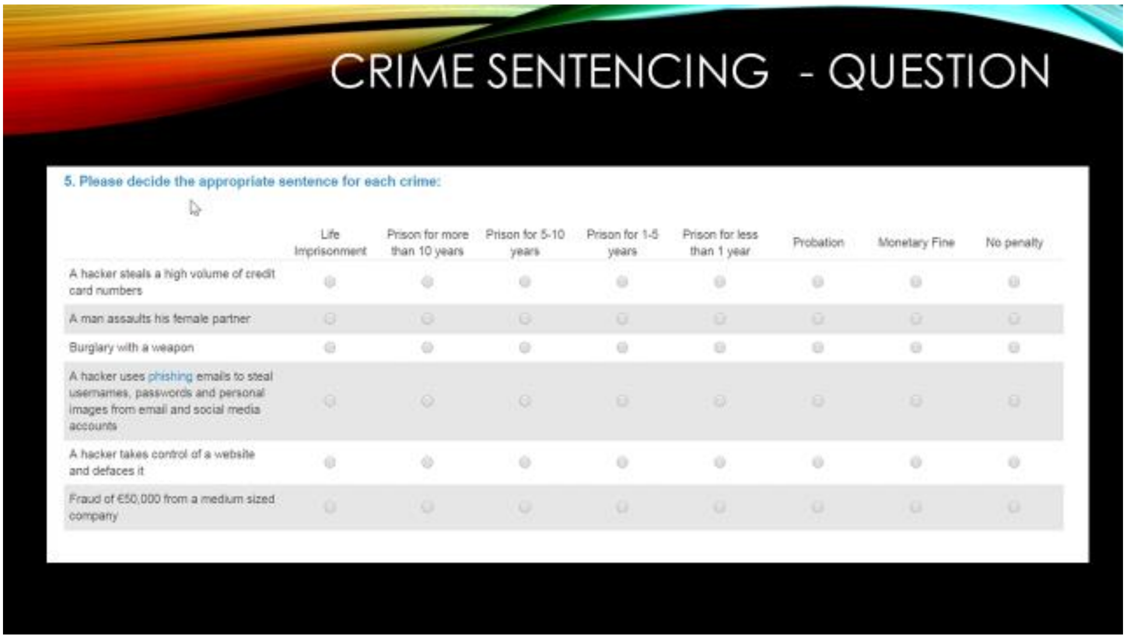


CRIME RANKINGS – OVERALL RESULT

Ranking	Crime	Total Points
1	Man Assaults Female Partner	983
2	Armed Burglary	882
3	Hackers Steals Credit Card Numbers	658
4	Fraud of €50,000	538
5	Phishing Scam to Steal Images & Passwords	516
6	Hack & Deface Website	308



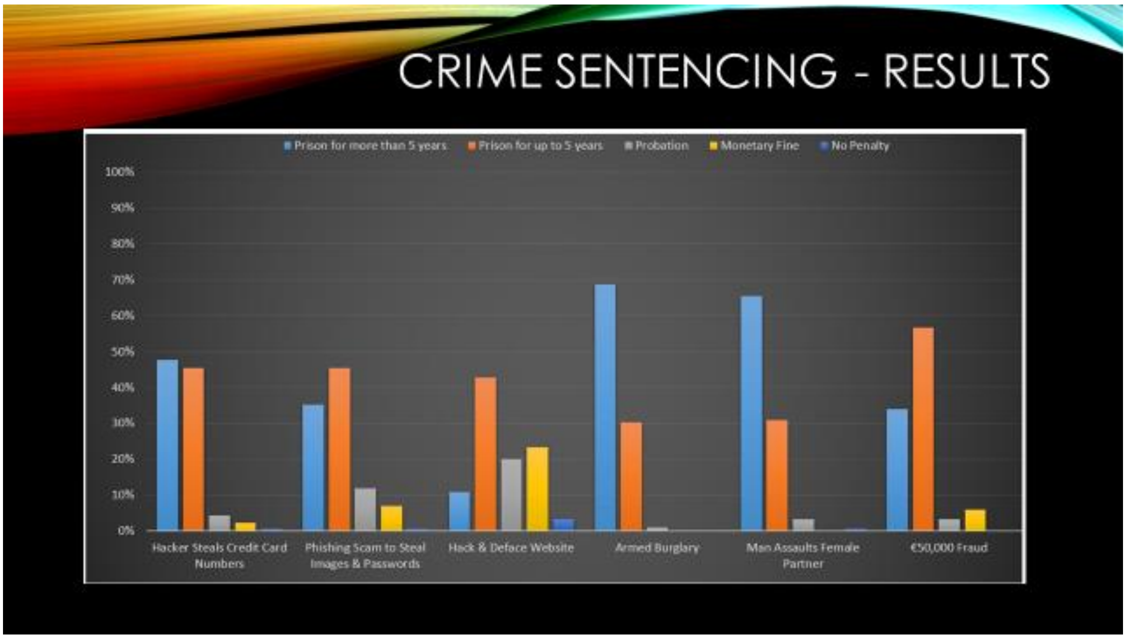
CRIME RANKINGS - RESULT



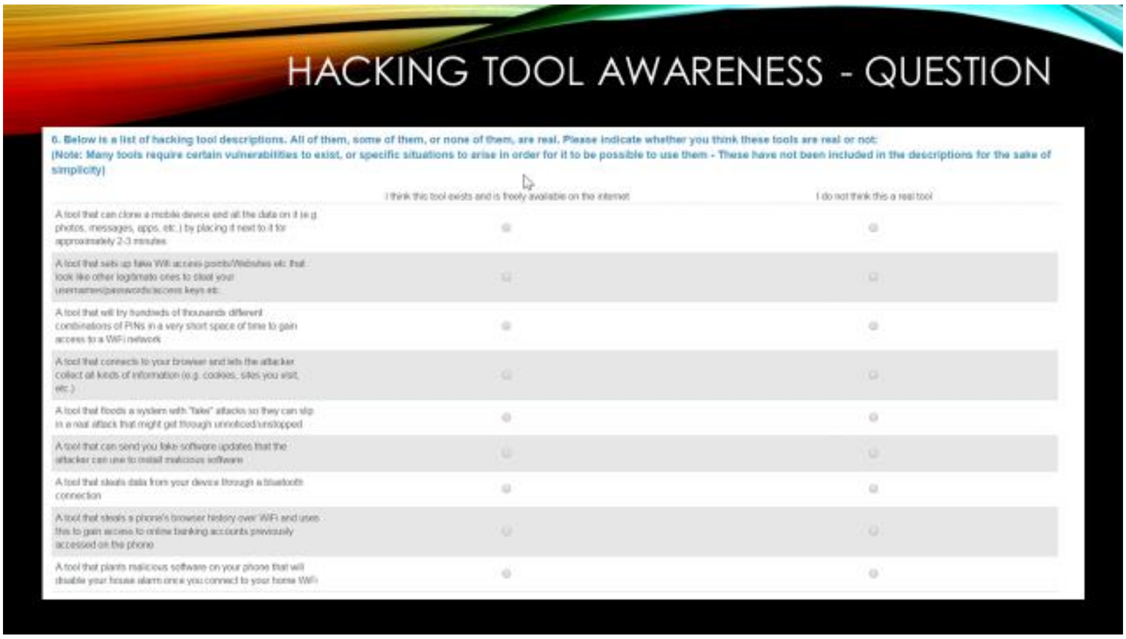
CRIME SENTENCING - QUESTION

5. Please decide the appropriate sentence for each crime:

	Life Imprisonment	Prison for more than 10 years	Prison for 5-10 years	Prison for 1-5 years	Prison for less than 1 year	Probation	Monetary Fine	No penalty
A hacker steals a high volume of credit card numbers	○	○	○	○	○	○	○	○
A man assaults his female partner	○	○	○	○	○	○	○	○
Burglary with a weapon	○	○	○	○	○	○	○	○
A hacker uses phishing emails to steal usernames, passwords and personal images from email and social media accounts	○	○	○	○	○	○	○	○
A hacker takes control of a website and defaces it	○	○	○	○	○	○	○	○
Fraud of €50,000 from a medium sized company	○	○	○	○	○	○	○	○



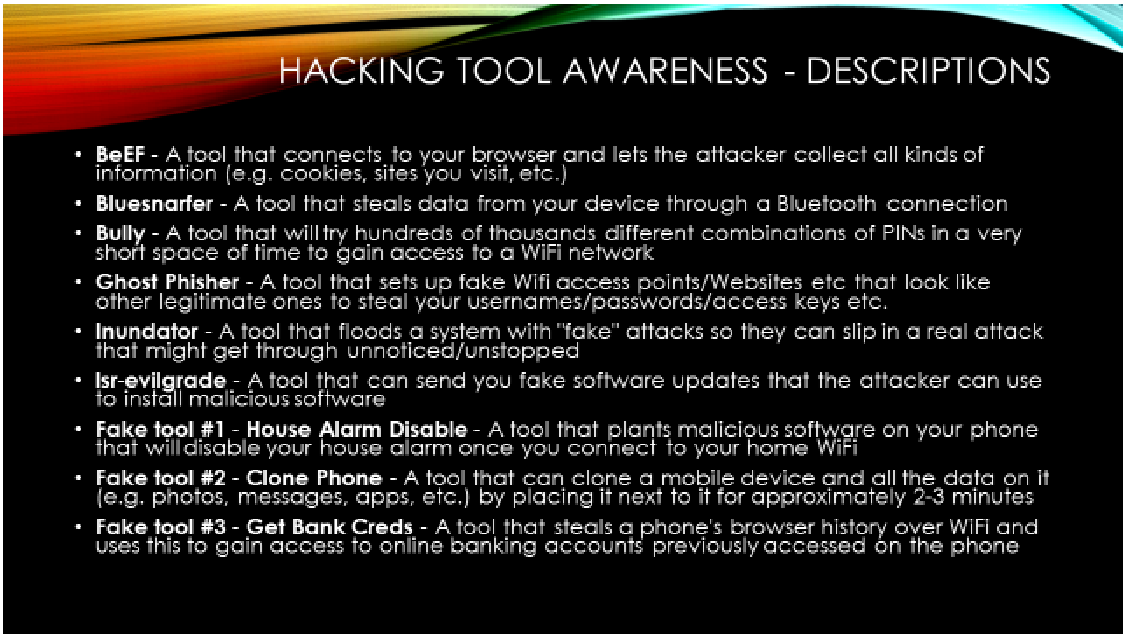
CRIME SENTENCING - RESULTS



HACKING TOOL AWARENESS - QUESTION

6. Below is a list of hacking tool descriptions. All of them, some of them, or none of them, are real. Please indicate whether you think these tools are real or not:
(Note: Many tools require certain vulnerabilities to exist, or specific situations to arise in order for it to be possible to use them - These have not been included in the descriptions for the sake of simplicity)

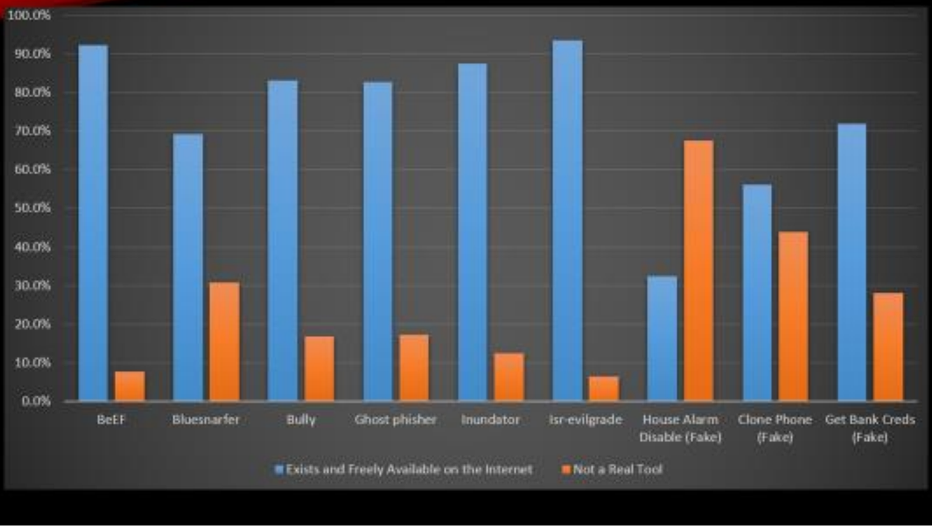
	I think this tool exists and is freely available on the internet	I do not think this a real tool
A tool that can clone a mobile device and all the data on it (e.g. photos, messages, apps, etc.) by placing it next to it for approximately 2-3 minutes	○	○
A tool that sets up fake Wifi access points/Websites etc that look like other legitimate ones to steal your usernames/passwords/access keys etc.	○	○
A tool that will try hundreds of thousands different combinations of PINs in a very short space of time to gain access to a WiFi network	○	○
A tool that connects to your browser and lets the attacker collect all kinds of information (e.g. cookies, sites you visit, etc.)	○	○
A tool that floods a system with "fake" attacks so they can slip in a real attack that might get through unnoticed/unstopped	○	○
A tool that can send you fake software updates that the attacker can use to install malicious software	○	○
A tool that steals data from your device through a bluetooth connection	○	○
A tool that steals a phone's browser history over WiFi and uses this to gain access to online banking accounts previously accessed on the phone	○	○
A tool that plants malicious software on your phone that will disable your house alarm once you connect to your home WiFi	○	○



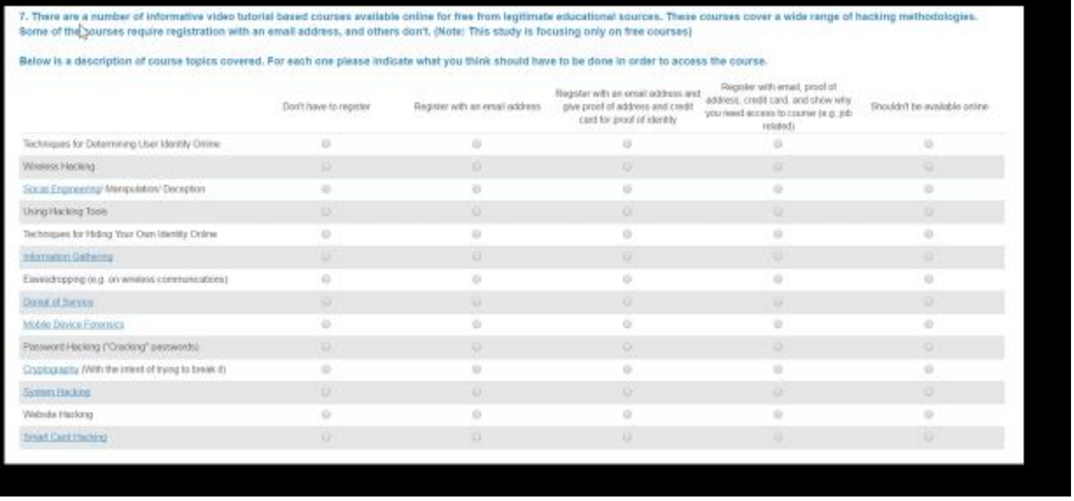
HACKING TOOL AWARENESS - DESCRIPTIONS

- **BeEF** - A tool that connects to your browser and lets the attacker collect all kinds of information (e.g. cookies, sites you visit, etc.)
- **Bluesnarfer** - A tool that steals data from your device through a Bluetooth connection
- **Bully** - A tool that will try hundreds of thousands different combinations of PINs in a very short space of time to gain access to a WiFi network
- **Ghost Phisher** - A tool that sets up fake Wifi access points/Websites etc that look like other legitimate ones to steal your usernames/passwords/access keys etc.
- **Inundator** - A tool that floods a system with "fake" attacks so they can slip in a real attack that might get through unnoticed/unstopped
- **Isr-evilgrade** - A tool that can send you fake software updates that the attacker can use to install malicious software
- **Fake tool #1 - House Alarm Disable** - A tool that plants malicious software on your phone that will disable your house alarm once you connect to your home WiFi
- **Fake tool #2 - Clone Phone** - A tool that can clone a mobile device and all the data on it (e.g. photos, messages, apps, etc.) by placing it next to it for approximately 2-3 minutes
- **Fake tool #3 - Get Bank Creds** - A tool that steals a phone's browser history over WiFi and uses this to gain access to online banking accounts previously accessed on the phone

HACKING TOOL AWARENESS - RESULTS



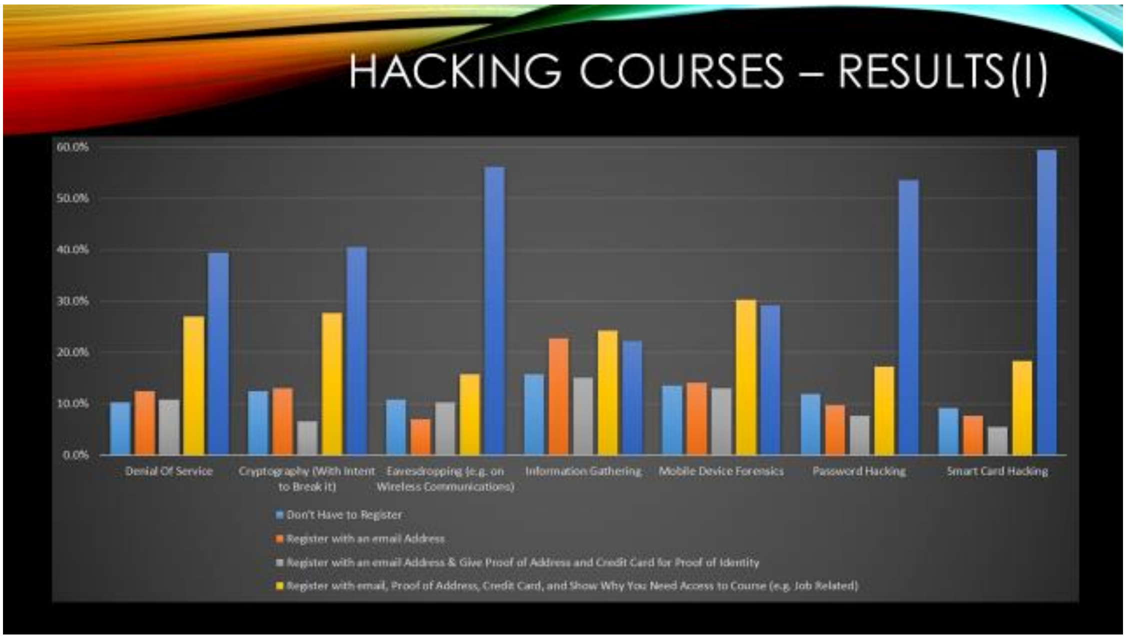
HACKING COURSES - QUESTION



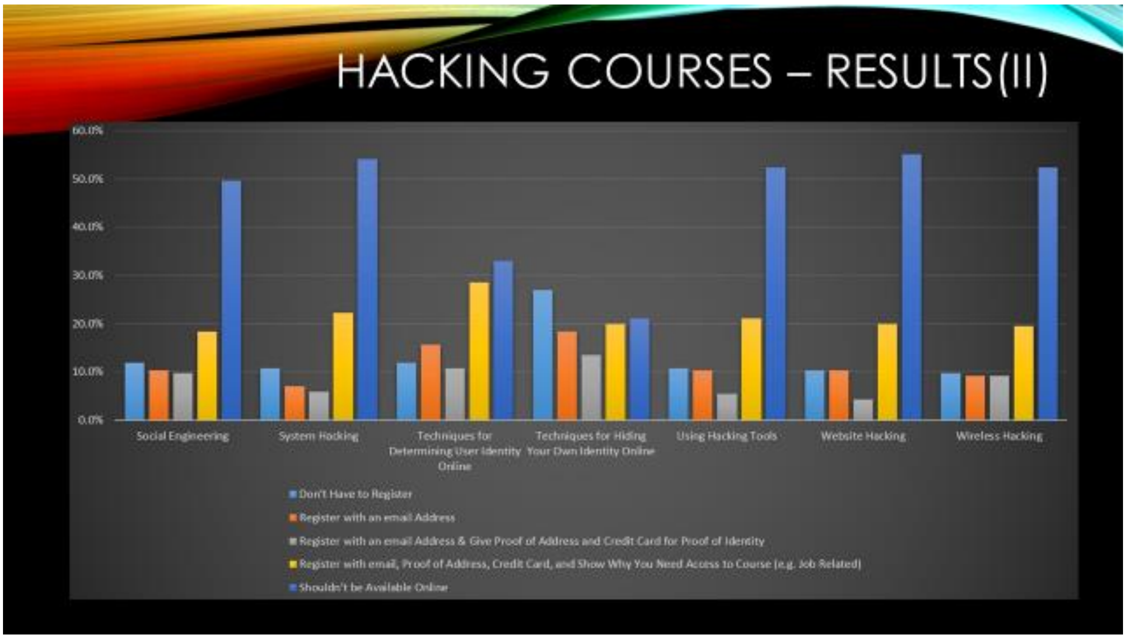
7. There are a number of informative video tutorial based courses available online for free from legitimate educational sources. These courses cover a wide range of hacking methodologies. Some of the courses require registration with an email address, and others don't. (Note: This study is focusing only on free courses)

Below is a description of course topics covered. For each one please indicate what you think should have to be done in order to access the course.

	Don't have to register	Register with an email address	Register with an email address and give proof of address and credit card for proof of identity	Register with email, proof of address, credit card, and show why you need access to course (e.g. job related)	Shouldn't be available online
Techniques for Determining User Identity Online	○	○	○	○	○
Wireless Hacking	○	○	○	○	○
Social Engineering/ Manipulation/ Deception	○	○	○	○	○
Using Hacking Tools	○	○	○	○	○
Techniques for Hiding Your Own Identity Online	○	○	○	○	○
Information Gathering	○	○	○	○	○
Eavesdropping (e.g. on wireless communications)	○	○	○	○	○
Denial of Service	○	○	○	○	○
Mobile Device Forensics	○	○	○	○	○
Password Hacking ("Cracking" passwords)	○	○	○	○	○
Cryptography (With the intent of trying to break it)	○	○	○	○	○
System Hacking	○	○	○	○	○
Website Hacking	○	○	○	○	○
Smart Card Hacking	○	○	○	○	○



HACKING COURSES – RESULTS(I)



HACKING COURSES – RESULTS(II)

THANK YOU FOR YOUR PARTICIPATION