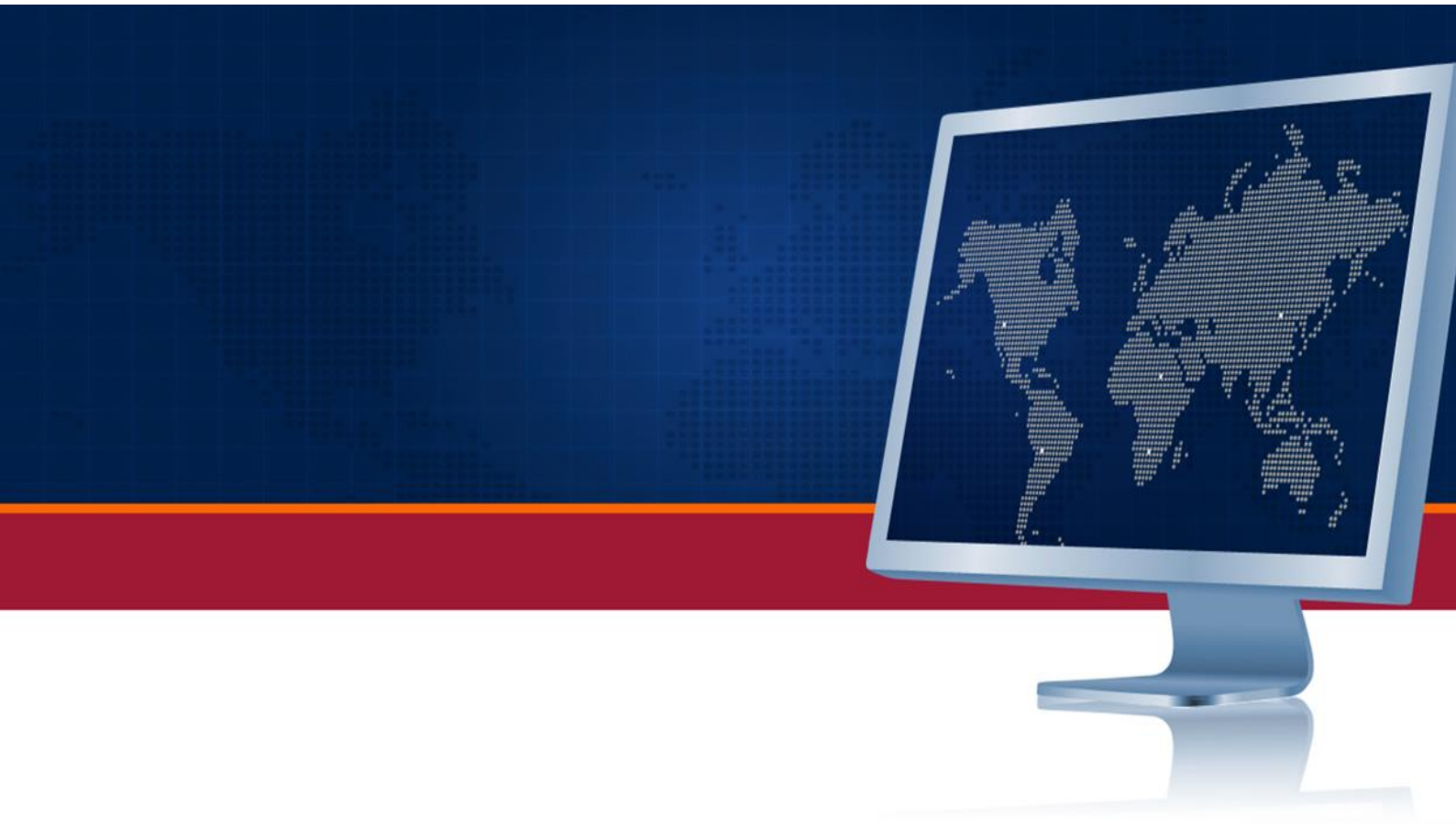


CARDING

Crime prevention analysis

Tristan Janothan Meijerink

t.j.meijerink@student.utwente.nl
01/02/2013

UNIVERSITEIT TWENTE.

POLITIE
Netherlands Police Agency

Abstract.

This bachelor thesis focuses on carding, a type of cybercrime. This exploratory case study highlights aspects and processes of carding in order to find effective ways of combating it. The processes discussed in this study are phishing, skimming, making of counterfeit cards and money mules. This study searches for patterns and steps in those criminal processes of carding by using the best available information from police reports, other sources, (scientific) literature and online news articles on carding and its processes. Patterns are those actions or activities that emerge each time a carding scheme or process related to carding takes place. Think of activities, actors or tools. By using news articles online, which are not so reliable, relevant data and information can be retrieved for developing models and descriptions of several carding processes. The analyzed online news articles, relate to: carding arrests and suspects, what was going on, and the crime or activities of the suspects. The news articles are categorized for later comparison and development of clear patterns, so that models could be made to fight this crime. Although some literature explains what carding is and its relevant processes, none explains the sequence or variants of activities. The data gained from news articles and other literature complements the basic information only partly and leaves much room available for variation and commentary. By combining data from news articles and literature, models are created covering the most common carding scenarios (phishing, skimming, making of counterfeit cards and money mules). The models are in fact a summary of what is stated in the cited news articles. Using patterns and models, a barrier model can be created that may produce an effective way to prevent carding by intervening in the most effective places and ways by different authorities and organizations. This study helps people better understand the carding process and documents much of the carding knowledge found within the National High Tech Crime Unit (NHTCU) of the Netherlands' Police Agency. Eventually, researchers can compare these results with the results of other types of cybercrime studies with the aim of finding patterns related to cybercrime as a whole.

The structure of this study is as follows. First, an introduction will be given followed by the objectives and research questions, the definitions used within this study and limitations of previous studies. After that, the methodologies, data collection and analysis are discussed. Once these issues are covered, the patterns that are recognized during the study are discussed in the results. Then, two barrier models based on the analysis and results are presented where the link with organizations and authorities, and opportunity-reducing techniques is added. Finally, a discussion follows, including the conclusions, recommendations, and concerns.

Keywords: Cybercrime, high Tech crime, carding, phishing, malware, social engineering, police, criminal process, counterfeit cards, model, money mule, situational crime prevention, barrier model.

Table of contents

1. Understanding processes of carding

According to Leukfeldt (2010) and Taylor et al (2006), internet fraud will target many victims in the future. Computer criminals are constantly looking for new and better methods to increase their chances of success. An organization called Citigroup suffered about $2.7 million in losses - which is just one of many examples - after hackers found a way to steal credit card information from its website and post fraudulent charges (McMillan, (2011).

People nowadays are dependent on the use of computers, as they have a major impact on someone's social life and the way he or she conducts business (Ayaz, 2006). Digitalization and globalization ensure that national and international crime over the internet gets easier and becomes more widespread. Even tactics about performing a crime are being spread throughout the Internet. For example, on the website of darknet.org.uk, a list is being made of the top 15 security/hacking tools and utilities. The motto of this site is 'hack to learn'. Although the given information is not completely objective, the 138 reactions and number of views (so far 1,438,949 views) on it are quite interesting. When analyzing this webpage, the posted reactions seem to come from people who are familiar with hacking. Some reactions even mention other tools or utilities that are not on the list. Although there is no evidence for it, looking at some of these reactions one might think they come from people who have experience in hacking (Darknet, 2006). Anyhow, cybercrime is a problem and more victims in the future are expected.

This study discusses carding. Carding can be divided in two separate steps: the set of techniques by which [1] information from credit cards and other payment information get into the hands of criminals and [2] how this information is used by criminals (the Netherlands' Police Agency, DNR, 2009, p.69).

To show the importance of carding and other types of cybercrime, the internet crime complaint centre of the US (The National White Collar Crime Centre (NCW3)) (Reed, 2011) reports that they received more than two million complaints in 2010 alone. On average, the Internet Crime Complaint Centre (IC3) receives and processes 25,000 complaints per month. These figures all cover cybercrime and not just carding. However, since carding spans multiple forms of cybercrime (such as spamming, identity theft or credit card fraud) as well, carding must be taken seriously.

Aside from examining figures showing how often cybercrime occurs, one can also look at the financial damage it causes. According Sanders (2006), online crime in the United States caused $67.2 billion in damages in 2006. These figures are taken from an FBI survey. The findings are based on a poll of 2,066 organizations, of which nearly 90 percent had experienced a computer security incident (as victims) over the past 12 months (Sanders, 2006). In addition, Carl Clump, CEO of Retail Decisions, said that Payment fraud reached $2.14 billion in 2009 in the United States (Hernandez, 2010). In the United Kingdom, card fraud cost £610 million pounds in 2008. The British Crime Survey - based on interviews with

40,000 households - shows there were 2.8 million fraudulent card transactions in 2008 in the UK (Hickley, 2009). The information exposes the general trend and represents the amount of victims and complaints sent to Internet Crime Complaint Centre in the US. When looking at financial damage in the Netherlands, the Dutch Association of Banks (Nederlandse Vereniging van Banken, NVB 2008, 2011) provides figures about internet banking fraud. See table 1.

Internetbankieren	2008	2009	2010
Nederland	2.100.000	1.900.000	9.800.000

Table 1. Internet banking fraud figures of the Netherlands in euros.

The average loss per successful incident in the Netherlands in 2010 was 7100 euros (NVB, 2011). Although authorities find it hard to ascertain the exact amount of financial damage, these examples show us that the damage done by carding and other cybercrimes is high.

1.1 Objectives

This study has several objectives. These are:

1. The results of this study hope to contribute to the control and prevention of carding.

   To achieve this, this case study describes and develops some models of the important processes of carding. Next to that, this study searches for patterns in the processes of carding. This way, the modus operandi of carding partially becomes clear and interventions may be developed. The National Police Agency of the Netherlands would appreciate visible patterns and activities, so they can act and intervene quickly by using comprehensive descriptions and models. The models in this study are representations of the most common schemes and important recurring terms (patterns that have to do with activities or persons involved).

2. Because carding is related to other (cyber) crimes, the techniques and processes that are used may recur in other types of cybercrime. This implies that interventions that could affect carding may also be useful to stop other types of cybercrimes.

3. Having the results (patterns and modus operandi), barrier models tell us which aspects of carding are most effective at enhancing carding prevention. Solutions from the barrier models are linked and compared with opportunity-reducing techniques that will help authorities and organizations with carding prevention.

This way, one can effectively apply an intervention. When it becomes clear what aspects are important and where intervention seems most effective using barrier models, the police and relevant actors can make the right policy choices. The outcomes of this study and solutions of the barrier models could support the tasks and objectives from the police and in particular NHTCU. The barrier models will contribute to achieving objective one and two. Next to developing barrier models, the solutions from the barrier models are linked and compared with

opportunity-reducing techniques by Clarke that authorities and organizations can use in their 'battle' against the discussed types of carding. By linking and comparing the solutions from the barrier models with the opportunity-reducing techniques by Clark ed., it becomes clear on what techniques the authorities or organizations ('battling' actors) should focus. In accordance, the techniques are linked with authorities or organizations who should execute them.

Briefly, the objectives are:

1. *Describe carding as a type of cybercrime*.
2. *Develop an intervention point of carding*.

To fulfil the first objective, three questions are formulated:

1. *How is carding organized and what are their sub processes?*
2. *What are the actors in the main processes?*
3. *To what extent do the developed models correspond with information and expertise from the National High Tech Crime Unit?*
4. *Which opportunity reducing-techniques by Clark ed. are the most relevant to the prevention of different types of carding by authorities and organizations?*

The first question focuses on the criminal process and the modus operandi of carding. With help of the descriptions and realized models, the organization of carding is portrayed as accurately as possible. The second sub-question lays the focus on what model can be used to describe the processes within carding best. Question three focuses on testing the models. It is necessary to verify and review the accuracy and completeness of the developed models. Eventually, question four focuses on the opportunity-reducing techniques of Clark ed. to see what techniques are most relevant for authorities and organizations that deal with carding.

Once objective one is fulfilled, several intervention points of carding can be developed.

Apart from that, the main objective of this study is to find patterns in the criminal process of carding so the modus operandi becomes clear. Therefore, a central research question is necessary:

To what extent are patterns recognizable in the criminal process of carding?

Below, the definitions related to carding and to this study are itemized. These are based on existing sources. It is necessary to understand some of the definitions that are used later on to understand descriptions and models.

1.2 Definitions of carding

This paragraph describes the definitions related to carding. These definitions mainly stem from the High Tech Crime - Crime Pattern Analysis sub report of the Netherlands' Police Agency (2009).

Carding can be seen as a combination of cybercrime and high tech crime. Cybercrimes are crimes that are related to internet or computerized methods. The Netherlands' Police Agency, defines cybercrime as 'punishable activities in which the use of automated operations for the processing and transfer of information has a substantial part'. The term 'automated operations' includes computers, cell phones, credit cards and other forms of advanced technology (the Netherlands' Police Agency, DNR, 2009, p.12).

High tech crime is understood to mean specific forms of cybercrime that can be qualified as forms of serious and organized crime. According to the 'Research and Documentation Centre (Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC))', high tech crime is an umbrella definition that is used when we refer to the use of ICT for committing criminal acts against persons, property, organizations or electronic communications networks and information systems (Van der Hulst & Neve, 2008, p.39).

Cybercrime is seen as the use of computer techniques to commit 'normal' crime, for instance stealing money from citizens or banks. However, this occurs with the uses of advanced technologies, which is a feature of high tech crime. Therefore carding can be seen as both cybercrime and high tech crime.

To understand carding better, the concepts of the carding techniques that are used are discussed below.

Phishing is the process of tricking or social engineering an organization's customer into imparting their confidential information for misuse. In other words, phishing is the process that causes computer users to give away personal information (Ollman, 2004; p.3). To show the extent and severity of phishing, Rasmussen and Aaron (2010) note that at least 48,244 phishing attacks occurred in the first half of 2010 worldwide. By 'attack', they mean phishing sites that target a specific brand or entity (Rasmussen and Aaron, 2010) However, they do not mention whether or not these phishing attacks are successful or not.

When phishing occurs, a computer criminal acts like a reliable and legitimate actor to steal personal information through email, SMS, voice over IP (VoIP) or spam. The messages are made in such a way that they look like they come from legitimate and trustworthy actors. In doing so, computer criminals make use of social engineering.

Phishing cannot occur without the concept of social engineering. Social engineering is an attack technique that abuses the social psychological behaviour of a computer user. A user of a computer or the internet is persuaded to click on something, not knowing that they start a program or open a fraudulent website or transfer personal information (the Netherlands' Police Agency, DNR, 2009, p.23-29).

Skimming means obtaining credit card information and additional information to make payments on behalf of the victims. So-called skimmers copy magnetic strips from bankcards

and credit cards using hardware modifications. Keyed codes - e.g. PINs - are traced by using cameras or an magnetic strip reading device inside the card slot of an ATM (Scarafile, Cappio, 2007) or being traced with an "overlay". An overlay is a fake keyboard on top of the existing keyboard of an automated teller machine (ATM) that can trace the keys that are used and store them (the Netherlands' Police Agency, DNR, 2009, p.75)

Hacking is defined as the intrusion into a computer system. Once a hacker gains access to a computer, data mining techniques are used to collect or trace useful and sensitive information and keystrokes (the Netherlands' Police Agency, DNR, 2009, p.72). Although hacking is a broad concept and several methods are possible, in relation to carding, it is about gaining access to financial information by computer criminals and using that information (the Netherlands' Police Agency, DNR, 2009, p.31).

After collecting information by using these techniques, the information is used to steal money (apart from exceptions like selling or trading). The process of using that information to steal money is cashing. This is discussed in the following paragraph.

Cashing as a collective term - a process of carding - can be divided into four different types (Peretti, 2009, p.390-393) of methods. The following definitions are summarized:

- **Carding Online** refers to the use of stolen credit card information to purchase goods online (no need for counterfeit bankcards).
- **In-store Carding** is making a false credit card encoded with stolen account information, which is used in a physical location (store).
- **Gift Card Vending** includes the purchase of gift certificates from retailers in physical stores using counterfeit credit cards. Then criminals sell these cards for a percentage of their true value.
- **Cashing** refers to obtaining money instead of goods and services through unauthorized use of stolen financial information.

Instead of using the stolen information, criminals can also sell or exchange these with the use of carding forums.

Carding forums are meeting places (convergence settings) where tutorials, software and stolen information are exchanged or sold. Indicated with the term trafficking. The purposes or intentions according to Peretti (2009) of a carding forum are informing, helping, teaching and creating the possibility to trade or offer stolen information or resources to make carding possible.

Crime scripts are useful analytical tools to look for behavioral routines. It ensures that knowledge is being generated, organized and systemized about the procedural aspect and requirements of a crime. It organizes knowledge about people and events (Cornish, 1994, p.151-158). Crime scripts are very handy when studying processes (activities and actors) and will be used since no other method suits.

Situational Crime Prevention is according to Clark (1997) 'proceeding from an analysis of the circumstances giving rise to specific kinds of crime, it introduces discrete managerial and environmental change to reduce the opportunity for those crimes to occur'. Situational crime prevention emphasizes the settings and occurrence of a crime and aims to make criminal actions less attractive to offenders and reduce the opportunities for different crimes (Clark, 1997).

Opportunity-reducing techniques are one of the key elements or components of situational crime prevention. Apart from the situational crime prevention, Clarke, Homel (1997 mention twenty-five opportunity-reducing techniques that can be seen as techniques that contribute in situational crime prevention. These can be used later in relation to the solutions mentioned in the barrier models. The techniques are presented below in table 2. Each of the twenty-five opportunity reducing techniques mentions two random examples.

Increase the effort	**Increase the risks**	**Reduce the rewards**	**Reduce provocations**	**Remove the excuses**
1. Harden Targets immobilisers in cars anti-robbery screens	***6. Extend guardianship*** cocooning neighbourhood watch	***11. Conceal targets*** gender-neutral phone directories off-street parking	***16. Reduce frustration and stress*** efficient queuing soothing lighting	***21. Set rules*** rental agreements hotel registration
2. Control access to facilities alley-gating entry phones	***7. Assist natural surveillance*** improved street lighting neighbourhood watch hotlines	***12. Remove targets*** removable car radios pre-paid public phone cards	***17. Avoid disputes*** fixed cab fares reduce crowding in pubs	***22. Post instructions*** 'No parking' 'Private property'
3. Screen exits tickets needed electronic tags for libraries	***8. Reduce anonymity*** taxi driver ID's 'how's my driving?' signs	***13. Identify property*** property marking vehicle licensing	***18. Reduce emotional arousal*** controls on violent porn prohibit paedophiles working with children	***23. Alert conscience*** roadside speed display signs 'shoplifting is stealing'

4. Deflect offenders street closures in red light district separate toilets for women	***9. Utilise place managers*** train employees to prevent crime support whistle blowers	***14. Disrupt markets*** checks on pawn brokers licensed street vendors	***19. Neutralise peer pressure*** 'idiots drink and drive' 'it's ok to say no'	***24. Assist compliance*** litter bins public lavatories
5. Control tools/weapons toughened beer glasses photos on credit cards	***10. Strengthen formal surveillance*** speed cameras CCTV in town centres	***15. Deny benefits*** ink merchandise tags graffiti cleaning	***20. Discourage imitation*** rapid vandalism repair V-chips in TV's	***25. Control drugs /alcohol*** breathalysers in pubs alcohol-free events

Table 2. Situational crime prevention. Techniques for reducing the opportunity for crime by Clarke and Cornish (2003).

1.3 Limitations of previous studies

The government and authorities in general, seem to be struggling with cyber criminality. Currently, authorities try to battle carding by compiling computer crime squads (Garfinkel, 2002), tearing down active carding forums, informing people to check their accounts frequently, investing in computer and/or card security (such as antivirus software), formulating cyber laws that may stop cybercrime (Ayaz, 2006) and help law enforcement or developing innovative tools that make carding more difficult.

Unfortunately, even with the written literature and advice of today that is not enough to stop carding. Therefore, the struggle remains.

Methodology

2.1 Relevant articles

This study mainly uses online news articles to describe and model the processes of carding. This is because it is very hard to find other scientific literature that contains information needed. Most of the literature contains information about theories how to stop carding which are not relevant for this study.

This study searches for patterns and steps in the criminal processes of carding. By comparing the online news articles and their contents, patterns are found by underlining important recurring terms and appropriate crime scripts are modelled. Steps are the activities that, once they are put together show the modus operandi of processes of carding. In addition, patterns are those actions or activities that emerge each time a carding scheme or process related to carding takes place and can also be found in the modus operandi. The modus operandi can,

for instance, be divided into actors or activities. Both activities and actors are discussed. The good thing about online news articles is that they tell something about what happened, what general actions and activities are taken or what actors are involved.

This study looked what authors of the articles do and do not tell people. The question to answer is: to what extent do the authors of the articles mention the activities of a carding process (for phishing and skimming only). Therefore, the used online news articles are compared mutually in this study. By putting the results in SPSS (software for statistical data), the collected data for frequencies and correlations between variables can be tested. When speaking of correlations, perhaps, the connections can be drawn between techniques (by computer criminals) and the amount of money that is involved or the connection between the amounts of money and how money is cashed. This way, statements can be made about patterns by using the quantitative outcomes.

This study creates models of two elements of processes of carding. First, the activities of a process of carding get attention. For example: phishing. A second model shows us the involved actors, related data flows (resources, goods, services and connections). Each process is described and modeled on its activities and actors involved and can be seen as a crime script. By making models of the existing patterns and crime scripts data is recorded in an orderly way. The models are nothing more than summaries of what is found in the online news articles and other literature.

In this study, mainly phishing and skimming will be broadly discussed (attacking techniques). Other processes such as carding forums, money mules e.g. that fall under the sections cashing and trafficking are discussed in outline but less intensive, due to the absence of sources, in particular online news articles. Verification of these other processes is not possible or too difficult and therefore omitted. In addition, where possible, figures will be presented.

Above will be implemented in the analysis section of this study. Subsequently, the results discusses the patterns and the verifying, and barrier models are presented.

2.2 Studying articles

Once the online news articles are categorized and saved, the analyzing starts. For actual analysis, the articles are printed and bundled. Once printed and bundled, useful information was underlined. The online news articles eventually got summarized and patterns are written down. Here the most important and recurring terms (patterns) are sketched in a software tool called Mind Manager. Mind Manager helps to order the activities and connections in the right sequence. This is useful because there are a lot of possible combinations and sequences possible. Asking experts of NHTCU and specifically searching for other literature help manage the sketching of models. In addition, it is important that the models must be summaries of what is stated in the online news articles. Eventually the sketched models are put in MS Visio, which organizes the models better.

These online news articles are found by using several queries. The used queries include carding, phishing, skimming, identity theft and card fraud. After applying this, news related websites encounter with an online database containing more online news articles of the same subject. Used websites are: securityfocus.com; searchjustice.usdoj.gov; cgisecurity.com, curc.org.

To prevent this study from being 'out-dated', most gathered online news articles are dated between 2008 and 2010. Subsequently, the gathered data is tested for its uniqueness. The articles that discussed arrest, charges or suspects are saved and categorized per subject. A distinction is made between subjects such as phishing, skimming, carding or forums.

The Internet provides lots of articles concerning arrests, charges and suspects. Due to a limited time, the search stopped after gathering 20 or more online news articles related to phishing and skimming. Other processes like the use of carding forums, money mules e.g. are less often mentioned in online news articles. A limitation of 20 does not apply to these other processes. See paragraph 2.5 for a better understanding.

During modelling the processes, each of the treated criminal process of carding is presented to an expert of the NHTCU with a good understanding of the processes. However, this can bring subjectivity, as the view of one expert is not per se objective. Each expert can have his own vision of a discipline. However, testing models for its correctness can hardly bring subjectivity with it, because the expert can only answer by saying the model is correct or not correct. In addition, no other testing methods seem available.

A first look by the employee of NHTCU resulted in the remarks that some activities are missing and some terms like cashing or carding e.g. could be wrong interpreted and need to be reconsidered. As mentioned before, the results of this study leave room for a considerable amount of variation, comments and complements.

After gathering the online news articles, the concepts and definition of carding are compared with the online news articles to see whether or not the online news articles and authors have an understanding of carding. The titles of the articles are for example: '38 Individuals in US and Romania charged in two related cases of computer fraud involving international organized crime' (Department of Justice, 2008) or 'Six indicted in Colorado on bank fraud charges'.

In relation to developing models, the bottom-up approach is used. This means that models are sketched from a particular described scenario in an online news article and expanded when additional information is found. This continues until they reached the desired results so they can be tested and verified by experts.

In addition, the theory of a crime script is studied. The basics of a crime script are used for developing and describing processes of carding. Just as the models and descriptions, later on in this study, crime scripts focus on activities and actors (as variables) and come in very

handy when studying processes (activities and actors) and will be used since no other method suits.

Besides the theory of a crime script, situational crime prevention and relevant techniques that reduce the opportunity to commit a crime are studied to expand this study with information that helps authorities and organizations to prevent crimes and thus carding. The techniques that can be used and authorities or organizations in relation to carding are discussed in part two of this study, the barrier model.

This study looked what authors of the articles do and do not tell people. The results of SPSS are put in a chart which includes the activities (variables) of a carding process, the number of treated articles (N) and the sum. The values of the variables are: 0 = not treated in the articles and 1 = treated in the articles. Then there is the variable conscious or unconscious, which differs. The values are 0 = unconscious and 1 = conscious. To give an example of how the table is categorized:

Activity	N	Sum

Figure 1. Table example

Eventually, barrier models can be made based on the analysis. This is discussed in paragraph 2.4

2.3 Verifying

In-depth interview was held with an expert from NHTCU who has certain expertise and experience and who is involved in creating relevant police files of the NHTCU. The interview was held on 1-9-2011. Purpose of these interviews was to 1) understand which elements are missing in the criminal process around carding and 2) understand if the connections between activities or actors are correctly documented. The remarks are incorporated into the text where previous stated information come short or is wrong. Using interviews is a great opportunity to further resolve ambiguities or to confirm results.

Before taking interviews, it is necessary to derive and store information properly. Information from interviews can be difficult to record because there may be interpretation. Interviewers must be neutral (Babbie, 2007, p.265-280). The extracted information has to remain objective. An issue of conducting interviews is that the interviewer himself handles information. This information is often affected by subjectivity or interpretation and affects thus reliability and validity.

2.4 Barrier models

To make sure the construction and lay out of barrier models matches with the information of this study, the activities are categorized. Once the activities are categorized, related actions, involved actors and measures can be add to the categories to create a better understanding and

interpretation of the mentioned activity. The used formats for a barrier model are based on examples of the police and NHTCU.

2.4.1. Opportunity-reducing techniques

After finishing the barrier models, the solutions can be derived from these models and linked and compared with the opportunity-reducing techniques by Clark ed. Table 2 on page 6 and 7 concerns twenty-five techniques but only five main categories. The solutions stated in the barrier models are categorized according to the five main categories, named rational choice categories by Clark (1997). This way it becomes clear which of the five categories are most important in battling and preventing phishing and skimming. Organizations and authorities can benefit from these outcomes, because they know where to put the focus on.

2.4.2. 'Battling' actors

Apart from this, the different solutions derived from the barrier models are linked with 'battling' actors. 'Battling actors' are organizations and authorizes that play a key role in preventing and stopping carding. These actors are introduced later in this study. By linking these actors with the solutions derived from the barrier models it becomes clear which actors can implement the different solutions and are the designees to execute or implement the solutions. No theories or methods are used with linking actors to solutions.

2. Data

The present study is based on a number of sources, literature and articles.

3.1 Literature

White papers, theses, internal records, published (news) articles, forums, books and databases of the University of Twente are used to get an understanding of carding. Information from the NHTCU of the Netherlands' police agency could be used as well. Apart from giving a better understanding of carding, the (scientific) literature and information from the NHTCU that is useful can underpin the research empirical or complement the found information in the online news articles.

3.2 Online news articles

Online news articles on the Internet are used to search for patterns and steps in criminal processes of carding. The online news articles are about arrests, charges and suspects related to processes within carding, such as phishing or skimming.

3. Analysis

The analysis is split into part one and two. In part one, the data related to phishing and skimming encountered statistics. Here the study looked what authors of the articles do and do not tell people. This is analyzed and the results of this analysis are presented in table 2.

Basically, the questions: how many articles mentioned the variables of phishing and skimming?

In part two, the crime scripts of carding (‘carding’ script) are analyzed and the results are put on paper as descriptions or models.

Part one: data statistic

Below an analysis chart is presented which include the activities (variables) of phishing used in online news articles, the number of treated articles (N) and the sum of how many articles mentioned the different variables. On top of that, the sum of whether the articles mention conscious or unconscious attacks is included.

Variables of phishing used in Articles for matching	N	How many articles mentioned the different variables?
Preparation of a phishing attack	13	6
Target.mentioning	13	11
use.fake.email.account	13	0
get.phishing.software	13	5
get.server	13	4
obtain.email.adresses	13	0
buy.phishing.software	13	4
create.phishing.software	13	5
use.fake.website	13	12
hosting.website	13	6
mention.actual.attack	13	10
spam.email.people	13	8
get.past.spam.filter	13	1
convince.people	13	5
victim.directed.to.fake.website	13	9
victim.download.file.containing.malware	13	2
get.information.from.victim	13	12
verification.code	13	1
cashing.selling	13	7
Valid N (listwise)	13	
Conscious chosen victims	13	10

Table 3. Descriptive statistics of phishing.

This analysis is only being made for phishing. This is because phishing has more variances possible in activities then skimming and thus easier to analyze. Looking at skimming as a process (which is abstracter then phishing), the accentuated activities in our models are all named in the articles and seem logical.

Sub conclusion Only in phishing a variety of variables is recognized. Skimming doesn't show any differences. That means that all variables are relevant and each activity is equally important.

Part two: The carding script

Within carding, there is a distinction to make within the process of stealing and the process of using information. The second process of using information can be divided into trafficking and cashing (trading) with the use of forums and messaging tools.

When asked to explain the processes within carding, it is assumed that carding all starts with picking out a victim and gain entrance. Once victims are picked and entrance to personal information is gained, the following process of stealing information starts.

It is assumed that when an attack occurs other computer criminals can be involved. The stolen information can be advertised and sold (trafficking) or directly used by the computer criminal himself. Eventually, the person who possesses the information will use it to gain cash. Here four different cashing methods can be mentioned. These include cashing, in-store carding, gift card vending and online carding which are all mentioned by Peretti (2009, p.390-393).

Besides online carding, a computer criminal must have counterfeit cards to cash. That also depends on what attack techniques are used and what information the computer criminal catches.

Eventually, money laundering may take place, trying to erase any possible evidence. Taking this view in account, the following model shows an example of the activities of carding. The model below is based on what is discussed above. The numbers in the model indicate the paragraphs and subjects that will be discussed.

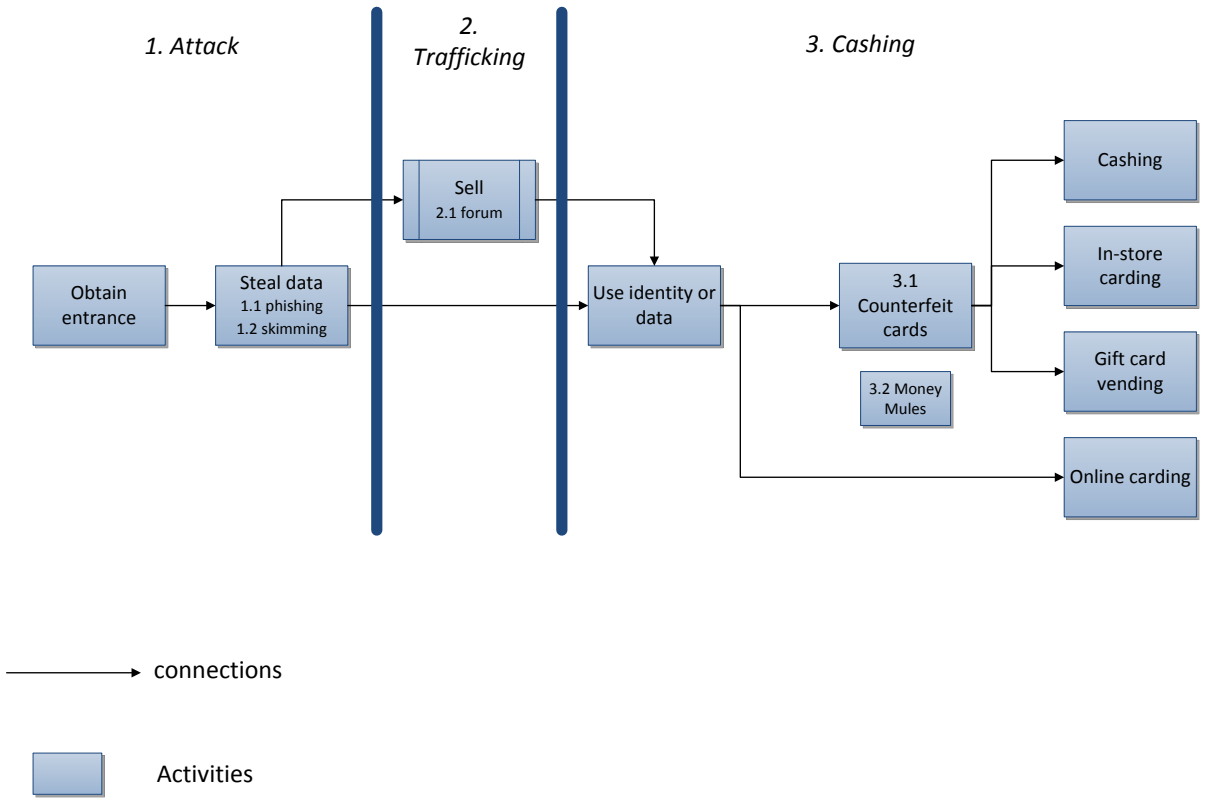


Figure 2. The carding script (developed by author).

This model shows three different steps that are separated from each other by thick lines. Each sector stands for a different overall process within carding, namely the use of attacking techniques, the possible presence of trafficking and eventually cashing.

4.1 Attacking techniques

4.1.1 Phishing

The focus at phishing lies on using e-mail but nowadays other messaging tools can be used to trick, lure or attack people. The available online news articles on phishing however only spoke about phishing by e-mail. The activities can be divided stepwise. See figure 3a for a better understanding. The activities are discussed below.

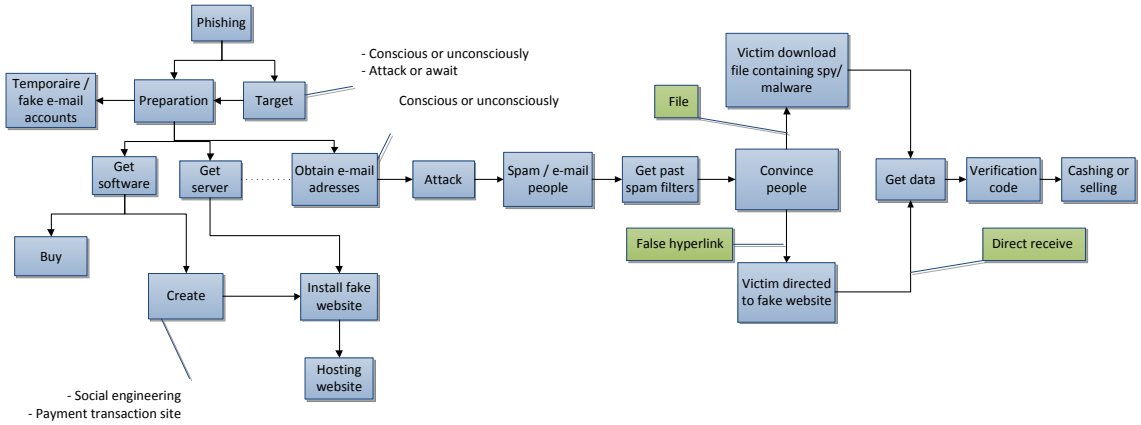


Figure 3a. Activities related to phishing.

4.1.1.1 Activities

1. 1. Before a phishing attack occurs, preparation is needed. A temporary and fake e-mail account is necessary to decrease the risk of being caught. However, just a fake e-mail account does not give someone the opportunity to commit a phishing scheme. Some software is needed too. Phishing kits and pre-built websites can be bought from other criminals, which look just like realistic ones (Goodin, 2008; Buchanan, 2006). These phishing kits support a future criminal making false and mimic websites. These fake websites are used to lure people and convince them that the websites or received files per email look like they come from a legitimate and trustful source, by using social engineering. Such websites usually are a copy of a payment transaction site (Goodin, 2008; Buchanan, 2006). A phisher can also make a fake website himself (Goodin, 2008).

2. Another essential part of the preparation is using a server. A server is basically a computer that plays a supportive role to other computers in a network (Van Dale, 2012). A criminal can use bulletproof hosting for example (McMillan, 2009). Bulletproof hosting is using a server and related (rented) services to send spam and thus e-mail that according to Krebs (2010) ‘are largely immune from takedown requests and pressure from Western law enforcement agencies’. Another option is to hack a server. This means a criminal get access to a server and the abilities to use the server. Created fake messages and websites will be put on that server and hosted for limited time.

   There are several ways to obtain e-mail addresses of victims that are chosen specific or at random. First, hacked servers could be used (Department of Justice, 2006). Second, e-mail addresses could be gathered by searching on the internet for organizations that contain contacts (at ‘Kamer van Koophandel’ for example). Third, a computer user could buy a list with e-mail addresses (Brownlow, 2010). Finally yet importantly, a phisher could make use of a botnet. A botnet exists when several computers contain a program that independently execute software, are connected with a central server and

can therefore be centrally controlled (the Netherlands' Police Agency, DNR, 2009, p.191-192). The victimized computers send e-mails, other messages or malware without further notice. The gathering of e-mail addresses depends on the creativity of phishers.

3. A computer criminal picks a victim consciously or unconsciously. However, there are situations where there is no target selected at the beginning of the scheme. If this is the case, a target will be picked later on when a phishing attack is made possible.

4. After e-mail addresses of computer users are collected legally or illegally and victims are chosen, the attack can take place. The phisher then sends e-mails, which is a form of spamming. These e-mails contain tools which a phisher uses to collect information. When sending e-mails, it is important that a fraudulent e-mail - containing fraudulent files or a link to a fraudulent website - get past any spam filters.

5. The task is to convince people that the e-mail can be taken seriously, that the content of such e-mail is reliable and legitimate. This is the most critical moment. People are just one button away from being victimized or not. A user who downloads an attached file, not knowing that the file contains forms of malware or spyware that will steal information. Alternatively, a victim clicks on a hyperlink that is sending him to a fake website, which is under control of the phisher. The victim must here fill in crucial information - PIN, Card number and so on - which the phisher can use to cash money. It is necessary that a phisher also finds the verification codes that can be used to complete transactions. These codes differ each time an online transaction is being made.

   It is assumed that all four cashing methods (cashing, carding online, in-store carding and gift card vending) are possible. Furthermore, it is assumed that individuals or small groups of phishers see no reason to trade or sell their stolen information as no online news article or other literature mention this.

4.1.1.2 Actors

The people involved and the information flows among them will be discussed here. Figure 3b shows what actors and information flows are related to phishing.

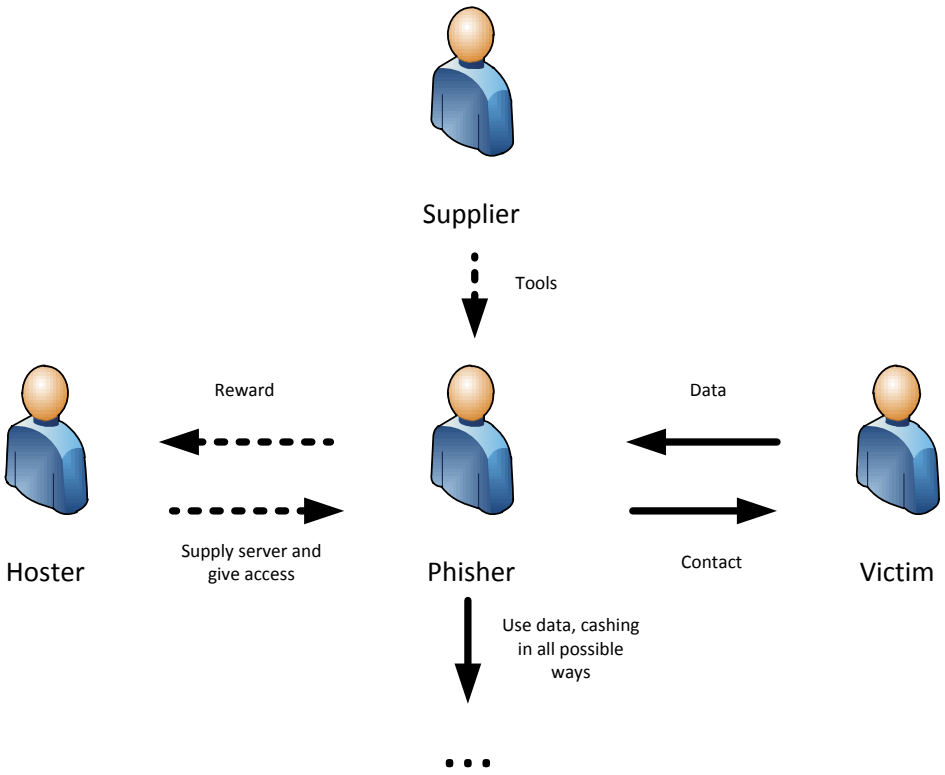


Figure 3b. Actors and information flow related to phishing.

Because some preparation for phishing is needed, several suppliers and server hosters may be involved. Besides suppliers and hosters, there are no other actors involved. The phisher attacks a victim possibly with help of suppliers and hosters, get information if he is lucky and then uses that information for cashing. Phishing can be summarized with a few essential aspects, namely attack, target, preparation, convincing and stealing. However, it requires a lot of skills and energy to get things done.

4.1.2 Skimming

A second attacking technique is skimming. Skimming differs with the other attacking techniques because information is obtained by devices instead of breaking in using computers. These devices can be purchased or made. The activities can be divided stepwise. See figure 4a which presents the activities related to skimming.

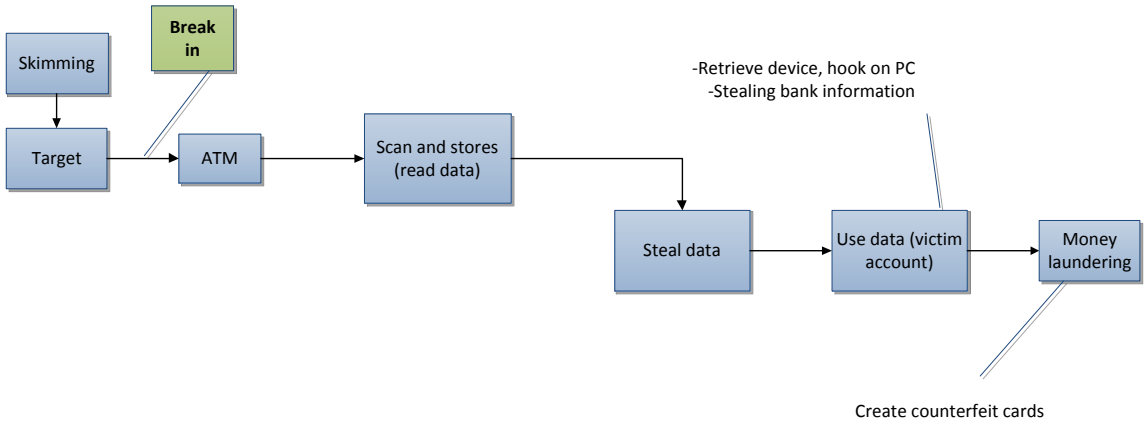


Figure 4a. Activities related to skimming.

4.1.2.1 Activities

1. It starts with picking a target (see figure 4a). This could be an ATM in a highly populated area (Ambrose, 2010). Targets such as banks, stores, restaurants or other places can be picked, where people pay using ATM's, skimmers make use of these ATM's to gain information.

2. 1. When gaining information from stores, restaurants and such, the skimmer first must infiltrate (gain access) a target and place a card reading device on the target's ATM. This mostly occurs in stores. To get inside a store, a skimmer may convince or ask people such as employees - willingly or unwillingly - to place a device on a store's ATM. After information is stored on the device, the device gets retrieved. The skimmer receives money and people or employees may get a share of that money for participating in the skimming act (Wesh, 2010).

   2. A slightly different method is placing a device on an ATM at a bank or gas station at to scan, copy and store the information of the magnetic strips of credit cards from innocent customers at night (Sugimoto, 2011). This scenario occurs most often. Installing devices or card readers happens within a few minutes. Moreover; generally more than one person often does the installation of a device. A second person looks if things seem safe to install such device (Duecy, 2010; Sugimoto, 2011). To know the customers PIN, a small pinhole camera or a keyboard overlay is installed which functions as a key logger device. It scans and stores the typed numbers.

3. After collecting information from stores, restaurants, banks or gas stations the skimmer - disguised - returns to the ATM and collect the devices, which contain all necessary information which the skimmer can use to cash or sell. This can be within a few hours (Duecy, 2010) or several months (Vijayan, 2010). However, returning to an ATM to pick up the devices is not required. It depends on the capabilities of the devices; some may have wireless capabilities (The Global ATM Security Alliance,

The ATM Industry Association, Fair Isaac Corporation's Card Alert Fraud Manager Service, 2008).

4.1.2.2 Actors

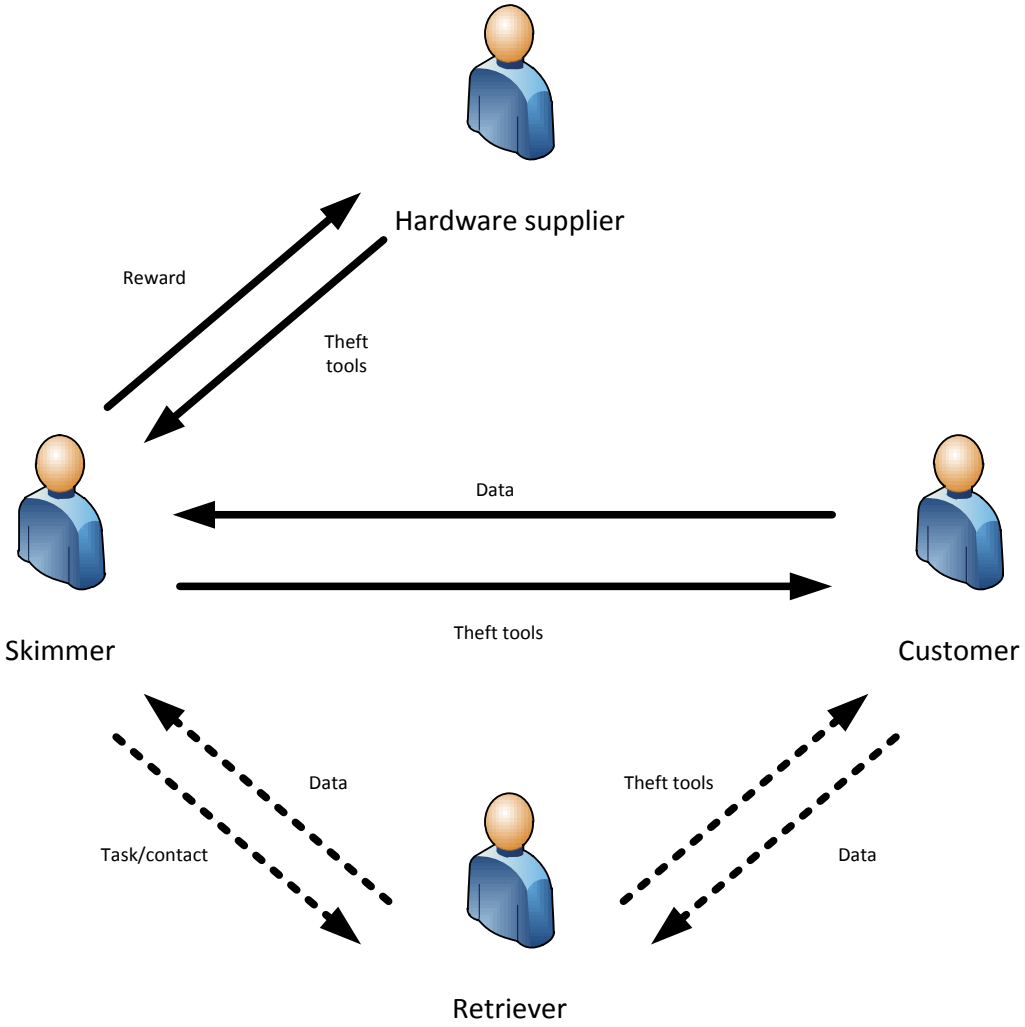


Figure 4b. Actors and information flow related to skimming.

Within the process of skimming, some actors are involved as well as is shown in figure 4b. When picking a store or restaurant, most of the time this is commissioned to an employer or someone who has access to the store ATM. A skimmer can also infiltrate a store or other organization by himself. Although, according to the online news articles this is not standard. It is easier for a skimmer giving the task to an employee to infiltrate.
Furthermore, there are hardware (skimming devices) suppliers who, obviously, supply the skimmer with all the necessary theft tools like devices, card readers, small cameras or keyboard overlays. Here too, the skimmer can do it himself, but again, it is a lot easier or cheaper to get someone else who supplies theft tools.

Eventually, personal information (PIN, credit card information and verification codes) will be taken from a customer or victim using theft tools. A skimmer can use information to make counterfeit cards and use these cards to withdraw money from an ATM or sell the information. A retriever may participate by using the victim's information to withdraw money from ATM's with fraudulent cards and then give it to the skimmer for a possible small reward.

Another possible skimming scenario that can be named but is not mentioned by the treated articles is that a skimming scheme can take place on the street where skimmers convince - with false pretenses - or force young people to hand over their credit cards and pin-codes. With this payment information, money can directly be withdrawn from ATM's (de Gelderlander, 2011). This is an example to show that the results of this study can be complemented.

4.2 Trafficking

4.2.1 Selling

An important part of trafficking is selling stolen personal information. A criminal can decide to keep the information for own use or sell it to others on diverse messaging tools. The trafficking and selling happens through the use of messaging tools. The most used messaging tools are forums, also known as carding forums. First the use of carding forums will be described. After that the use of other messaging tools that are also used for trafficking and selling are discussed.

4.2.1.1 Carding forum

According to Peretti (2009), criminals who are engaged in carding processes often use forums to contact others for help, services, software (tools), tips and so forth.

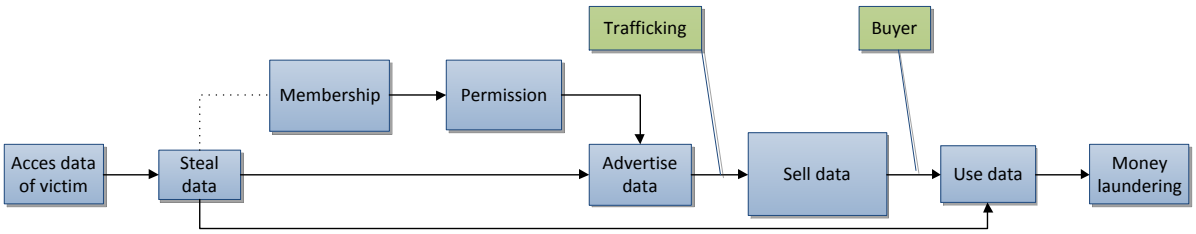


Figure 5a. Activities related to the use of carding forums.

Within the processes of a carding forum, several activities can be highlighted. These are put in figure 5a. Shown in figure 5a, the use of carding forums starts with getting access to personal information from a victim and stealing that information. The criminal can choose to use the information directly by him or advertise and sell the information. When a criminal wants to

sell his information for ‘clean’ money, he must have a membership on a forum and permission to advertise his information.

To get a membership, new members are being reviewed and supervised till founders and reviewers are convinced enough to welcome new members and let them do their thing (selling, trading, questioning e.g.). Once someone is interested in the offered information, the member will contact the vendors.

The deal takes place outside the carding forum using messaging tools and other convergence settings (See paragraph 4.2.1.2). Once information is sold, the criminal that provides information get money and reputation from the buyer. Like in most forums, the members may give other members positive or negative scores which indicate or result in several achievable statuses within a forum.

The time and actions between advertising and actual selling is called trafficking. Besides a place where information can be sold, the carding forum has other purposes.

- Selling or sharing software.
- Provide information and tutorials. A carding forum offers a good opportunity to learn from each other or exchange information.
- Tips and hints (*experience).* Based on experience, members can give advises or tips to people who want to commit a cybercrime. It is another learning process. In addition, members can give each other hints, such as sharing knowledge about a weak protected bank or network.
- Other facilitating services

Carding forums are well organized because there is a recognizable hierarchy. Here is a simple overview of the (hierarchical) organization of a carding forum that can be derived from Peretti (2009, p.383). Figure 5b is based on the statuses on a carding forum.

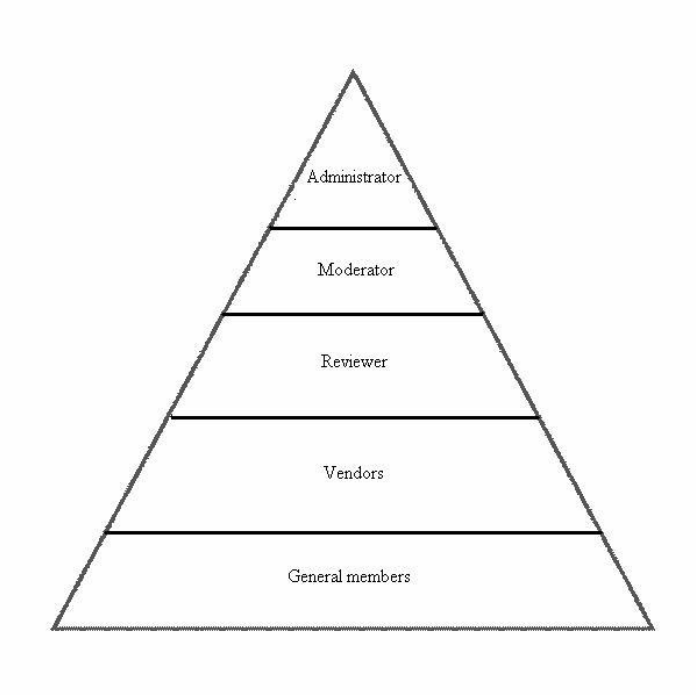


Figure 5b. Organization chart of a carding forum (modified by author and based on Peretti. 2009, p.383).

The definitions in the triangle are those that Peretti used to indicate the statuses within a carding forum.

4.2.1.2 Messaging tools

Nowadays there seems to be a shift going on in the cyber underground from forums to other messaging tools where criminals meet each other and where the actual selling occurs (as mentioned in paragraph 2.1). This is partly due to the intervention of the police. Here, the traffic and selling processes that can be done using messaging tools and other convergence settings are described.

Looking more specifically on the use of messaging tools and the actors involved, it can be said that once a vendor (seller) or person is contacted by an interested general member or person they negotiate outside the forum, using messaging tools such as ICQ, YAHOO, MSN, AIM, IRC, JABBER or chat rooms (multiplayer game servers). On these messaging tools, carders can easily contact each other and negotiate. The information flows that occur due to these conversations contain mainly information and money. When this occurs, trafficking and selling of illegally obtained information occurs.

4.3 Cashing

Finally yet importantly, the process of cashing is analysed. According to all relative online news articles, the four different types of cashing according to Peretti (2009) seem valid. All four types of cashing did occur in the treated online news articles.

4.3.1 Counterfeit cards

In this paragraph, the making and use of counterfeit cards is discussed. For three of different ways (cashing, gift card vending and in-store carding) of cashing a counterfeit card is necessary.

Several tools are necessary to make counterfeit cards. Buying or getting tools to make counterfeit cards is no hard task. There are even companies who produce skimming devices when an order is given. Companies in that manner only care about supply and demand. Therefore, it is plausible that often services of others are used. For making counterfeit cards at least the following components are needed (CTV Montreal, 2010):

- Computer (encoder)
- Information
- Printer
- Tools to assemble ATM cloning devices
- ATM parts
- Camera or key logger device (overlay)
- Card readers
- Plastic cards with magnetic strips
- Clothes for disguise

Once creating counterfeit cards - by the criminal or by other hardware suppliers - and the PIN-code is familiar, the counterfeit cards are distributed. Criminals can sell these counterfeit cards, give them to runners or cashiers in exchange for a share, or test and use those cards themselves. Runners or cashiers are actors in service of a criminal that try to use the different cashing methods Peretti mentioned. Before criminals, use counterfeit cards themselves, runners or cashiers (Department of Justice, 2008) at stores or ATM's may test the cards.

According to one online news article, runners or cashiers call a special number to give notice of a working counterfeit card (Pankratz, 2010). Once the counterfeit cards seem to work, the card will be used for further cashing by the criminal himself, which means he ask the counterfeit cards back. The cashing continues until 1) the bank account of a victim blocks 2) enough money is gained 3) the situation is getting too risky or 4) obviously get caught. Below, both activities as actors and information flows are presented in figure 6a and 6b.

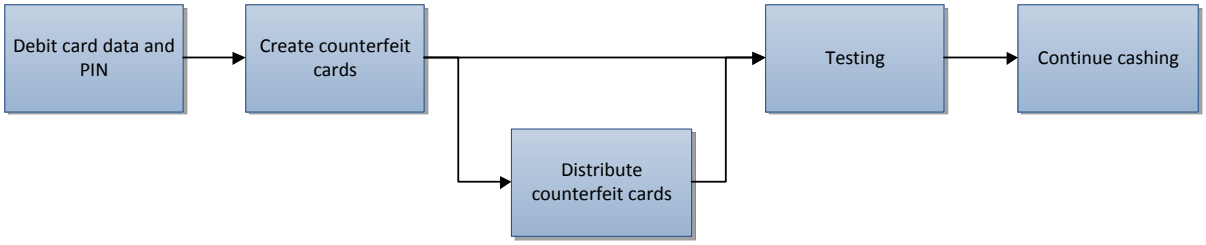


Figure 6a. Activities related to the use of counterfeit cards.

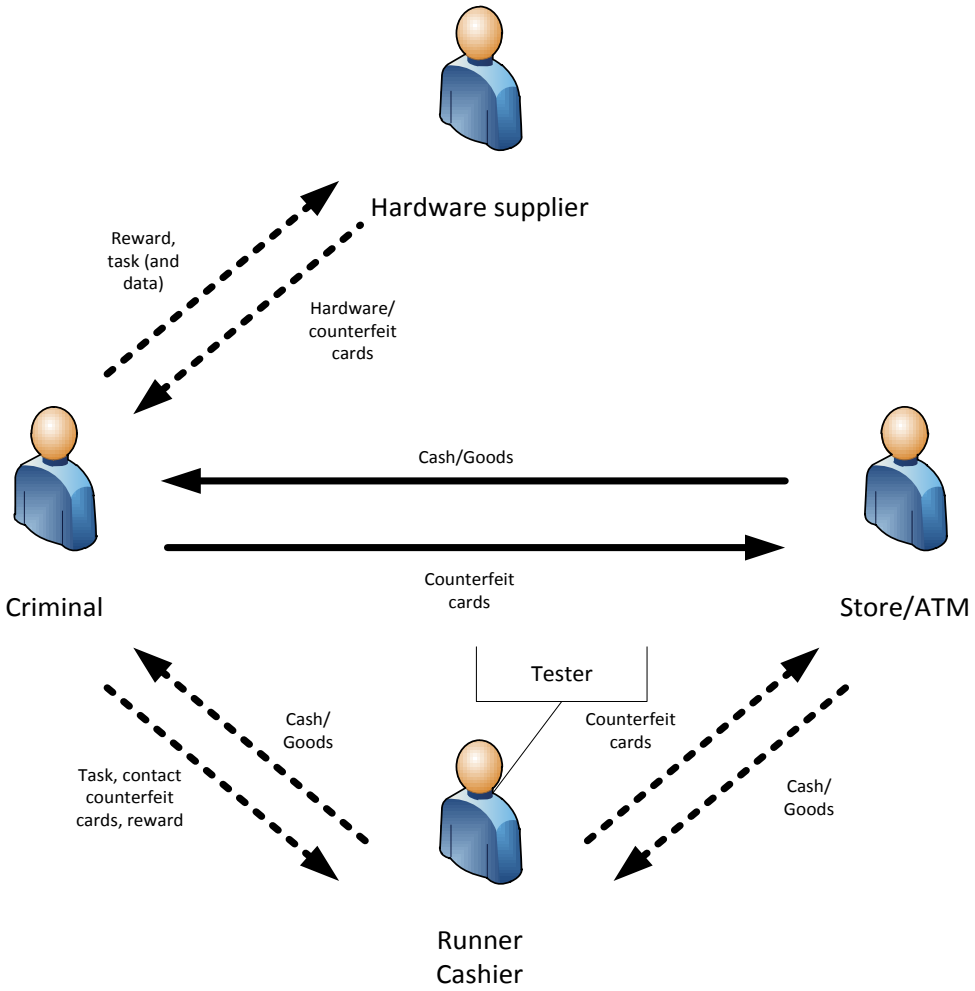


Figure 6b. Actors related to the use of counterfeit cards.

4.3.2 Money Mules

Money mules are people that help criminals (carders) by transferring stolen money from bank accounts. A criminal can recruit people through advertisements who are willing to help by telling and convincing people (falsely persuaded) that they can easily earn money (Banksafeonline, 2008). These people do not know that the money is illegally obtained. (Aston, McCombie, Reardon and Watters, 2009, p.482).

What people have to do is accept money, then transfer that money. In exchange the people may keep a percentage of the money. By using money mules, money is sent between several accounts all over the world to minimize evidence or to wipe out any trail. Here for, money mules can be used to launder the stolen money and eventually cash it (carding online). According to Ken Dunham, director of the Rapid Response Team at iDefense, in Dulles, Va: "*Without the money mule, they (criminals) really can't do anything with stolen credit card credentials*" (Nairane, 2006). Some well-known internet payment systems that may support money mules are Western Union and Web Money.

5. Results

5.1 verifying

Nearly all online news articles mention getting information after a committed crime and the occurrence of an attack. 12 news articles mention the use of fake websites, which points to the fact that in most cases fake websites are used. Ten out of thirteen online news articles mention that the committed phishing crime is a conscious act.

Besides looking at high sums, low sums can also be looked at. None of the online news articles mention the use of fake email accounts or (the method of) obtaining email addresses. This seems logical because the police gave this information. The police gave also the remarks that contaminated emails must avoid spam filters and that verification codes are needed to take money from a victim. This explains the low sums of these variables.

At the same time, using SPSS, the average, maximum and minimum year can be figured out of the published news articles online. Online news articles regarding phishing are dated between 2004 and 2011, with a mean of 2008. The articles related to skimming are dated between 2008 and 2011 with an average of 2010. There are 25 online news articles related to skimming and 13 articles related to phishing.

The purpose of these tables is to show that the treated online news articles are relatively up to date and that the findings can therefore be useful for different purposes.

5.2 the barrier model

Based on the results in part one of this study the barrier models can be assembled. This study gives two barrier models for phishing and skimming.

The constructions of these models are based on examples of the police, which have similar models of other crimes. The advantage of this structure is that the focus can lay on actors and

measures per categorized activity, rather than naming actors and measures of skimming or phishing on a whole, which are two broad terms.

The actors and related activities are bases on the results of this study, where the measures that can be taken are self-administered. In addition, the measures that can be taken are complementary. The barrier models are based on similar models the police have.

The related actions of phishing and skimming are added to the categories to create a better understanding and interpretation of the mentioned activity. The categorized activities are put in circles. Next, the involved actors of the activity are added in particular on top. Last, the measures that can be taken for the named activities are summed at the bottom.

5.3 Barrier model of Phishing

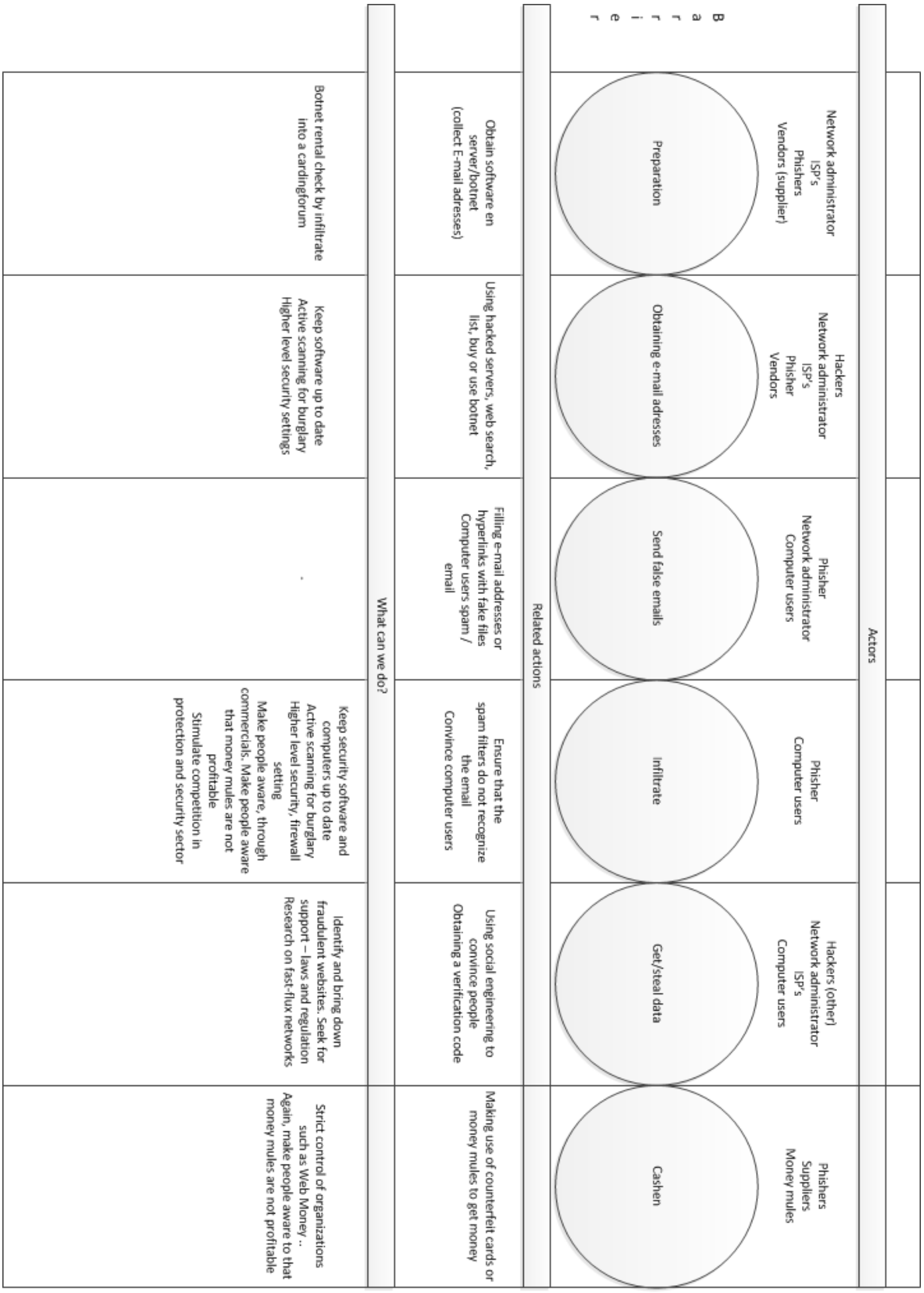


Figure 7. Barrier model of phishing

5.4 Barrier model of Skimming

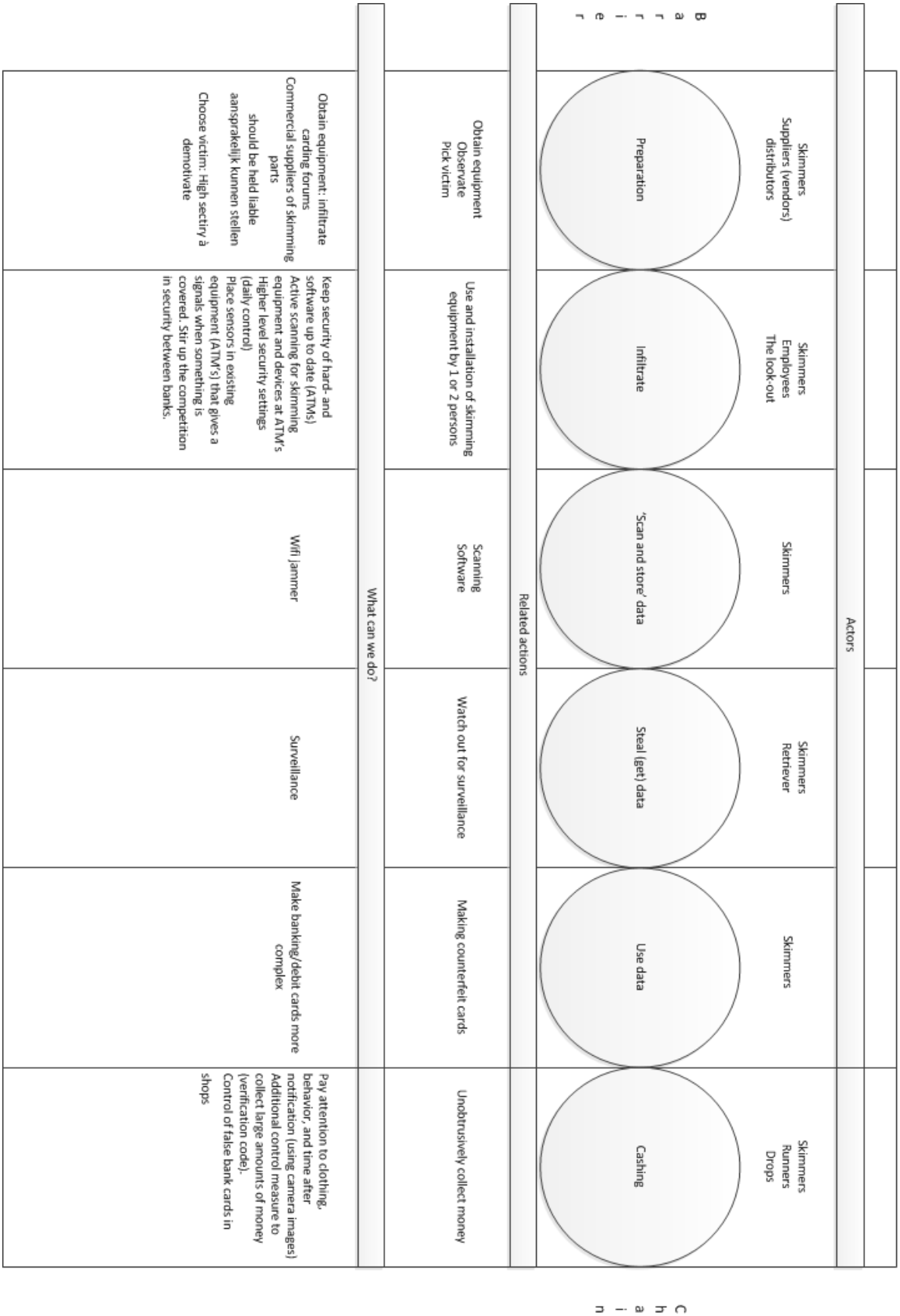


Figure 8. Barrier model of skimming

5.5 Actors in ‘battle’

Apart from these barrier models, several authorities and organization or actors can be or are involved in the ‘battle’ against carding. The most relevant and important actors are discussed below.

The Police

A first relevant actor is the Dutch police. The police is an organization that is created by government and operates in accordance with the ‘politiewet 1993’ (police law). The main goals and tasks are containing public order, and providing assistance to those who need it. This happens in accordance with the rules in force (law and legislation). This means the police have several powers and responsibilities, like the monopoly on - proportional – violence. The police is essential in preventing and stopping crime and therefor worthwhile to mention in the battle against carding.

The National Government

Although the Police is a governmental body, the National Government can be named as a different actor too. Here the focus lies on the political aspect. The National government can briefly introduce new laws, policies, and organizations. It controls the society. Because of the powers of the government, apart of those from the police, that can help in the prevention and battle against carding it is important to mention it.

Bank

Banks are relevant actors too. Dutch banking companies, like ING, Rabobank, ABN Amro ed. can introduce and invent new and better security techniques or methods that can help prevent and stop carding.

Private security

Apart from security derived from the public sector like the national police (public security), the private security sector is also worth mentioning. Several companies like Fox-it and anti-virus organizations focuses on better security by innovating and supplying techniques, policies, services to secure people or authorities and organizations such as banks, police or government. These actors can also prevent and join the battle to stop carding.

Civilians can also be named as relevant actors, but can do little in ‘battling’ carding. At least not at a large scale. Therefore, civilians are excluded in the following paragraphs as ‘battling’ actors.

So far, the most important actors are introduced briefly. The actors above can execute the solutions derived from the barrier models (stated in ‘what can we do’). Apart from these solutions, Clark ed. mentions twenty-five opportunity-reducing techniques that actors can use in their battle against crime.

5.6 Solutions versus actors versus opportunity reducing techniques

Categorizing solutions for phishing

The solutions mentioned in the barrier model of phishing can be categorized using the same table where Clark's techniques of situational crime prevention are put into. This results in the following table where the solutions are categorized by the main five rational choice categories.

Before further reading and presenting the table, it should be noted that there is some unavoidable overlap among categories. Solutions or measures that increase the effort demanded for crime and delay the offender will also increase the risks of apprehension. This means that there is sometimes difficulty in deciding where a particular measure best fits into the classification in Table 1, and indeed some measures can serve more than one purpose (Clark, 1997, p. 17).

Increase the effort	Increase the risks	Reduce the rewards	Reduce provocations	Remove the excuses
Keep security software and computers up to date	Active scanning for burglary	-	-	Seek for support from government (police issue) – laws and regulation
Make people aware, through commercials/that money mules are not profitable	Strict control of organizations such as web money.			Make people aware, through commercials/that money mules are not profitable
Higher level security, firewall settings	Identify and bring down fraudulent websites.			
Identify and bring down fraudulent websites.	Botnet rental check by infiltrate into a carding forum			

Table 4. Barrier model solutions of phishing categorized under the rational choice categories by Clark (1997)

What stands out is that only three rational choice categories are interesting namely increase the effort, increase the risk and remove the excuses. The solutions related to phishing do not fit under the categories reduce rewards and provocations.

Two solutions did not fit into the table, namely research on fast flux networks and stimulating competition in protection and security sectors. This is because these are indirect solutions whereas the table by Clark is only ideal for direct measures and solutions. However, the outcomes of these solutions may contribute to increasing the effort and risk of a crime.

Actor perspective phishing

Here, the solutions derived from the barrier model of phishing are linked with the 'battling' actors. It should be noted that there is some overlap when it comes to designating solutions to the actors.

The National Police

- Seek for support from government (police issue) – laws and regulation
- Botnet rental check by infiltrate into a carding forum
- Identify and bring down fraudulent websites.
- Active scanning for burglary
- Strict control of organizations such as web money.
- Research on fast flux networks
- Make people aware, through commercials/that money mules are not profitable

National government

- Make people aware, through commercials/that money mules are not profitable

Banks

- Stimulate competition in protection and security sector
- Make people aware, through commercials/that money mules are not profitable

Private security

- Keep security software and computers up to date
- Higher level security, firewall settings
- Make people aware, through commercials/that money mules are not profitable

Another rather important finding is that most solutions for phishing are executable by the national police rather than actors such as banks, private security or the national government.

Categorizing solutions for skimming

The solutions mentioned in the barrier model of skimming can be categorized using the same table where Clark's techniques of situational crime prevention are put into. This results in the following table where the solutions are categorized by the main five rational choice categories. Once more, it should be noted that, according to Clark (1997) there is some unavoidable overlap among categories.

Increase the effort	**Increase the risks**	**Reduce the rewards**	**Reduce provocations**	**Remove the excuses**
Keep security of hard and software up to date (ATM) Higher level security settings (daily control) Wi-Fi jammer Make banking/debit cards more complex Additional control measure to collect large amounts of money	Obtain equipment: infiltrate carding forums Control of false bankcards in shops. Surveillance Active scanning for skimming equipment and devices at ATM Place sensors in existing equipment (ATM) that gives a signal	-	-	Commercial suppliers or skimming parts should be held accountable

(verification code) Make banking/debit cards more complex	when something is covered Pay attention to clothing, behaviour and time after notification (camera images)			

Table 5. Barrier model solutions of skimming categorized under the rational choice categories by Clark (1997)

What stands out is that once again the solutions mentioned in the barrier model of skimming only concerns three of the five main rational choice categories, namely increasing the effort, the risk and removing the excuses. The solutions do not fit under the categories reducing rewards and provocations. This could mean that the abovementioned actors should focus on these three categories.

One solution, stir up the competition in security between banks, did not fit into the table at all due to the fact that is in an indirect solution to skimming whereas all other solutions seem direct solutions.

Actor perspective skimming

National Police can:

- Obtain equipment: infiltrate carding forums
- Surveillance

National government

- Commercial suppliers or skimming parts should be held accountable
- Stir up the competition in security between banks

Banks

- Keep security of hard and software up to date (ATM)
- Active scanning for skimming equipment and devices at ATM
- Higher level security settings (daily control)
- Wi-Fi jammer
- Place sensors in existing equipment (ATM) that gives a signal when something is covered
- Surveillance
- Make banking/debit cards more complex
- Pay attention to clothing, behaviour and time after notification (camera images)
- Additional control measure to collect large amounts of money (verification code)

Private security

- Make banking/debit cards more complex

- Control of false bankcards in shops.

Apart from above, one solution remain after linking them to the actors. Namely high security demotivates. This solution is too general and not assignable to any of the abovementioned actors.
A remarkable finding is that banks rather than other actors such as the national police, government or private security organizations are the designee to execute most solutions for skimming.

5.7 Patterns and findings

1. When a phishing scheme occurs, fake imitating websites are being used. In addition, the model of phishing shows that a critical part in the phishing scheme is to persuade people to react. Therefore, it is assumed that within a phishing scheme the most critical part for the criminal is to get past spam filters and persuade people to react on messages.

2. After analyzing the online news articles, there was no sign that skimmers sold their stolen information or employed others to do so. In addition, a skimmer did not make online purchases according to the online news articles. This is because it is difficult, because a verification code is needed for online purchase which is not encoded on the magnetic strip of a credit card (Merchant account blog, 2006). Analyzing the online news articles, it can be said that all skimmers had counterfeit cards to cash their stolen information. When a skimming scheme occurs all criminals use counterfeit cards to cash. The articles that mentioned which cashing method was used all indicated this was done by the use of false debit cards.

3. A majority (21 of 23 online news articles) of the selected articles reported that the skimming scheme is done by at least two people. The articles that reported a single person arrest give the presumption that these are drops or runners, without knowing they are part of a larger group.

4. The financial damage is more extreme and spread (over one million dollar loss) when a skimming scheme is done by a large group.

5. The opportunity-reducing techniques by Clark, ed. can be used in relation to phishing and skimming.

6. All ‘battling’ actors (authorities and organizations) should focus on three rational choice categories are interesting namely increase the effort, increase the risk and remove the excuses when it comes to prevent and stop skimming or phishing.

7. Most solutions for phishing are executable by the national police rather than actors such as banks, private security or the national government.

8. Banks rather than other actors such as the national police, government or private security organizations are the designees to execute most solutions for skimming.

6. Discussion

In this chapter, the question '*is our goal achieved?*' is answered. Then this discussion gives a consideration about what could be the easiest way to succeed a carding scheme. Second, the limitations of this study are discussed. Third, recommendations and concerns follow, which are drawn during and after treating study material of carding. These recommendations or and concerns can match the findings or are apart from it. Finally, future research is discussed.

To answer the first question, the purpose and objectives of this study will be repeated. The purpose of this exploratory case study is to model important processes and aspects of carding. This way the modus operandi of carding partially becomes known and which may be able to contribute to the control and prevention of carding and other (cyber) crimes, because the techniques and processes that are used often recur in other types of cybercrime. When it becomes clear which aspects are important and where intervention seems most effective, the police and relevant actors can make the right policy. The objectives of this study are:

1. *Describe carding as a type of cybercrime*.
2. *Develop an intervention point of carding*.

Objective one is achieved. The processes of carding are described and modeled according of what is stated in the online news articles and additional literature. By treating the processes of carding, carding self is well described. By reading this study, people get familiar with the definition of carding as a type of cybercrime.
Objective two is not achieved yet. The developed barrier models give us possible intervention points of carding. However, the measures stated in the two barrier models do not cover carding entirely but only counts for phishing and skimming schemes. The processes of carding differ greatly, so similarities or patterns between processes are not found.

6.1 Easiest way

Although only a few patterns have been found, it became clear what tactic could be used of succeed a carding scheme (plea): If someone wants to commit a carding crime to get financial benefits and that someone is lacks knowledge of computers (language) he or she should use skimming as attacking technique. However, if someone does understand the use of computers, the other two attacking techniques are options as well. Nevertheless, it is assumed that most people do not know much about how to hack systems, steal online, or set up other plans to commit crime by the use of internet. Phishing requires more knowledge. Of course, people

may be assigned to do that, but skimming is easier to do and understand, although there is need for some devices. However, these can easily be bought. Another issue why choosing skimming rather than phishing is that everything that is said on the internet may be/get traced, which may be used against a computer user when he or she get caught. Another research is necessary to show us in what caught cyber criminals know of computer language and what attacking techniques they preferred and chose. To get information of bank accounts a person has to assign store personnel to gain information in exchange for a small reward. A criminal may then - once information is gained - make counterfeit cards for cashing. The criminal then must use those cards at stores where people least expect them, instead of ATM's where there could be more surveillance. According to the online news articles, when payments are made in stores, the police did not exactly find out what the financial damage figures exactly are.

6.2 Limitations of this study

1. A question that can be asked is if the information and information from online news articles are valid and reliable. The answer to this question is no, because online news articles do not contain empirical facts and can be written by anyone. This directly shows the limitation of this study, namely validity. Nevertheless, since there is no other source available there is no other way. It must be assumed that the authors who wrote articles all have some knowledge about the treated subjects because they write for organizations whom are involved in security and internet issues. In addition, other (scientific) literature is occasionally used to underpin the research empirical or to complement the information that was found in the articles. Nevertheless, if someone will repeat this study, the findings of that study will be the same.

2. The limitation is that the information gathered from online news articles and some literature sources does not give a complete view of all the processes that can take place within carding. There could be (useful) data missing. Using online news articles may imply that this study could be incomplete. Although, less useful data could help to confirm data found in other articles. Nevertheless, data could still be missing. Based on the limited time and resources however, no alternative seems possible. Therefore, it must be said that data gained from online news articles can be complemented by other literature and leaves room for adjustments.

3. The number of articles used are doubtful. The results will be better if more online news articles are analyzed and are proportionally distributed in frequency. Not every process of carding that is described and modeled in this study, is based on the same number of online news articles.

   A good theoretical framework is missing in this study. Partly due to the moderate number of theories that may apply to carding. Moreover, the theories may be out dated because crime through the use of internet and hardware differs with street crime. Future research should include a well-fitting theoretical framework. Due to a shortage of theories and methods in analyzing data the validity can be criticized.

4. Another issue is that only one expert and organization is asked to give remarks of the results. Although it is said that giving remarks on models is especially objective, one expert may lack knowledge of all the possible scenarios and schemes. Due to time, only one expert was approached.

5. Because of previous named limitations, the findings are not completely valid. The findings should be generalized with caution. In addition, some findings are derived from barrier models which are already findings of what is studied.

6.3 Recommendations

Although the barrier models mention several solutions, recommendations, and findings are discussed in paragraph 5.7, here some recommendations in general are stated. These can overlap.

1. As a continuation of what is stated above, the NHTCU should further focus on phishing, hacking and the use of messaging tools such as Jabber, ICQ or MSN where cyber criminals meet. NHTCU must search for all possible and newly used messaging tools (due to possible displacement) and give less attention to skimming because patrol officers may prevent skimming because it occurs mainly on the street. Regarding to news articles online related to skimming, it is assumed that when a skimming scheme occur all criminals use counterfeit cards to cash at ATM's It is partly a visible crime and therefore a task for patrol police officers or bank employees. Phishing or hacking and other computerized attacking techniques are only visible on the internet. NHTCU should therefore receive feedback from police officers who found skimming devices. If new, advanced and innovative methods are used, the NHTCU must be informed so new techniques can be studied. The NHTCU can then inform police officers how the new techniques work (feedback and feed-forward). Networking with other police units and corps is therefore very important.

2. Banks, gas stations or stores should check their ATM's every day so devices - by definition - are quickly found and schemes that take a day or longer cannot occur (Ambrose, 2010). Once skimming devices are found, replace the devices with normal devices and wait until skimmers restore it (Goodin, 2011). Regarding to news articles related to skimming, it is assumed that when a skimming scheme occur all criminals use counterfeit cards to cash at ATM's.

3. The police and companies like Fox-IT and the virus industry should stir up the competition between banks in security and safety. People bring their money to well protected banks with a good reputation. What banks want is contracting customers, a lot of them. To get customers, banks are forced to invest in security and safety of information or ATM's (NVB, 2008). By investing in security and safety, banks get a reputation (often the bank that lacks protection and security is getting a bad reputation)

which may influence people thoughts of picking a bank. This competitive battle can be stimulated.

4. Authorities and organizations should focus on three rational choice categories, namely increase the effort, increase the risk and remove the excuses when it comes to prevent and stop skimming or phishing and perhaps carding. In particular, the National Police or NHTCU should focus on phishing whereas banks should focus on executing most solutions for skimming. However, tight collaboration between authorities and organizations is desirable and wise. Expertise and information should be shared to make collaboration possible.

6.4 Concerns

1. A shift will rise when battling carding becomes more successful. By taking some criminals into jail, the crime does not stop. Criminals look for other possibilities to commit carding, such as searching for bad security systems, like banks in Africa. The security and the knowledge of security of banks in Africa is suspect (Kumar, 2010). Although police forces managed to roll up a few carding forums, cybercrime cannot be stopped by this action alone. Carding is mobile.

2. Second, more often wire-less theft occur. Also known as war driving (Verini, 2010; Liebowitz, 2011). "*Hackers would sit in cars or vans in the parking lots of big-box stores with laptops and high-power radio antennae and burrow through companies" vulnerable Wi-Fi networks. Adepts could get into billion-dollar multinational servers in minutes*" (Verini, 2010). As long as people are not familiar with the vulnerabilities of Wi-Fi, this attacking technique is very hard to stop.

6.5 Future research

The descriptions and models of processes of carding are based on online news articles and additional literature. This means that only a limited number of data and information is used. Therefore the presented descriptions and models can be expanded with new data. In that sense, in the future the descriptions and models must be updated and expanded. A more specific research can contribute to show us how caught cyber criminals related to carding, their knowledge of computer language and what attacking techniques they preferred and chose. Researchers should ask them why they chose certain strategies. This way, the causes and roots of committing certain (cyber) crimes are revealed and future criminals discouraged. The outcomes could support police tasks and objectives and in particular NHTCU. In addition, the assumptions that are made in this study must be further tested. Lastly, future research should include a well-fitting theoretical framework.

7. Conclusion

Here the answers to the stated research questions are answered. First, the sub questions are answered. After that, the main research question is answered and some final words are given.

First sub question one, which is: *how is carding organized and what are their sub processes?*

1. What this study shows us, is that carding contains processes such as phishing, skimming, the use of carding forums, ways of cashing and other processes that are not discussed in this study. What can be said is that carding, as a whole process exists of three aspects, namely attacking, trafficking, and cashing. The processes related to carding can be placed under these three aspects. A representation of this assumption is given on page 12.

The second sub question is*: what are the actors in the main processes?*

2. During the section analysis, both activities as actors are discussed for the main processes. The answer to this question are put in descriptions and models under the headings ‘actors’.

The third sub question is*: To what extent do the developed models correspond with information and expertise from the National High Tech Crime Unit?*

3. The models that are developed correspond well with the information and expertise from NHTCU. Having an expert looked at the models did not give distressing remarks. A first look by the employee of NHTCU resulted in remarks that some activities are missing and others could wrongly interpret some terms. By implementing the remarks in the text, it can be said that the developed models correspond with information and expertise from the NHTCU. Nevertheless it is doubtful, because only one expert of NHTCU fully analyzed the developed models. The treated online news articles and additional literature give solid but limited views of what activities and actors are involved.

The 4th sub question is: *Which opportunity reducing-techniques by Clark ed. are the most relevant to the prevention of different types of carding by authorities and organizations?*

4. The answer to this question is that three categories of the opportunity-reducing techniques by Clark seem most relevant for authorities and organization to use. These are increase the risk, increase the effort and remove the excuses (see table 2 for a better understanding). The authorities and organizations that should use these are the National Police and government, banks and the private security sector. These are the most important actors in preventing and stopping phishing and skimming which are types of carding.

Instead of naming the most relevant opportunity-reducing techniques for authorities and organizations, this study brings along the solutions that each authority or organization should execute. The solutions from the barrier models fitted nicely within three categories of the opportunity-reducing techniques.

5. Eventually, the main question of this study is: *To what extent are patterns recognizable in the criminal process of carding?* Figure one on page 12 shows what activities occur when a carding scheme takes place, along with the three aspects. No matter what scheme is taking place, the schemes all descends from the activities shown on page 12. When looking at each different treated process within this study and comparing them, there is no one pattern visible. Phishing and skimming differ completely from each other because the crimes take place in different settings (real world versus internet). Besides these two attacking techniques, the use of a carding forum or cashing cannot be compared as they are completely different processes either. However, there are a few noticed patterns and assumptions within the processes self. Within a phishing scheme, the most critical part for the criminal is to get past spam filters and persuade people to react to messages. Second, when a skimming scheme occurs all criminals use counterfeit cards to cash. Third, a majority of the selected articles reported that at least two persons are involved during skimming schemes. Finally, the financial damage is more extreme and widespread (over one million-dollar losses) when a skimming scheme is done by a large group. Looking at the two barrier models, patterns in the criminal process of carding (preparation, infiltration, getting information) can be seen. However, the categorized activities are not comparative because there are differences between the two criminal processes.

6. The output of this study can give people, authorities and organizations a better understanding of carding and fulfil the request of NHTCU and other actors to support their tasks and objectives. With the realized models people can now easily see what activities and actors are involved when a carding process takes place, which could make intervening easier. Although, the validity of the results is questionable, this study gives answers to some research questions that can help authorities and organizations to understand, prevent and stop phishing and skimming. The recommendations, concerns and barrier models may help future policy.

   Because this study has no good theoretical framework (partly due to the few studies that is done about carding), there are however no fundamental conclusions to give. Rather, this study must be seen as a good starting point for adding new and more recent data or comments. Especially since the data that is used may already be out-dated and other techniques, activities, actors can or may be used. It is assumed that the results of this study will last for a couple of years and that the results are a good basis for future research and policy. As shown, the current situation of the existence and battle against carding cannot be solved easily.

References

Ambrose, E. (2010). *Columbia Bank the latest to be hit with ATM skimming scheme. Authorities expect such financial fraud to grow*. The Baltimore Sun. Retrieved, 2 July 2011, from: http://articles.baltimoresun.com/2010-12-06/business/bs-bz-ambrose-bank-skimming-20101207_1_account-information-atms-device

Aston, M., McCombie, S., Reardon, B., Watters, P., (2009). *A Preliminary profiling of Internet money mules: An Australian perspective*. Cybercrime Research Lab, Macquarie University.

Ayaz, M. (2006). *Cyber Crimes and Solutions*. Department of Computer Science, University of Karachi. Retrieved, 22 June 2011, from: http://ezinearticles.com/?Cyber-Crimes-And-Solutions&id=204167

Babbie, E. (2007). *The practice of social research*. *(*11th *ed.).* Belmont, CA*:* Thomson/ Wadsworth.

Banksafeonline. (2008). *Payment advice. Helpful information from the UK payments association. Money Mules.* Retrieved, 6 September 2011, from: http://www.banksafeonline.org.uk/documents/money_mules_advice_guide_final.pdf

Brownlow, M. (2010). *Email address lists: buy or leave alone?* Retrieved, 2 September 2011, from: http://www.email-marketing-reports.com/basics/bulk-email-lists.htm

Buchanan, M.B. (2006). *MIAMI MAN INDICTED IN ONLINE SCHEME TO DEFRAUD HURRICANE KATRINA RELIEF CONTRIBUTORS AND PNC BANK CUSTOMERS*. Retrieved, 22 June 2011, from: http://www.justice.gov/criminal/katrina/pr/2006/aug/08-16-06desirindict.pdf

Clarke, R.V. ed. (1997) *Situational Crime Prevention: successful case studies* (2nd edition). New York: Harrow and Heston.

Clarke, R.V. and Eck, J. (2003). *Become a Problem-Solving Crime Analyst*. London: Jill Dando Institute of Crime Science, University College London. www.jdi.ucl.ac.uk/publications/manual/crime_manual_content.php

Cornish, D. B. and Clarke, R. V. (2003) 'Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention', in Smith, M. and Cornish, D. B. (eds) Theory for Situational Crime Prevention, Crime Prevention Studies, Vol. 16, Criminal Justice Press, Monsey, New York.

Cornish, D.B. (1994). "*The Procedural Analysis of Offending and its Relevance for Situational Prevention*." In R.V. Clarke (ed*.),* Crime Prevention Studies, Vol. 3, pp. 151-196. Monsey, N.Y.: Criminal Justice Press.

CTV Montreal, (2010). *Police bust debit card cloning operation.* Retrieved, 29 June 2011, from:http://montreal.ctv.ca/servlet/an/local/CTVNews/20101116/mtl_debit_101116/20101116/?hu

Darknet.uk.org. (2006). Top 15 security/hacking tools & *utilities*. Retrieved, 29 June 2011, from: http://www.darknet.org.uk/2006/04/top-15-securityhacking-tools-utilities/

De Gelderlander. (2010). *Acht verdachten gepakt in pinpasfraudezaak.* Retrieved, 29 June 2011, from: http://www.gelderlander.nl/nieuws/algemeen/binnenland/9043204/Acht-verdachten-gepakt-in-pinpasfraudezaak.ece

Department of Justice, (2008). *38 Individuals in U.S. and Romania Charged in Two Related Cases of Computer Fraud Involving International Organized Crime International Law Enforcement Cooperation Leads to Disruption of Organized Crime Ring Operating in U.S. and Romania*. Retrieved, 24 June 2011, from: http://www.justice.gov/opa/pr/2008/May/08-odag-434.html

Duecy, L. (2010). *2 men accused of skimming at ATM machines*. Komonews. Retrieved, 29 June 2011, from: http://www.komonews.com/news/problemsolvers/112639209.html

Garfinkel, S. (2002). *The FBI's Cybercrime Crackdown. A new breed of special agent is taking on high tech criminals*. The FBI's Cybercrime Crackdown. 4/4/04. P.1.

Goodin, D. (2008). *Romanian national cops to $700,000 phishing trip*. *Who's your underworld Popa*? Retrieved, 22 June 2011, from: http://www.theregister.co.uk/2008/10/09/romanian_phishing_guilty_plea/

Goodin, D. (2011). *Men sentenced for role in international ATM skimming ring*. Security. Retrieved, 29 June 2011, from: http://www.theregister.co.uk/2011/01/12/atm_skimming_prison_senteces/

Hernandez, B.A. (2010). *Credit card fraud surpasses $1 Billion in half of 2010. Business news daily*. Retrieved, 22 June 2011, from: http://www.businessnewsdaily.com/credit-card-fraud-surpasses-1-billion-in-half-of-2010-0570/

Hickley, M. (2009). *Rise of the online credit card sharks: Annual crime figures reveal fraud soaring to 610m pound*. Daily Mail. Retrieved, 22 June 2011, from: http://www.dailymail.co.uk/news/article-1200183/Card-fraud-costs-UK-610m-chip-pin-fails-prevent-thefts.html

Hulst, R.C. van der &. Neve, R.J.M. (2008). *High-tech crime, soorten criminaliteit en hun daders. Een literatuurinventarisatie.* Den Haag: WODC/Boom Juridische uitgevers, nr. 264.

The National White Collar Crime Center (NW3C), (2011). *2010 internet crime report*. Retrieved, 22 June 2011, from: http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf

KLPD – Dienst Nationale Recherche. (2009). *High Tech Crime, criminaliteitsbeeldanalyse 2009*. Driebergen.

Krebs, B. (2010). *Body Armor for Bad Web Sites*. Retrieved, 2 September 2011, from: http://krebsonsecurity.com/2010/11/body-armor-for-bad-web-sites/

Kumar, N. (2010). *Africa Could Become The Cybercrime Capital Of The World*. PSFK. Retrieved, 22 June 2011, from: http://www.psfk.com/2010/04/africa-could-become-the-cybercrime-capital-of-the-world.html#ixzz1S4VRfsf0

Leukfeldt, E.R., Domenie, M.M.L., & Stol, W.Ph., (2010). *Verkenning cybercrime in Nederland 2009*, veiligheidsstudies. Den Haag: Boom juridische uitgevers.

Liebowitz, M. (2011). *'Wardriving' Black Mercedes Cracks Wi-Fi Networks*. SecurityNewsDaily. Retrieved, 22 June 2011, from: http://www.securitynewsdaily.com/wardriving-thieves-hacked-into-wi-fi-networks-from-black-mercedes-0723/

McMillan, R. (2011). *Citigroup hackers made $2.7 million*. Retrieved, 22 June 2011, from: http://www.computerworld.com/s/article/9217932/Citigroup_hackers_made_2.7_million?taxonomyId=82

McMillan, R. (2009). *In China, $700 puts a spammer in business*. Retrieved, 2 September 2011, from: http://www.computerworld.com/s/article/9132758/In_China_700_puts_a_spammer_in_business

Merchant account blog. (2006). *Credit card skimming – too easy to get skimming equipment!* Retrieved 2 September 2011, from: http://www.merchantequip.com/merchant-account-blog/149/credit-card-skimming-and-places-that-sell-skimming-devices

Nairane, R. (2006). *Money Mules: The Hidden Side of Phishing. Online fraud depends on an offline component—people who launder money*. Retrieved 6 September 2011, from: http://www.eweek.com/c/a/Security/Money-Mules-The-Hidden-Side-of-Phishing/

Nederlandse vereniging van banken (NVB). (2008). *Reactie NVB op de rijksbegroting 2009*. Retrieved, 17 September 2011, from: http://oikos.nvb.nl/index.php?p=115870&return=11219

Nederlandse Vereniging van Banken (2011). *Vragen en antwoorden: Fraude met internetbankieren en oprichting ECTF*. Retrieved, 26 September from: http://www.nvb.nl/scrivo/asset.php?id=574165

Ollman, G. (2004) *The Phishing Guide – Understanding and Preventing*, White Paper, Next Generation. Security Software Ltd.

Pankratz, H. (2010). *Six indicted in Colorado on bank fraud charges*. The Denver post. Retrieved, 22 June 2011, from: http://www.denverpost.com/breakingnews/ci_15497703

Peretti, K.K. (2009). *Data Breaches: What the underground world of "carding" reveals"*. Santa Clara Computer and High-Technology Law Journal. 25(2), 375-413.

Rasmussen, R., Aaron, G., (2010). G*lobal Phishing Survey: Trends and Domain Name Use in 1H2010*. APWG, October 2010.

Reed, P. (2011). *Online car-buying fraud*. Retrieved, 26 September 2011, from: http://www.edmunds.com/car-buying/online-car-buying-fraud.html

Sanders, T. (2006). *US cyber-crime damage pegged at $67bn*. Retrieved, 22 June 2011, from: http://www.v3.co.uk/v3-uk/news/1980516/us-cyber-crime-damage-pegged-usd67bn

Scarafile, P., Cappio, E.C., (2007). *Automated banking machine anti-skimming card reader*. United States patent. North Canton.

Sugimoto, M. (2011). *CA men indicted for allegedly stealing credit card info from 194 people in Hawaii*. Hawaii News Now. Retrieved, 22 June 2011, from: http://www.hawaiinewsnow.com/story/14302563/grand-jury-indictes-california-men-for-identi?redirected=true

The Global ATM Security Alliance, The ATM Industry Association, Fair Isaac Corporation's CardAlert Fraud Manager Service, 2008. *WIRELESS TECHNOLOGY PROVIDES POTENTIAL "NO STRINGS" ADVANTAGES FOR ATM THIEVES*. ISSUE NUMBER 2008-01. Retrieved, 3 September 2011, from: http://www.gasa-cognito.com/FraudLibrary/GASA%20Fraud%20Alert%202008-01.pdf

Van Dale, (2012). Betekenis 'server'. Retrieved, 6 September 2012, from: http://www.vandale.nl/opzoeken?pattern=server&lang=nn

Verini, J. (2010). *The great cyberheist*. The New York Times. Retrieved, 22 June 2011, from: http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html

Vijayan, J. (2010). *Aldi data breach shows payment terminal holes*. Retrieved, 22 June 2011, from: http://www.computerworld.com/s/article/9189982/Aldi_data_breach_shows_payment_terminal_holes?taxonomyId=17

Wesh., (2010). *Disney Clerk Accused Of Credit Card Skimming***.** Retrieved, 22 June 2011, from: http://www.wesh.com/entertainment/23781326/detail.html

Appendix

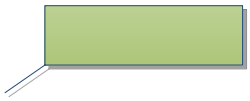
This appendix contains a legend that will help understand the models presented in the text.

Activity

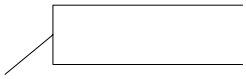
Connection

Optional

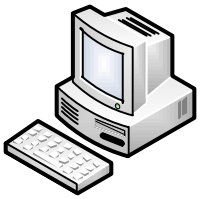
Connection /Dataflow



Remarks



Role clarification



Computer/ Internet

Actor