

The little green book on identity theft



NORMAN[®]



Now the serpent was more crafty than any of the wild animals the Lord God had made. He said to the woman, “Did God really say, ‘You must not eat from any tree in the garden’?” The woman said to the serpent, “We may eat fruit from the trees in the garden, but God did say, ‘You must not eat fruit from the tree that is in the middle of the garden, and you must not touch it, or you will die.’” “You will not surely die,” the serpent said to the woman. “For God knows that when you eat of it your eyes will be opened, and you will be like God, knowing good and evil.”

Genesis 3, 1-4

This text – from the very beginning of the Bible is probably the first example of identity theft: The Devil, masquerading as a serpent, tricks Eve to eat the fruit from the tree of knowledge of good and evil – the Devil has stolen the serpent’s identity.

Thus, identity theft is not a new phenomenon – it has been there from the beginning of time.

Content

The different roles as a potential victim	6
The intent of the identity thief	9
Techniques used for identity theft	11
The Internet – a plethora of information	16
Social engineering – THE most important tool to obtain information ...	17
How to protect yourself from identity theft	18
Closing words	22

Norman ASA is not liable for any form of loss or damage arising from use of the documentation or from errors or deficiencies therein, including but not limited to loss of earnings.

The information in this document is subject to change without notice. No part of this documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the explicit written permission of Norman ASA.

The Norman logo is a registered trademark of Norman ASA.

Names of products mentioned in this documentation are either trademarks or registered trademarks of their respective owners. They are mentioned for identification purposes only.

Copyright © 2006 Norman ASA.
All rights reserved.

Introduction and definition

This small book will discuss identity theft with particular emphasis on the extended possibilities that the Internet and computing offer.

One should note that identity theft assumes many forms from the playful to the extremely dangerous.

Consider these two scenarios:

1. By careful collection of information, interception of mail and theft of Carl's original proofs of identity, Frank is able to "become"

Carl in all matters that count. Only those who know Carl from before the theft took place can know that Carl is Carl. In all other contexts Frank is Carl.

2. Linda sends a postcard to Yvonne's aunt from Spain, congratulating her with her birthday, and signs it Yvonne. The aunt is amazed that Yvonne remembers her birthday while in Spain, and tells herself that Yvonne is a really considerate niece.

Both are examples of identity theft. Obviously the first is potentially quite severe for Carl, while the latter may be to



Yvonne's advantage (e.g. in her aunt's last will).

Thus, we cannot say that all kinds of identity theft are necessarily bad, as one can "borrow" another person's identity with good intent and outcome as the second example above shows.

We can therefore come up with a general definition of identity theft as **the act of pretending to be another person in communication with a third person or persons.**

However, identity theft is normally seen as something bad, which will also be the main

theme in this book. We will therefore hereafter restrict the general definition and refer to identity theft as **the act of pretending with malicious intent to be another person in communication with a third person or persons.**

This operative definition stated above does not define whether this malicious intent is directed against:

1. The person that has his/her identity stolen
2. A third party that may suffer from dealing with person x, while led to believe that it is person y that he is dealing with.
3. Both of the above mentioned.

It is important to be aware of the fact that all these are identity thefts. The party that might be hurt however will differ. Although the situation mentioned in item 1 above is the most focused in the press and other media, item 2 may be as important and as crucial to defend against.



A general definition of identity theft as the act of pretending to be another person in communication with a third person or persons.

This book will discuss various examples of identity theft and techniques used, as well as outlining how you can defend yourself against being victimized.

Although Internet-based techniques for identity theft (like phishing) are almost exclusively in focus presently, as we shall see, other old-fashioned techniques may be just as effective, often even more.

No matter how sophisticated malicious software that is created, no matter which sneaky hardware devices that is set up – the human being (wetware) is still the main security risk.

Nevertheless, this book will focus in particular on the use on Internet as means for Identity theft.

Throughout this book we will, when relevant, refer to the victim of identity theft as a “he” while the identity thief will be a female. This is of course for simplification reasons only.

The different roles as a potential victim

Defining roles

When discussing the means and techniques of identity theft, it is often useful to consider the different roles a person has in order to consider which types of identity theft that you should beware of in the different roles.

Key words in the different roles are:

- Who you are
- What you know

Your role as a private person

As a private person your identity may be interesting for a number of totally different reasons, and the motivation for stealing your identity may be equally diversified.

If you for some reason have angered a person and this person wants to take revenge, she has a plethora of means liter-

ally available on her fingertips. All of which involve stealing your identity for a short while.

A couple of examples are:

- She can use any phone and order subscriptions of lots of different magazines in your name.
- She can write a letter, signed in your name, cancelling your newspaper subscription with immediate effect.

Common for these examples of such ad-hoc identity theft is that the thief is impersonating

you towards people who have no (practical) means to check if she is really you.

One may of course view the above mentioned as mere nuisances, which they to some extent also are. However, it can be quite tedious and time-consuming to cancel magazine subscriptions all the time. And the person that has become your enemy for some reason can of course escalate her harassment with even more annoying and severe acts (shutting off your electric-



She can use any phone and order subscriptions of lots of different magazines in your name.



ity because in her mail to the supplier - signed by “you” – she states that she (“you”) is going away on a long journey abroad).

Your role as a person in a corporation

On the other hand you should consider your role as e.g. an employee.



A more “popular” scenario is when someone attempts to steal your identity as a mean to steal something, like money from your bank account. Whether you are a tempting target will of course depend on how much money you have as well as how easy it is to steal your identity. This scenario will be discussed further in a later chapter.

Suffice it to say in this context that identity theft directed as the private person you are, is motivated by your characteristics as this person (rich, unpopular, popular, famous etc.). The identity thief will have you as her ultimate target.

In this case it is not you who are the target, but the corporation in which you are employed. Stealing your identity is only a means to be able to access/obtain something from your employer – this is usually some kind of industrial espionage.

Again, some examples illustrate this:

You work as a janitor and are currently deployed to clean the premises of a big company. One of this company’s competitors hires a person to steal your identity as a tool to be able to go through the company’s dustbins hoping to

find information of interest, or adding a little black box at the rear end of your computer that monitors all key strokes from the keyboard. Imper-

Later in this book we will go into more detail regarding the implementation of these kinds of identity theft. The point we want to make here

“

By social engineering techniques she can trick a person to reveal his user name and password to a company server.

sonating you (stealing your identity) could be done easily by showing up at another time of the day than you usually do (who would notice in a large corporation?).

Another scenario is if you are employed in the company's IT department. The thief of your identity could then call someone in the company pretending to be you, and by social engineering techniques she tricks that person to reveal his user name and password to a company server. Again it is possible to obtain information that the company does not want to fall into the hands of the competitor.

is merely that it is your role as a corporate person that is the intermediate target here. The main target is not you.

The intent of the identity thief

Keeping the theft secret or not

The previous chapter's examples show that the time frame of the identity theft will differ, depending on the intent of the identity thief.

In most of the cases the identity thief only needed to steal a person's identity for a very short time in order to accom-

plish a particular task. Often it does not even matter if the person who had his identity stolen notices this after the theft took place.

In the example where you were the victim of harassment it is actually a point in itself that you are aware of the fact that someone is harassing you. On the other hand, the example of industrial espionage would probably be more successful if it was not revealed that secret information was in the hand of the wrong persons. If your bank account is emptied, the identity thief has accomplished what she wanted; that particular theft would probably not succeed a second and third time with you and your bank account.

She becomes you

As a special case we should consider when someone takes over your complete identity to become you. If this is conducted in the most sophisticated manner it actually does not matter if the scam is known or not. As several horror stories have shown, you may then

have a major problem proving to lots of different public and corporate parties, that you actually is you.

An interesting exercise for each and every one of us is to consider is this:

How do you proceed if someone has managed to get a driver's license, a passport and several credit cards in your name. She then takes control of your bank account, asks for and is granted a loan (in your name of course) and the monthly instalments are not met. The credit cards are heavily used and you get huge bills from credit card companies you never had plans to do business with.

What do you do?

“

Industrial espionage would probably be more successful if it was not revealed that secret information was in the hand of the wrong persons.

Techniques used for identity theft

General

In a previous chapter a few examples of identity theft were briefly discussed. We will in this chapter discuss in more detail some of the different techniques that may be used for information gathering. In particular we will emphasize the use of tools available on the Internet for such information gathering.

In general there are two approaches to information gathering with the attempt to steal someone's identity:

- Collecting as much information as possible about one or a very few individuals

- Attempting to harvest information from a huge number of individuals hoping that someone is willing to offer the desired information.

Specialized information gathering

When the identity thief knows a person and a few potential persons whose identity she needs to steal, there is a need to gather some kind of information about that person to facilitate this identity takeover.

There are different techniques that an identity thief may use to gather information about the person she wants to be. In many cases she already knows something about the person



(name, gender, address etc.) but this is not always the case.

Scenario 1 – the victim is a particular identified person

When some information (e.g. name) is known about the per-

stealing the victim's bank account statements)

- Purchasing credit information on the victim
- Hacking the victims computer
- Social engineering techniques by using the



When the identity thief has the information she needs, she can set the theft itself into action.

son our identity thief wants to target, she can use some of the following techniques to gather more information:

- Telephone directories for obtaining telephone numbers and address
- Internet search engines for any information about the person that is available on the World Wide Web. This information can be anything from the extremely useful (for the thief) to the trivial.
- Trash bin investigation (e.g.

telephone or email to obtain particular information.

When the identity thief has the information she needs, she can set the theft itself into action by impersonating the victim as needed.

Scenario 2 – the victim is not identified, but his role is

This would be the case when an organization is the ultimate target. The identity thief will attempt to target the organiza-

tion by stealing the identity of one of its employees. She is not interested in a random employee, but preferably one who has particular access rights and/or one from the management.

Internet sites host such information, e.g.

<http://www.whois.org/>,
<http://www.allwhois.com/>
etc.

After a few seconds she has gathered information that



A good start would be to identify the organization's management and technical staff in the IT department. The obvious starting point is the corporation's web site! It is more normal than not that the web site has information about management, other contact persons, telephone numbers, email addresses etc. She may add and cross check this information by checking the persons who are the contacts on the corporation's domain registration. Several

enables her to target more systematically one or a few key persons using the techniques that is mentioned in Scenario 1 above.

Bulk information gathering

A totally different approach is used if the identity thief wants to obtain some kind of special information regardless of whether it is obtained from one individual or another, as long as the type of information is the same.

Typically this may be

- password(s) to access a special resource (e.g. bank accounts)
- valid credit card numbers

This can be carried out by employing a different set of tools. However, use of the Internet is unrivalled as the tool to use in these cases, as it facilitates:

- a certain degree of anonymity on the identity thief's side
- malicious programs that can be installed on users' computers to reveal confidential information to the identity thief
- possibilities to send a huge number of emails to potential victims
- setting up fake web sites tailored to the identity thief's needs

The use of the Internet to gather information with the attempt to commit fraud is called phishing (derived from "fishing"). This will be discussed in more detail in a separate chapter below.

Phishing – a special case of bulk information gathering

Phishing is an increasingly popular way to obtain information from users – information that may be used to commit crime. New phishing attempts are set up daily.

A typical phishing scheme would be carried out in this manner:

1. The identity thief purchases or harvests electronically in



some manner a large set of email addresses.

2. She sends an email to these addresses with a spoofed sender (e.g. a bank)
3. In the email she claims that something wrong happened with the user's account and requesting a confirmation of the password.

Quite a lot of such emails have a spoofed link to a web site that looks (almost) identical to the institution's real one. However, it is of course a fake site that attempts to obtain secret user information with the intent to commit fraud.

An identity thief may also use special malicious programs to collect information. Details regarding the techniques used to insert such malicious

programs (malware) on a computer are beyond this book.

Suffice it to mention that distributing malware through emails, network spreaders, utilization of vulnerabilities in operating systems and applications, are all popular and widely used techniques to distribute malware.

Keyloggers, trojans and back-doors are typical malware used by the identity thief.

Although these tools are mainly used in a bulk information gathering scheme, it is obviously likely that malicious software may be targeted on a particular person/organization exclusively. Then it would be quite difficult to detect, as most antivirus and antispyware products may not uncover it unless detected by SandBox-like techniques similar to the one integrated in Norman's antivirus products.

Online questionnaires are also efficient tools to gather information about you – information that you normally would not offer to anyone, but which you may be tricked into giving



The use of the Internet to gather information with the attempt to commit fraud is called phishing.

because the questions appears on an official looking (though fake) web site.

Norman has previously published “Norman’s little green book of phishing”, which covers this topic in more detail. Please refer to this book for more in-depth information.

Internet may be so dangerous with respect to identity theft is that its electronic form enables automatic processing and systematization. As more and more personal information (hospital records, bank information, insurance data etc.) are accessible through the Internet, it is of utmost impor-

“

The Internet has made the task for the identity thief much easier.



The Internet – a plethora of information

Although identity theft has been possible and carried out for ages, the Internet has made the task for the identity thief much easier. We have discussed some of these issues above.

One of the main reasons why the information on the

tance that this information is stored in a way that ensures that it cannot be accessed by someone who is not legitimate. Unfortunately we often see examples that this is not the case.

Securing digital information is becoming increasingly important as our lives are evolving more and more into a networked society.

Social engineering – THE most important tool to obtain information

Regardless of the fact that the Internet has made the identity thief's task easier, the by far most important tool for her is good old social engineering techniques.

The most famous hacker of our time – Kevin David Mitnick – is (in)famous for breaking into high-profile computer systems. He was eventually arrested (in 1995) and spent some years in prison. The fact, however, is that Mitnick's attacks were mainly based on social engineering techniques. It is maintained that he was very convincing and persuasive in his attempts to trick people to disclose information that he needed.

The reason why social engineering techniques are so effective is that most humans are eager to please. When someone asks you for assistance your initial reaction is to help that person.

If you work in a large organization and someone calls you on your phone, saying that she is from your organization's IT department and asks for your password because she has to update your account (for whatever reason), most persons would be inclined to give the password rather than challenge the caller's identity.

Another trick it to count on your vanity. Like it or not, most of us are susceptible to flattery, and a skilled person can utilize this to persuade you into giving her information that you should not part with.

The set of conventional social engineering tools available for the identity thief is only limited by her imagination.

When discussing social engineering however, the social engineering aspect involved in identity theft by use of the Internet as a channel cannot be ignored. Most phishing attempts will rely on social engineering. The more elegantly performed the more likely to

succeed. An email written in English attempting to phish for secret user information from users of a Norwegian bank is not likely to succeed... (real life example!)

Social engineering works over and over again because unfortunately users are gullible!

How to protect yourself from identity theft

General

It is presumably possible to be totally protected against any kind of danger. The disadvantage is that if you are, it will either be extremely expensive or, conducting your normal tasks will be extremely cumbersome or even impossible.

The correct general approach to risk is therefore not elimination, but rather finding the correct balance between the risk you expose yourself to and the price you pay if you are being hit by an incident that is not avoided (for whatever reason).

This view should also be taken when protection from identity theft is the issue.

Different protection depending on the thief's approach

Obviously there are different approaches that should be applied to the different kinds of identity theft that are discussed in previous chapters. We will go through some useful guidelines here.



It is presumably possible to be totally protected against any kind of danger.

Two general guidelines to keep in mind:

1. Everything is not necessarily what it seems like
2. There are some people that may not have your welfare as their top priority

Protection against conventional social engineering

Social engineering is probably the most difficult to resist. One approach that may work quite well is to switch into a permanent paranoid mode:

Assume that anyone who contacts you for whatever reason is not the one she claims to be, and that her intentions are nasty.

activity, not to mention that you will lose all your friends in quite a short time.

A better operational approach is use intelligent scepticism.

Try asking yourself whether an initiated contact and her reason for contacting you is probable. Would a person from the IT department really need your password? Is it



This may be a tempting approach to shield against conventional social engineering, but will probably not be applicable in real life. It will be too cumbersome to conduct normal social and professional

likely that the person from the credit card company doesn't know and cannot find your credit card's number and expiry date? Why would your bank representative need your pin code?

By asking yourself such common sense questions instead of supplying the requested information just to be helpful, you will be better prepared

what information you disclose, in which environment, and to whom.

It may be wise to destroy your

“

It may be wise to destroy your credit card statements before throwing them in the dust bin. It is not particularly smart to leave your cash dispenser withdrawals receipt in the open beside the bank

and protected from becoming the victim of social engineering techniques.

Protection against conventional “espionage”

Espionage with the intent of identity theft would use a lot of the same techniques as seen in spy movies:

- dustbin harvesting
- telephone tapping
- monitoring conversations behind closed doors
- impersonation
- information gathering and systematization

The general rule to observe is that you should beware of

credit card statements before throwing them in the dust bin. It is not particularly smart to leave your cash dispenser withdrawals receipt in the open beside the bank. The most secret company information drafts should not be disposed of in an off-hand manner.

Protection against Internet based social engineering

Much of the same approach is sufficient when protecting yourself from Internet based social engineering techniques as for conventional social engineering. Again:

Use intelligent scepticism.

Is it likely that your local bank is sending emails in English? Why would your Internet shop

You will also remember to update your operating system and applications with the latest program patches, as you know that authors of malware are



ask for your password – can you think of anything credible that explains such a request?

Protection against Internet based “espionage”

If you follow the general guideline about intelligent scepticism you will also to some extent be protected against Internet based espionage. You will of course not open the attachment in the email (allegedly) from your favorite female movie star who for some weird reason has decided to email you her nude photographs.

effective in utilizing newly discovered program deficiencies. And of course you update your antivirus and antispyware programs often, and you use a firewall.

In spite of all these precautions someone may write a malicious piece of software that is placed on your PC without your knowledge. An additional level of protection would then be to encrypt the information that is available on your hard drive or network.

Closing words

This book has briefly discussed some aspects of identity theft. Much more information is freely available in interesting articles on the Internet and as printed books. Although – as shown at the very start of this book – identity theft is not a new phenomenon. The Internet and gathering of electronic information about each and every one of us in huge databases (that may in some cases be cross-referenced) make

stealing a person's identity easier and much more difficult to reclaim. The presence of Internet accessible databases that hold electronic information about each and every one of us makes identity theft easier. And more difficult to reclaim your identity if stolen.

There are strong indications that identity theft will prevail for a long time in some form or another. To end this book on a similar note as it started – this time from the end of the Bible, where the identity thief is imprisoned:



And I saw an angel coming down out of heaven, having the key to the Abyss and holding in his hand a great chain. He seized the dragon, that ancient serpent, who is the devil, or Satan, and bound him for a thousand years. He threw him into the Abyss, and locked and sealed it over him, to keep him from deceiving the nations anymore until the thousand years were ended. After that, he must be set free for a short time.

Revelation 20, 1-4

Norway

Norman ASA
Strandv. 37, Postboks 43
1324 Lysaker, Norway
Tel: +47 67 10 97 00
email: norman@norman.no
www.norman.no

Denmark

Norman Data Defense Systems A/S
Blangstedgårdsvej 1
5220 Odense SØ, Denmark
Tel: +45 63 11 05 08
email: info@normandk.com
www.norman.com/dk

Sweden

Norman Data Defense Systems AB
ProNova Science Park, Korsgata 2
602 33 Norrköping, Sweden
Tel: +46 011-230 330
email: sales.se@norman.no
www.norman.com/se

UK

Norman Data Defense Systems (UK) Ltd
15 Linford Forum, Rockingham Drive
Linford Wood
Milton Keynes
MK14 6LY, UK
Tel: +44-1908 678496
email: norman@normanuk.com
www.normanuk.com

Germany

Norman Data Defense Systems GmbH
Gladbecker Strasse 3
40472 Düsseldorf, Germany
Tel: +49-211 / 5 86 99-0
email: info@norman.de
www.norman.de

Germany

Norman Data Defense Systems GmbH
Niederlassung München
Ludwigstr. 47
85399 Hallbergmoos, Germany
Tel: +49-811 / 5 41 84-0
email: info@norman.de
www.norman.de

Switzerland

Norman Data Defense Systems AG
Münchensteinerstrasse 43
4052 Basel, Switzerland
Tel: +41-61 317 25 25
email: norman@norman.ch
www.norman.ch

The Netherlands and Luxemburg

Norman/SHARK BV
Postbus 159
2130 AD Hoofddorp, The Netherlands
Tel.: +31-23-7890222
email: info@norman.nl
www.norman.nl

Belgium

Norman/SHARK BV
Grote Baan 119/2
3511 Kuringen (Hasselt), Belgium
Tel: +32 89 24 37 04
email: belgium@norman.nl

France

Norman France
8 rue de Berri
75008 Paris, France
Tel : + 33 1 42 99 94 14
email: info@norman.fr
www.norman.fr

Spain

Norman Data Defense Systems
Camino Cerro de los Gamos 1, Edif.1
28224 Pozuelo de Alarcón MADRID, Spain
Tel: +34 (0)91 790 11 31
email: norman@normandata.es
www.normandata.es

Italy

Norman Data Defense Systems
Centro Direzionale Lombardo
Via Roma, 108
20060 Cassina de'Pecchi (MI), Italy
Tel: +39 02 951 58 952
email: info@normanit.com
www.normanit.com

USA

Norman Data Defense Systems Inc
9302 Lee Highway, Suite 950A
Fairfax, VA 22031, USA
Tel: +1-703 267 6109
email: norman@norman.com
www.norman.com



NORMAN[®]

www.norman.com