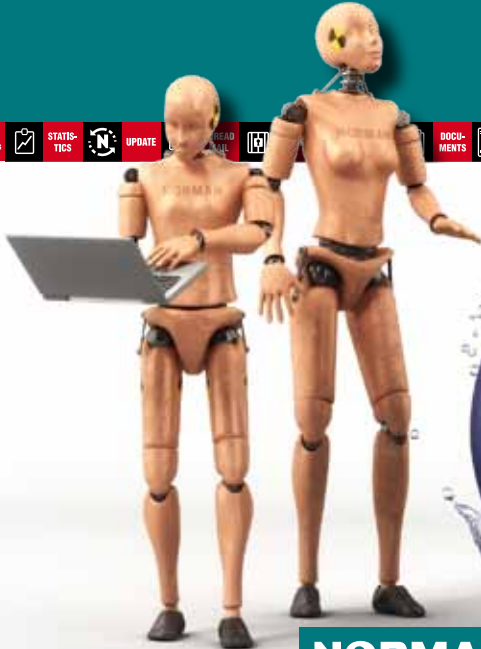


THE LITTLE GREEN BOOK ON
**INTERNET
SECURITY**



NORMAN[®]

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 user'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 may be either trademarks or registered trademarks of their respective owners. They are mentioned for identification purposes only.

Copyright © 2010 Norman ASA.

All rights reserved.

CONTENTS

Safe presence on the Internet	4
How to stay safe on the Internet - 10 advices	6
For the wireless networks user	10
Some common threats	11
Other types of threats.....	16
Spreading mechanisms.....	20
Proactive vs traditional antivirus solutions	22
Norman offices	26

SAFE PRESENCE ON THE INTERNET

It is not an easy task to keep track of the evolvement within the field of IT security and crime. However, the need for effective protection is apparent, and a basic knowledge about the most frequent threats is imperative. The intention of this book is to identify current and common threats, how computer malware can affect the user, and what measures you can take for protection.

Computer viruses and other threats against IT security have been well known problems for a long period of time. The first computer virus was discovered more than 25 years ago, and the problem has evolved at an alarming speed over the years. While the earliest viruses were designed to destroy and to crash machines, today's creators of malicious software (commonly known as malware) are far more advanced and usually have economic incentives. The most active

Note

IT criminals are getting more organized and create more sophisticated threats.

malware authors are often well organised and use sophisticated methods for their software's propagation. Hackers can steal your private information for economic purposes, or they can monitor your surfing habits on the Internet in order to supply you with tailor-made advertising. Some hackers also collect email addresses from your system for selling them to other companies.

How to be a safer user

There are many perils on the Internet. Users of wireless networks (WLAN) and Bluetooth-enabled devices are more exposed to threats than others. Those who use mobile technology should be particularly observant of potential hazards that jeopardize their security.

Mobile users should switch off the Bluetooth connection when it is not needed. The first thing that a potential hacker of a Bluetooth device is looking for is the service set identifier (SSID) – which is impossible to find when the connection is shut down.

Another possible danger is the risk of physical data loss. With more people working at home and outside the company office, the risk of physical theft is increasing. Be careful as to where you leave your laptop or your external memory sticks.

Vulnerabilities as well as malware that exploits these vulnerabilities have already been detected in mobile phones and

Automatic Teller Machines (ATM) or net banks. One example is the Cabir virus that can spread from one mobile phone to another. One may expect that as devices in general are getting increasingly sophisticated regarding their use of computer technology, they are vulnerable for malware attacks.

See also the separate section below on wireless network users.



HOW TO STAY SAFE ON THE INTERNET - 10 ADVICES

1. Never invite strangers home

Be aware of how your PC is configured before you connect to the Internet. It is vital that you are conscious of shared folders/resources. It is not likely that you intend to share your private data with the entire Internet community, which is the effect of exposing your data in an unsafe manner. This is one of the most dangerous security breaches in Windows systems and frequently exploited by intruders. You should also turn off the PC when it is not in use.

2. Use professional “cleaners”

It is a mandatory security measure to install antivirus software. Note that it is equally important to update your antivirus software regularly, preferably automatically whenever you connect to the Internet.

Installation of antispysware and anti-adware products will help you stay clean and keep spyware and adware away from your systems. It is also a good idea



*Software
vendors never
send security
updates as
mass-distributed
emails!*

to let an antivirus system scan your incoming mails before emails are allowed into your computer.

3. Update the operating system continuously

The operating system is the core of all activity in the PC. There is no such thing as a 100% bug free operating system. Virus writers often take advantage of software bugs, so make sure that all important security updates are downloaded and installed continuously as quickly as possible after they are available from the software vendors.

4. Be critical to the “Postal Service”

Apply some common sense rules. If just one of the following situations is true, then simply delete the email:

- The sender is unknown.
- The subject field does not make sense.
- The mail contains a link, and you are not sure where it will direct you on the Internet.
- The email as such is suspicious.
- The email contains a suspicious attachment.

- The email seems to be from a software vendor with an attached program that claims to be a security update. Software vendors never send security updates as mass-distributed emails!

- Use of the preview function in email clients is a security risk. You should turn it off, thus being able to delete unwanted emails without any kind of opening.

- A spam filter will save you a lot of time and frustration involved with cleaning up unsolicited emails, which often contain malicious software. You should never reply to spam messages – replying confirms that the email is valid and monitored.

- You should encrypt confidential information before you send it.

5. Get a trustworthy “doorman”

Your computer has many “entrances” (ports) for different tasks. Open ports could allow unlimited access to your machine’s resources. For instance, port 25 is normally used for email, and this is the port most spammers use. Port 80 is the



normal web entrance. The main purpose of a personal firewall is to protect your computer against “visitors”, i.e. attacks, from the Internet. Most firewalls can also be configured to block access from certain addresses.

6. Lock up “filing cabinets” with sensitive information

Store your confidential data securely. On portable machines that are more likely to go astray, this is particularly important. The best solution is to use encryption tools, which handle folders as well as individual files.

7. Do not let anybody in

Configure your web browser to ask if you allow “active content”.

Many web sites use scripts and other kind of programs to enhance your surfing experience. However, this represents a security risk as it involves program code to run on your computer. Be selective with regard to which web sites you grant access to your own computer, and be critical about programs you download from the web and from peer-to-peer (P2P) systems.

Note

Be careful about revealing personal information on the Internet.

8. Take advice from experienced IT personnel

If you work at a home office or use a portable computer in your daily work, you should first and foremost familiarize yourself with your employer’s rules and regulations on IT security. You may avoid many future problems by consulting your company’s IT personnel.

9. Disclose as little as possible about yourself

Never reveal information of a personal nature if it is not absolutely necessary. It may be a good idea to use separate email addresses for different requests.

10. Back up relevant information

Data erasure can occur by accident, malware activity, or by evil-doers who get access to your data. Back up vital data regularly. The most valuable data is in the files that you have invested time and effort to create. Software and other system files can be reinstalled if they are damaged.

FOR THE WIRELESS NETWORKS USER

Users of wireless networks (WLAN) should take extra precautions in order to stay protected. A wireless network is easy to manage and effective for the users. On the other hand it is easily accessible and thereby vulnerable for intruders and illegitimate users. If you do not protect your wireless network system, it may be accessed covertly and used for illegal downloading or distribution of spam, for example. In a worst case scenario intruders can get access to your computer.

Here is some advice for the wireless user in particular:

Secure your network with an authorization key

The user documentation tells you how to do this. It is a simple procedure that can be done by anybody; you just need to enter the correct code to access the network.

When you enable an authorization key you are sure that only those computers with the correct key can access your

personal network, and that the traffic in the network is encrypted. The most common encryption methods are WEP and WPA.

Note

Always switch off your computer when not in use.

Use antivirus programs

Like all network users, the wireless user should be protected by an antivirus program. Wireless networks are particularly vulnerable, and antivirus software protects you from viruses, worms, trojans and other malicious code. The best programs are the proactive antivirus solutions that do not rely on traditional signature-based technology. The proactive antivirus solutions detect new and unknown viruses, thus providing more effective protection for your computer.

Use antispyware and antiadware programs

These types of programs remove spyware and block illegitimate programs that monitor your Internet activity.

Encrypt your personal data

You would not like to share your data with everyone. The best way of maintaining privacy is to encrypt your files. You can install encryption programs and encrypt emails, personal files, corporate information, confidential records and email attachments.

SOME COMMON THREATS

There are several threats that can harm you as a user. Here are the most common ones:

Malware

Computer malware (short for “malicious software”) is the generic term for program code designed to disturb or destroy a computer system. Below you will find short descriptions of some of the most common types of malware.

1. Virus

A computer virus is a program designed to copy itself and propagate, usually by attaching itself to applications. When an

infected application is running, it can infect other files. Human action is necessary for a virus to spread between machines and systems. This can be done by downloading files, exchanging CD/DVD disks and USB sticks, copying files to and from file servers, or by opening infected email attachments.

A virus may appear in different forms:

File virus:

A file virus is attached to a program file. It uses different techniques to infect other program files. This type of virus may be transferred to/from all kinds of storage media (only to writable devices) and in a network.

System virus:

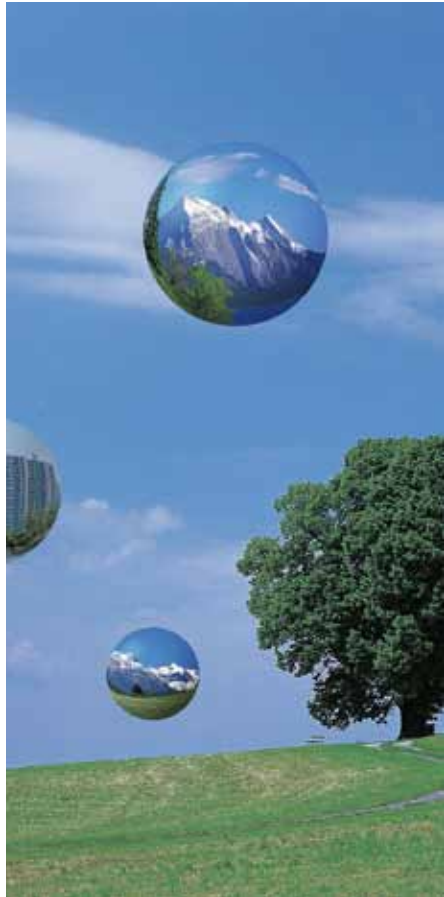
System viruses, also called boot viruses, may be present on boot devices (like USB sticks and CDs) without the user’s knowledge. When a user starts or restarts the computer, the system virus will infect the Master Boot Sector (MBS) and System Boot Sector (SBS) if the computer is booted from the infected device.

Dropper virus:

A dropper is a program that is created or modified to “install” a virus on the target computer. The dropper is like the envelope in which the virus resides. The infection is a fact when the virus is installed on the computer. It is the virus itself that propagates, not the dropper. The dropper may have a name like README.exe that makes the user curious so that he or she will open the file. A dropper is actually a trojan horse, which intends to install a virus.

Macro virus:

Macro viruses can be included in file types that use a macro language, such as Word, Excel and Access. The virus propagates from one document to another, and the infection takes place when the document is opened. Some years ago macro viruses were a “popular” type of malware. In recent years they are being increasingly less wide-spread and new variants are not appearing as frequent as other types of malware.



2. Worms

A network worm infects other computers and spreads automatically in a network independent of human action. The fact that it does not rely on human action in order to propagate, helps it spread much faster than a virus. A network worm can be injected into the network initially by any type of means, for example an USB stick or as an email attachment. An email worm is transferred via email, often without the infected user being aware of it. It is characteristic for an email worm to send itself to all email addresses it finds on the infected PC. The email then appears to originate from the infected user, who may be someone you know, and can catch you off guard.

3. Trojan

A trojan – or a trojan horse - is a program that seems harmless at first glance. It can in fact appear to be useful and trick you into using it. But then, while the program is running, the trojan may open backdoor(s) and expose your computer to hackers. Normally, the immediate damage will be

insignificant, but it leaves your machine unprotected, enabling criminals to steal sensitive information and/or to remotely take control of your machine for malicious purpose.

4. Spyware

Spyware is any form of technology that is used to collect information about a person or an organization without their knowledge or consent. Spyware is often secretly installed, either when a file is downloaded or by clicking on a pop-up commercial.

Note

The majority of spyware programs are not easily deleted.

Spyware programs can reset your auto signature, disable or bypass your uninstalled features, monitor your keystrokes, scan files on your drive, access your applications, change homepages, in addition to displaying advertising content online or offline.

The best programs are the proactive antivirus solutions that do not rely on traditional signature-based technology.

They can read, write and delete files and even reformat your hard drive, while at the same time sending a steady stream of information back to the person that controls the spyware. Once installed, some of these programs cannot easily be deleted from your system by normal methods. They often leave components behind to continue to monitor your behavior and reinstall themselves.

5. Adware

Adware is closely connected with spyware, and many spyware programs are installed with the intention of running adware programs. Adware software launches advertisements, most often in the form of pop-ups. These are customized to you as a user, primarily based on your behavior on the Internet which may be monitored by spyware.

6. Backdoor

A backdoor is a program that opens your computer for access that you did not intend to allow. Such backdoors may therefore enable remote access, bypassing the authentication schemes that you may have set up to be secure.

The backdoor programs will typically open certain ports that the author tries to connect to. If someone has “succeeded” in infecting several computers with backdoors, he/she may scan whole computer ranges to identify and use them for special tasks, for example as zombie computers (see below).

7. Combinations of malware

Lately there has been a rapidly growing trend where malware combines several of the above mentioned threats. Worms are used to spread viruses that install

backdoors and spyware, while spyware programs are used to direct tailor-made advertisements to you and even use your PC as a mail server to send spam (see below).

The most noticeable, however is the ability for malware to update themselves by downloading new components from the Internet. These new modules could in principle be anything, and may introduce new types of malware compared to the original one as well as new functionality.

The differences between the various kinds of threats are becoming more blurred. The authors of malware are now dominated by commercial interests with substantial resources. The result is that malware has become significantly more sophisticated.

OTHER TYPES OF THREATS

1. Spam

Spam may be defined as unwanted emails that are sent randomly in batches. It is an extremely efficient and cheap way to market any product. Most users are exposed to spam, which is confirmed in surveys that show that more than 50% of all Internet emails are spam.

Note

Surveys show that more than 50% of all Internet emails are spam.

Spam is not a direct threat, but the amount of emails generated and the time it takes for organizations and single-users to relate to it and remove it, represents an annoying and expensive element to Internet users and organizations.

Spam is also used to send different kinds of malware of the types discussed above.

2. Phishing

Phishing is the act of fraudulently acquiring sensitive personal information such as passwords and credit card details. This is accomplished by disguising for example a phishing attempt as an official-looking email, trying to impersonate someone trustworthy with a legitimate need for information. Popular targets are users of online banking services, and auction sites.

Phishers usually work by sending out email spam to a large number of potential victims. These emails direct the recipient to a web page, which appears to belong to his/her online bank, but in fact captures the account information for the phisher's illegitimate use.

A special variant of phishing is so-called "spear phishing", which targets only a small group of recipients (e.g. company leaders). This enables more advanced customized phishing attempt.



3. Pharming

Pharming is a more sophisticated form of phishing. Pharmers exploit the DNS system, i.e. the system that translates a computer address into an Internet Protocol address (IP address). By doing this the pharmers can create e.g. a fake web site that looks like the real one, for instance a web bank site, and then harvest information that the users think they are giving to their real bank. Pharming is also referred to as DNS-poisoning.

4. Distributed Denial of Service attacks

Several high profile web sites have been attacked by so-called Distributed Denial of Service-attacks. (DDoS attacks). These attacks are often made by several bots (short for “robots”) that simultaneously send out large amounts of request to one particular machine or network. As a consequence, the workload chokes the network or machine for legitimate use. The attacking computers - the bots - are often computers that have open backdoors so that they can be used for this particular purpose. Presumably most of

the computer owners are unaware of this scam, and the infected computers are therefore often called “zombies”.

They are set up and ready to act when some remote hacker pushes the right button. Your machine can actually be used to perform illegal actions.

5. Keyloggers

Keyloggers are designed to record the user’s keystrokes, either from a specific application or more generally from the entire system. Keylogging allows criminals to look for particular bits of information that can be used for identity theft, intellectual property theft or other fraudulent actions.

Credit card numbers, passwords and other sensitive information can be stolen through this method.

6. Browser Helper Objects

Browser Helper Objects (BHOs) are plugin components for Internet Explorer. A BHO has full access to everything that happens in the current browser session;

Credit card numbers, passwords and other sensitive information can be stolen through keylogging.

it is able to see which pages are shown, how they are shown and it can and does change the sides before they are exposed. In spite their bad reputation, BHOs are often used for legitimate purposes, like downloading, tooltips and popup removers.

Note

Norman has several products that ensure your safety on the Internet. Check them out at www.norman.com

7. Rogue security software

A special type of threat is software that claims to be security software, but is actually malware aimed to trick users that install this software to pay a (small) sum of money to be really protected (which they will not be). There are numerous examples of this, in particular software that pretends to be antispyware and antivirus programs.

SPREADING MECHANISMS

In the old days of computer viruses, the main spreading mechanism was by diskettes. This type of media is now almost not in use at all, and newer and more effective spreading technology has evolved.

These days malware often exploits known vulnerabilities in various types of applications and operating systems to propagate. It is not uncommon that the malware attempts to utilize several different vulnerabilities in various applications.

Email attachments

Malware as an attachment to emails was the most popular spreading mechanism at the end of the last and the beginning of this century. The technique used was that an attachment to an email was infected and some users were tricked to click on that attachment. When the attachment was run, the computer became infected.

Malware spreading by email is often accomplished by email worms that send themselves automatically without the infected user's knowledge.

Network spreading

Among the most dangerous malware spreaders for organizations are those who spread over networks, attempting to infect network shares. One infected computer may infect a large network in seconds.

Since these network spreaders are so quick and efficient in their infection mechanism, they may be extremely difficult to get rid of.

USB sticks

These may be viewed as the diskettes' successors. Easy to transport, and with storage capacity sufficient for most purposes when the goal is to move data from one computer to another.



Unfortunately they are efficient as malware spreaders as well, particularly when a computer's autorun functionality is enabled. Since USB sticks are small, portable devices plugged into individual computers, they will often not be included in an organization's security policy regarding introducing new devices to the network.

Infected web sites

One of the most popular spreading vectors these days are infected web sites. Normally such infections are carried out without the knowledge of the web site's owner – for example by exploiting a software vulnerability in the web server's applications.

Innocent surfers are then tricked – by several different techniques – to visit an infected web site. The result is that the surfers themselves are infected.

This type of infection scenario is often called “Drive-by infections”.

PROACTIVE VS TRADITIONAL ANTIVIRUS SOLUTIONS

The difference between traditional signature-based antivirus solutions and the new proactive antivirus technology can be the difference between life or death for your computer systems. Proactive solutions are able to detect new threats that signature-based solutions are unable to cope with. As the virus authors are becoming far more advanced and new virus variants are flooding the net, traditional solutions are no longer sufficient. The need for proactive solutions is urgent.

This is a brief description of the two technologies.

Traditional antivirus solutions

With traditional signature-based antivirus solutions, a virus has to be discovered by someone, identified as a virus and analyzed before the antivirus industry can provide proper protection. Only after these necessary initial steps are completed, a virus signature file can be published. In average it takes 6 to 24 hours before an updated signature file is

distributed. This file is used for updating each and every customer's antivirus program in order to detect and stop the virus infection attempts from that point in time. Obviously, the period from the virus is published until an updated signature file is distributed, is critical to the users who still run a potential risk of being infected by the actual virus.

Note

Proactive antivirus solutions can detect new and unknown viruses.

Proactive solutions

A proactive antivirus solution detects new and unknown viruses without updated signature files. Norman has unique proactive solutions.

Norman SandBox®

Norman SandBox® is actually a fully simulated computer environment isolated from the real processing environment.

All incoming files enter the simulated computer (the SandBox). Here the files are monitored and if any suspicious action is discovered, the file will be stopped

You can check your files for viruses for free at Norman SandBox Center. Try it on <http://sandbox.norman.no/>

and denied access to the real computer. If it acts according to expected behaviour it will be granted permission to the real computer. So-called Day Zero attacks – assaults that take place the same day a software vulnerability is publicly known and a malicious program that exploits this vulnerability is created – is an increasing threat. Only proactive solutions are able to cope with this threat.

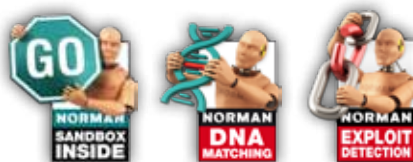
Norman DNA Matching

Computer code and instructions can be seen as the sequences of a program’s “DNA profile”. Norman uses this approach to detect and stop new malware that has not yet been fingerprinted (with virus signatures) in the traditional way. If a new malware looks like a mutation of a previously known malware - in the sense that it has inherited or reused some of the same or similar malicious code - we can conclude that it is most probably malware of the same family.

When new unknown programs are created and distributed Norman uses the DNA Matching technology to determine whether such programs have malicious, suspicious or legitimate behaviour. If too much of a new program’s DNA consists of malicious elements the new program is most likely malicious too.

Norman Exploit Detection

is a technology for detecting malware exploiting vulnerabilities in widely used document types like, OLE2 (Office documents), MDB (Access), WMF (Windows Media File), JPEG (pictures), RIFF (Windows media meta-format) and SWF (Flash).





NORMAN OFFICES

Norway

Norman ASA
Strandvn. 37, Postboks 43
1324 Lysaker, Norway
Tel: +47 67 10 97 00
Email: norman@norman.no
Web: 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
Web: www.norman.com/dk

Sweden

Norman Data Defense Systems AB
Södra Grytsgatan 7, 3tr, Norrköping Science Park
602 33 Norrköping, Sweden
Tel: +46 011 - 230 330
Email: sales.se@norman.no
Web: www.norman.com/se

United Kingdom

Norman Data Defense Systems (UK) Ltd
CBXII, West Wing
382-390 Midsummer Boulevard
Central Milton Keynes
MK9 2RG, UK
Tel: +44-01908 847413
Email: norman@normanuk.com
Web: 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
Web: www.norman.de

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

Switzerland

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

Netherlands, Belgium, Luxembourg

Norman Data Defense Systems B.V
Diamantlaan 4
Postbus 159
2130 AD Hoofddorp, The Netherlands
Tel: +31-23-7890222
Email: info@norman.nl
Web: www.norman.nl

France

Norman Data Defense Systems
Centre NCI
8 rue de Berri
75008 Paris, France
Tel: + 33 1 42 99 94 14
Email: info@norman.fr
Web: 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
Web: www.normandata.es

Italy

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

Norman Data Defense Systems, Inc.
2603 Camino Ramon, Suite 200,
San Ramon, CA-94582, USA
Tel: +1 (703) 279-6668
Email: sandbox@norman.com
Web: www.norman.com
www.malwareanalyzer.com

Norman ASA is a world leading company within the field of data security, internet protection and analysis tools. Through its SandBox technology Norman offers a unique and proactive protection unlike any other competitor.



While focusing on its proactive antivirus technology, the company has formed alliances which enable Norman to offer a complete range of data security services. Norman was established in 1984 and is headquartered in Norway with continental Europe, UK and US as its main markets.

NORMAN[®]