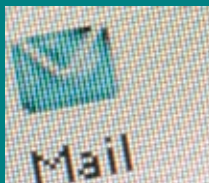


The little green book of phishing



NORMAN®

www.norman.com



The little green book of phishing

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.

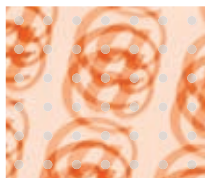
Names of products mentioned in this documentation are either trademarks or registered trademarks of their respective owners. They are mentioned for identification purposes only.

Copyright © 2006 Norman ASA.

All rights reserved.



Content



What is phishing really?.....	4
Phishing includes	4
Different forms of phishing.....	5
How can phishing be prevented.....	8
Why protect your email infrastructure with Norman?.....	10

What is phishing really?

- and some possible counter measures to prevent phishing attacks.

Most security organizations hold phishing to be one of the most prevalent threats against computer security during 2006. The Gartner Group estimates that the direct phishing-related loss to US banks and credit card issuers in 2003 was \$ 1.2 billion.

Phishing is a complex phenomenon that includes so-

cial factors as well as technology. In brief, phishing can be explained as a kind of online identity theft in which confidential information is obtained from an individual or an organization.

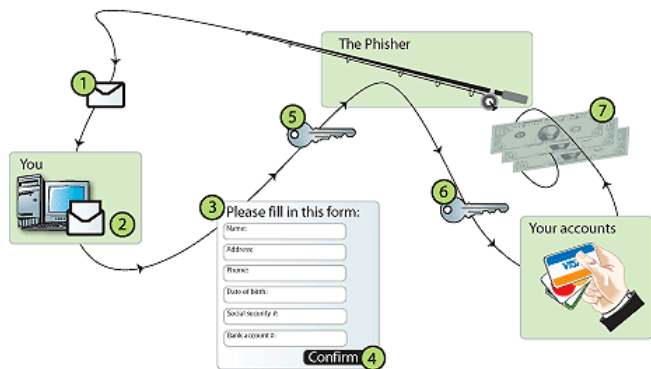
Phishing includes

- deceptive attacks, in which users are tricked by fraudulent messages into giving out information
- malware attacks, in which malicious software causes data compromises
- DNS-based attacks, in which the look-up of host names is altered to send users to a fraudulent computer aka “pharming”.



The first recorded mention of phishing took place in January 1996, although the term may have appeared even earlier. The term phishing was coined by crackers attempting to “fish” for accounts from unsuspecting AOL members.

- ① The phisher prepares for attack
- ② A malicious payload arrives through some propagation vector
- ③ The user takes an action that makes him or her vulnerable to an information compromise
- ④ The user is prompted for confidential information, either by a remote web site or locally by a trojan
- ⑤ The confidential information is transmitted from a phishing server to the phisher
- ⑥ The confidential information is used to impersonate the user
- ⑦ The phisher engages in fraud using the compromised information



Source: Aaron Emigh, Radix Labs (with sponsorship from US Department of Homeland Security, Science and Technology Directorate)

Different forms of phishing

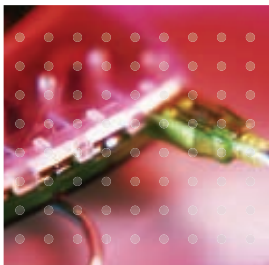
Phishing is perpetrated in many different ways. Phishers are technically innovative and are often able to invest in technology. Most phishing attacks are carried out as professional

crime schemes. As financial institutions have increased their online presence, the economic value of compromising account information has increased dramatically.

Phishing thus includes many different types of attacks including:

1. Deceptive attacks, in which users are tricked by fraudulent messages into giving information.

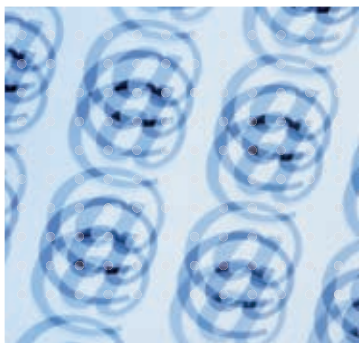
The most common method for deceptive phishing today is email. In a typical scenario, a phisher sends deceptive emails, in bulk,



with a “call to action” that demands the recipient to click on a link. Examples of a “call to action” include:

- A statement that there is a problem with the recipient’s account data with a financial institution or other businesses. The email asks the recipient to visit a web site to correct the problem, using a deceptive link in the email.
- A statement that the recipient’s account is at risk, and offering to enrol the recipient in an anti-fraud program
- A fictitious invoice for merchandise, often offensive merchandise, that the recipient did not order, with a link to cancel the fake order
- A fraudulent notice of an undesirable change made to the user’s account, with a link to “dispute” the unauthorized change
- A claim that a new service is being rolled out at a financial institution, and offering the recipient, as a current member, a limited time opportunity to get the service for free.

In many cases the phisher does not directly cause the economic damage,



Like phishing, pharming aims to gather personal information from unsuspecting victims; the difference is that pharming doesn't rely on email solicitation to ensnare its victims, and it can be done without any active mistake on the part of the victim.



ity vulnerability. A typical social engineering attack is to convince a user to open an email attachment or download a file from a web site; often claiming the attachment has something to do with pornography, salacious celebrity photos or gossip.

but resells the illicitly obtained information on a secondary market.

2. Malware attacks, in which malicious software causes data compromises.

This refers to any type of phishing that involves running malicious software on the user's machine. In general this malware is spread either by social engineering or by exploiting a secu-

Malware attacks can also take place in forms of keyloggers that install themselves either into a web browser or as a device driver, which monitor data input and send relevant data to the phisher's computer. Web trojans are malicious programs that pop up over login screens to collect credentials.



3. DNS-based attacks, in which the look-up of host names is altered to send users to a fraudulent server.

This refers to any form of phishing that interferes with the integrity of the look-up process for a do-

main name. This includes host file poisoning, even though the host file is not properly part of the Domain Name System.

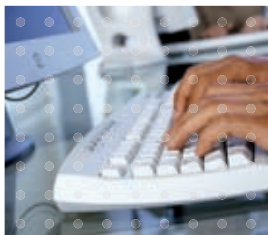
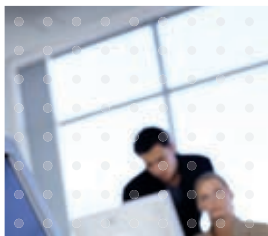
This form for phishing is often very sophisticated and is also referred to as “pharming”.

How can phishing be prevented?

It is not an easy task to stay fully protected against phishing attacks, but there are some measures that can be taken in order to reduce the danger:

1. **Monitoring** potentially malicious activity such as web site usage and domain registrations made by the users, detecting a phishing attack before it starts, and interrupting the phisher’s preparations. Pre-emptive domain registrations targeting likely spoof domain names may reduce the availability of the most deceptively named domains.

2. **Authenticating** email messages so unauthenticated messages can be discarded. Once a phishing attack is under way, the first opportunity to prevent a phishing attack is to prevent a phishing payload, such as an email or security exploit from ever reaching



Once a phishing attack is under way, the first opportunity to prevent a phishing attack is to prevent a phishing payload, such as an email or security exploit from ever reaching users.



The use of ph in “phishing” and “pharming” is a common hacker replacement for f, and is a nod to an older form of hacking known as “Phone breaking”.

users. Message authentication provides an assurance that an email was really sent by the party named as the sender. Once widely deployed, email authentication has the potential to prevent forgery of a return address and force a phisher to either reveal a suspicious looking return address, or register an official looking domain name.

3. Detecting the unauthorized use of trademarks, logos and other proprietary imagery.

4. Improving the security patching infrastructure to increase resistance to malware that utilizes vulnerabilities in installed software. Phishing at-

tacks that involve malware are often installed via an exploit of a security vulnerability. One promising proposal for rapid distribution and application of patches, without leaking vulnerability information, is to distribute focused security patches for specific vulnerabilities encrypted using a separate symmetric key for each patch. The key will be kept secret by each vendor.

5. Using personalized information to authenticate an email directly to a user.

6. Detecting a fraudulent web site and alerting the legitimate organization that is being an indirect victim of the scheme.

7. Using mutual authentication protocols.

8. Establishing a trusted path between the user and a web site to ensure that information can be used only by its intended recipient.

Why protect your email infrastructure with Norman?

We give you the best options on how to protect your email infrastructure. Software, Appliance or Managed Service? The choice is yours...



Norman Online Protection

A subscription service that protects networks from all inbound and outbound email threats.

www.norman.com/nop



Norman Email Protection

An email security solution with sophisticated management tools including a rock-solid perimeter defense guarding the perimeter of the corporate network.

www.norman.com/nep



Norman NetProtector 3000

Pre-loaded gateway appliance providing email security against virus, spam and phishing. Installed in less than 15 minutes!

www.norman.com/np3000



Norway

Norman ASA
Strandvn. 37
Postboks 43
1324 Lysaker, Norway
Phone: +47-67 10 97 00
norman@norman.no
www.norman.no

Denmark

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

Sweden

Norman Data Defense Systems AB
ProNova Science Park
Korsgata 2
602 33 Norrköping, Sweden
Phone: +46-011-230 330
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
Phone: +44-1908 678496
norman@normanuk.com
www.normanuk.com

Germany

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

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

Switzerland

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

Benelux

Norman / SHARK BV
Postbus 159
2130 AD Hoofddorp, The Netherlands
Phone: +31-23-789022
info@norman.nl
www.norman.nl

USA

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



www.norman.com : stay updated



NORMAN[®]