Social Engineering is Not This Obvious

Internet social engineering is getting more sophisticated.

Protect yourself and learn to recognize social engineering scams such as phishing, pharming, and spoofing.

FREE NUIT TECH TALK
Unmasking Social Engineering
Friday, April 7 • Noon - 1 p.m.
University Library Forum Room
and Wieboldt Hall, Room 421

Please register online at
www.it.northwestern.edu
Social Engineering

Dave Kovarik

Director, Information & Systems Security/Compliance
What is Social Engineering?

• Obtaining confidential information by manipulation

• **Tricking** people into revealing sensitive information

• **Exploiting** the natural tendency of a person to trust and assist others
What’s at Risk?

For You:
• Identity information lost
• Money stolen from credit cards or bank accounts
• Computer unavailable if it is infected or crashes

For University:
• Campus computers and servers unsecured or unreliable
• Confidential data or information lost
• Violation of federal and state privacy laws
What’s at Risk?

• **In Brazil:**
  
  Computer fraud ring steals passwords and $450 million from 200 online bank accounts

• **From Sophos network security company:**
  
  Unprotected computers have a 94% chance of being infected after one hour online
What Does it Look Like?

• A telephone caller asking for personal or sensitive information
• Dumpster diving
• A cry for help
• Who was that guy?
• Certificate mismatch
### What Does it Look Like?

#### How You Might Respond:

<table>
<thead>
<tr>
<th>Situation:</th>
<th>Response:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephone caller asking for personal or sensitive information</td>
<td>“You tell me my account information, and I’ll tell you if it is correct.”</td>
</tr>
<tr>
<td>Dumpster diving</td>
<td>Shred papers with personal information</td>
</tr>
<tr>
<td></td>
<td>“Wipe clean” or destroy computer files and media</td>
</tr>
</tbody>
</table>

Information Technology
What Does it Look Like?

How You Might Respond:

<table>
<thead>
<tr>
<th>Situation</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>A “Cry for Help”</td>
<td>Just say “No”</td>
</tr>
<tr>
<td>Who was that guy?</td>
<td>“Can I help you?”</td>
</tr>
<tr>
<td>Certificate mismatch</td>
<td>Don’t accept it</td>
</tr>
</tbody>
</table>
What Does it Look Like Online?

- Phishing
- Spoofing
- Pharming
- Malware
Can You Spot Phishing?

Some of the latest scams:

• Look very professional
• Have fewer typos
• Can come through IM
• Make “For Free” offers
• Directs you to a spoof web site or installs malware on your computer
Can You Spot Phishing?

Phishers can also hijack University identifiers such as logos and “from” addresses

How to spot it:
- University e-mails will never request your NetID or password/passphrase
- Be skeptical of any University e-mail with a Zip file attached

How to protect yourself:
- Double check anything that looks suspicious
- Use the Online Directory to verify the sender
Can You Spot a Spoof?

Some of the latest scams:

• Look identical to the real site

• Collect your account & login

• Are connected from a phishing e-mail or address typo
What is Pharming?

• A sophisticated form of Phishing

• Plants virus seeds which come alive when you browse to a specific Web site

• Virus redirects browser to a spoof site, and steals login information

The Growing Technical Complexity of Phishing Attacks

Source: Computer Economics, 2006
How Does this Relate to Malware?

- Spread by Phishing and Spoofing
- Malicious software causes system instability or steals information

- **Trojans** – Gathers information or performs commands
- **Worms** – Spreads through e-mail and IM links or attachments
- **Viruses** – Infects executable files (*.exe) and can modify other programs
- **Keystroke Loggers** – Tracks information entered on a keyboard, stealing credit card numbers, passwords, etc.
Malware — How Can You Tell?

If your computer is infected by malware, you might notice:

– Computer slowness
– Changes to your browser homepage
– Changes to your computer desktop
– Excessive pop-up ads
What is NUIT Doing?

E-mail Defense System (EDS)

• EDS processed 89 million messages in first three months of 2006

• Of those, almost 50% were junk and 400,000 were viruses, which EDS prevented from delivery
Remember, EDS is not Perfect

- Some scams may still penetrate EDS and end up in your Northwestern inbox

- EDS doesn’t protect your personal mail accounts (from Gmail or Hotmail)
What is NUIT Doing?

• Established Incident Response Protocol (IRP)
• Developing policy & standards
• Promoting security awareness
• Assessing physical security
• Focusing on people, processes, and technology
What Else is NUIT Doing?

E-mail obscuring for the Online Directory:

t-test@northwestern.edu

- Helps protects your e-mail address from harvest programs
- Helps reduce the junk e-mail you receive
- Does not change the directory for on-campus users
What You Can Do

- Get & stay aware
- Protect yourself at all times
- Protect your computer
- Use your intuition
- Trust but verify
- Get a second opinion
What You Can Do

Awareness

• Maintain a healthy skepticism

• Learn more at www.it.northwestern.edu

• NUIT Social Engineering Security Tip of the Month at ../security/tip-of-the-month/

• Share your knowledge with others
What You Can Do

Awareness: Learn More

• SANS Institute
  Information security organization
  http://www.sans.org/rr/whitepapers/engineering/

• Federal Trade Commission
  http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm

• Anti-phishing Working Group
  http://www.antiphishing.org/

• Anti-pharming site
  http://www.pharming.org/
What You Can Do

Protect Yourself

• Keep passwords/passphrase and NetID secret

• Use different passwords for different classes of information

• Be skeptical of any request for social security numbers, credit card numbers, or other important information

• For personal IM use, block traffic from unfamiliar sources
What You Can Do

Protect Yourself

• Share information wisely!
  – Do not send important personal information such as SSNs or credit card numbers via e-mail

• Harvesters can easily capture live address links, so:
  – Protect your @northwestern.edu account
  – Do not use it to post blogs or discussion board messages
  – Use free e-mail accounts (Hotmail, Yahoo) for all non-university transactions
What You Can Do

Protect Your Computer

Keep your firewall and security software current
- Antivirus software
- Software updates
- Spyware detection
- Firewall protection

Follow 5 easy steps at:
http://www.it.northwestern.edu/5steps/
What You Can Do

Use Your Intuition

• Maintain healthy skepticism any time you use the Internet

• Watch for unexpected e-mail or IM, even from organizations you are familiar with
What You Can Do

Trust but Verify

• Double check sites’ URLs

• Look for “https” when entering personal information, this indicates a secure site

• Don’t click on links directly from an e-mail, enter the address yourself
What You Can Do

Get a Second Opinion

Offer sound too good to be true? It probably is!

“Free” offers for ring tones, screen savers, etc., may contain malware or may sell your information

Ask others about their experience with the site or offer before you download
If You Think You’ve Been Had…

• Take notes
• Preserve evidence
• Contact authorities
• Go to the FTC: www.ftc.gov
  – Take Charge: Fighting Back Against Identity Theft
Social Engineering
Questions?

Dave Kovarik
Information & Systems
Security/Compliance
(847) 467-5930
david-kovarik@northwestern.edu
NUIT Resources

Learn more at www.it.northwestern.edu/

NUIT Social Engineering Security Tip of the Month
www.it.northwestern.edu/security/tip-of-the-month/

“Get Control” Web site
www.it.northwestern.edu/5steps/

Computer and Network Security
www.it.northwestern.edu/security/
Please Join Us for the Next Tech Talk

Spring Cleaning: Keeping Your Computer in Great Shape

Next Friday, April 14, 2005
Same locations, Noon – 1 p.m.

Please register online: www.it.northwestern.edu