How attackers use social engineering to bypass your defenses.

Lenny Zeltser
Senior Faculty Member, SANS Institute
Product Management Director, NCR Corporation
Social engineers influence victims to perform actions desired by the attacker.
As the result:

Outsider == Insider
What social engineering tactics are being used?

Let’s look at examples, so we can learn from them.
Alternative Channels
Notices in the “physical” world invited victims to visit a fraudulent website.
PARKING VIOLATION

This vehicle is in violation of standard parking regulations.

To view pictures with information about your parking preferences, go to HORRIBLEPARKING.COM
<table>
<thead>
<tr>
<th>Registration of the International Trademark</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RENEW</strong></td>
</tr>
</tbody>
</table>

| CANADA                                     |

<table>
<thead>
<tr>
<th>Registration Number:</th>
</tr>
</thead>
<tbody>
<tr>
<td>3,840,247</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Publication Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010/08/31</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>International Class(es):</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>By Cheque</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Beneficiary:</th>
</tr>
</thead>
<tbody>
<tr>
<td>WDTP s.r.o.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td>P.O. BOX 652, CZ-66152 Brno, Czech Republic</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>By Credit Card</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Visit URL:</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://app.wipd.biz/pay/1000317423">http://app.wipd.biz/pay/1000317423</a></td>
</tr>
</tbody>
</table>

Source: Jerome Segura http://j.mp/IQjPhM
Phishing scam directed the target to a phone number.
“Your card has been suspended because we believe it was accessed by a third party. Please press 1 now to be transferred to our security department.”

Customers of Liberty Bank of Boulder Creek, CA

Source: BankInfoSecurity http://j.mp/3Gj0AA
USB keys were used as an infection vector.
Action=Open folder to view files
Icon=%systemroot%\system32\shell32.dll,4
Shellexecute=..\RECYCLER\S-5-3-42-28199...

(Conficker)

Source: Internet Storm Center http://j.mp/HGTgRX
“Real world” procedures were used to place malicious ads on Gawker sites.

A similar scam targeted the New York Times and other media sites.

See http://j.mp/IjqYWJ
The ads served PDF exploits to visitors.

Image Source: Business Insider
http://j.mp/IwnntL
“We want to run a performance campaign for Suzuki across your network. Our budget to start is $25k+. Campaign should be live by the end of the month.”

Source: Mediaite http://j.mp/HJO77c
Scammers called home users to help disinfect their PCs.

They pretended to find malware and clean it up; requested payment and other details.
“i got a call off a onlinepcdoctors.com and they said my pc was running slower because of malicious [sic] files. i let them take remote access of my computer...”
ZeuS on a Windows PC asked victims to install a security program on their Android phones.
Due to the becoming more frequent internet fraud cases with text messages it is strongly recommended to the customers owning mobile phones with Android OS to install a special program which will help to protect you from fraud.

For the software installation open the internet browser on the mobile and enter the following URL address:

http://[redacted].com/tr.apk

When the installation is completed you’ll see a new program called “Trusteer Rapport”. Open it from the Application folder on your mobile. You need to start the program then enter the activation code indicated there into the field below and press "Activate".

Activation code:       

Source: Kaspersky http://j.mp/pN6p60
Personally-Relevant Messaging
Malware spread by localizing its message (Waledac).

Powerful explosion burst in New York this morning.

At least 12 people have been killed and more than 40 wounded in a bomb blast near market in New York. Authorities suggested that explosion was caused by "dirty" bomb. Police said the bomb was

See http://j.mp/IG10kH
Geolocation was similarly used in a work-from-home scam.

Kelly Richards of **Clifton, New Jersey** is a regular mom who lost her job last year, after an unsuccessful job hunt. She was contacted by a fraudster who pretended to be a representative from a company in need of remote workers.

Kelly Richards of **Portland, Oregon** is a regular mom who lost her job last year, after an unsuccessful job hunt. She was contacted by a fraudster who pretended to be a representative from a company in need of remote workers.

Kelly Richards of **Roubaix, Nord-Pas-de-Calais** is a regular mom who lost her job last year, after an unsuccessful job hunt. She was contacted by a fraudster who pretended to be a representative from a company in need of remote workers.

See [http://j.mp/HGVHU9](http://j.mp/HGVHU9)
Malware spoofed email from trusted senders.
“Unfortunately we were not able to deliver the postal package ...

Please print out the invoice copy attached and collect the package at our department.

United Parcel Service of America.”

Source: Webroot http://j.mp/HHuYVB
Malicious messages matched the content the victim was used to receiving.

The attachments targeted client-side vulnerabilities.
Hi everyone!

I hope everyone has been as busy as I have reviewing our set of reference documents! With the meeting approaching, we can maximize our productivity with everyone familiar with the various projects & activities and ensure a smooth work effort.

here is an agenda outline for the upcoming meeting.

I look forward to seeing everyone there, and hope your week was uneventful.

-Alexis
Hey Neil, it’s Michelle here, it has been a long time huh? how’re you doing? how’s work? Is everything ok there? Hey, can you believe it! I got married to Brian! Yes believe me! I have no answer. You have changed your number, haven’t you? Just give me your current number in this mail. It’s really a pity that we did not see you in our wedding. I wanted to see you. I’m sending you a few pics taken in our wedding:

http://www.weddingphotos4u.net/Photos/Michelle/

Let’s keep in touch then.

Love,

Michelle & Brian
Attackers provided customer service to appear legitimate.

Image Source: Symantec
http://j.mp/HJOwGU
Fraudsters used Facebook chat for the “stuck in London” scam.

Source: Jason Cupp
http://j.mp/k9JFf9
Profile Spy claimed to track who viewed victims’ Facebook profiles.
Social Compliance
Malware spoofed product review sites to legitimize a fake anti-virus tool.
AntiVirus2010

REVIEW DATE: 08.08.08

✓ Editor's Rating: ⭐⭐⭐⭐⭐
✓ Reader Rating: ⭐⭐⭐⭐⭐

Discuss Total posts: 53

Buy It Here: $49.95 - $69.95

By Neil J. Rubenking

Symantec continues to polish and enhance its flagship AntiVirus2010 suite. The 2008 edition adds full-scale password and identity management, and its new BrowserDefender technology offers even stronger defense against Web-based attacks. AntiVirus2010 now offers a
Social networks have been used to spread malware (Koobface).
My home video :)  
http://tinyurl.com/l4bslp

Abel Saavedra Amazing Video http://snimka31082009.com/youtube seefilm

snimka31082009.com
Source: snimka31082009.com

Yesterday at 7:09am
Want 2 C Something Hot?

on, baby!
Malware dared victims to click the link to get them hooked.

Then asked to copy and paste JavaScript to spread on Facebook.
Copy the code below, paste it into your browser's address bar and press enter to load this video. Plz wait 7-8 secs for processing!!!
Malware manipulated download counters to appear popular (Nugache).

Source: Dave Dittrich http://j.mp/ITKJs7
This is a sample screenshot. It’s not representative of the sites actually manipulated by Nugache.
Money-mule recruiting sites looked like sites of many other legitimate companies.
Welcome To Our Company

24 Hour Express Service company the competence of leading consultants, specialists and analysts in the sphere of investment and strategic consulting. Project groups and a high-qualified manager are assigned to each project. This method guarantees individual approach to every client, adequate understanding of his problems and in the meantime allows solving a complete range of objectives settled. Competence in business specificity of every client ensures a high level of service granted.
A scam emphasized the popularity of the “work from home” kit.

See http://j.mp/HGVHU9
Reliance on Security Mechanisms
Similar to the fake counterfeit money-testing pen con.
“Security update” messages in several forms convinced users to download and install software.
Flash Player upgrade required
You must download and install the latest version of the Adobe Flash Player to view this content.

Download Flash

Welcome to Video
Your life in motion.

Share your personal videos.
Upload and tag videos of you and your friends on Facebook. Upload a new video

Record and send video messages.
Use your webcam to record yourself in a video message. Record a video message
Fake anti-virus tools confused the user about the need for security.
**Windows Internet Explorer**

NOTICE: If your computer is infected, you could suffer data loss, erratic PC behavior, PC freezes and crashes. Detect and remove viruses before they activate themselves on your PC to prevent all these problems.

Do you want to install AntiSpywareMaster to scan your PC for malware now? (Recommended)

**OK**  **Cancel**

---

**There were errors during security settings restore!**

System has detected spyware infection! It is recommended to use antispyware tool to prevent data loss and privacy information exposure.

Click OK to download antispyware tool

**OK**

---

**Security**

- Allow active content from CDs to run on my computer*
- Allow active content to run in files on My Computer*
- Allow software to run or install even if the signature is invalid
- Check for publisher's certificate revocation
- Check for server certificate revocation*
- Check for signatures on downloaded programs
- Do not save encrypted pages to disk
- Empty Temporary Internet Files folder when browser is closed
- Enable Integrated Windows Authentication*
- Enable native XMLHTTP support
- Phishing Filter
  - Disable Phishing Filter
    - Turn off automatic website checking
    - Turn on automatic website checking
  - SSL 2.0
Victims sometimes even got to choose their preferred rogue anti-virus product.
<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Scan result</th>
<th>Bases update</th>
<th>Removal tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOD32 Anti-Virus System</td>
<td>Nothing</td>
<td>1 hours ago</td>
<td>Free Install</td>
</tr>
<tr>
<td>Red Cross</td>
<td>Unknown Trojan</td>
<td>6 hours ago</td>
<td>Free Install</td>
</tr>
<tr>
<td>IKARUS security software</td>
<td>Nothing</td>
<td>6 hours ago</td>
<td>Free Install</td>
</tr>
<tr>
<td>VirusBuster</td>
<td>Nothing</td>
<td>24 hours ago</td>
<td>Free Install</td>
</tr>
<tr>
<td>Dr. Web</td>
<td>Nothing</td>
<td>2 hours ago</td>
<td>Free Install</td>
</tr>
<tr>
<td>avast!</td>
<td>Nothing</td>
<td>24 hours ago</td>
<td>Free Install</td>
</tr>
<tr>
<td>Peak Protection</td>
<td>Trojan Horse</td>
<td>24 hours ago</td>
<td>Free Install</td>
</tr>
<tr>
<td>McAfee</td>
<td>Nothing</td>
<td>1 hours ago</td>
<td>Free Install</td>
</tr>
<tr>
<td>bitdefender</td>
<td>Nothing</td>
<td>3 hours ago</td>
<td>Free Install</td>
</tr>
<tr>
<td>SOPHOS</td>
<td>Nothing</td>
<td>3 hours ago</td>
<td>Free Install</td>
</tr>
<tr>
<td>eTRUST</td>
<td>Nothing</td>
<td>Last bases</td>
<td>Free Install</td>
</tr>
<tr>
<td>AVG</td>
<td>Nothing</td>
<td>24 hours ago</td>
<td>Free Install</td>
</tr>
<tr>
<td>Clam AV</td>
<td>Nothing</td>
<td>11 hours ago</td>
<td>Free Install</td>
</tr>
</tbody>
</table>

Source: Sunbelt Software http://j.mp/IG29Jh
Malicious files were hosted behind a CAPTCHA screen.

See http://j.mp/HGWfJF
Scammers associated their "products" with trusted brands.
Generic Kamagra 10 capsules x 100mg = $68.84. Bonus pills. Mastercard and Visa

Kamagra (Generic) 30 capsules x 100mg = $195.98  No prescription required, Confidentiality, Guaranteed Fast Worldwide Delivery, 24/7 customer service.

http://www.bestedrugsite.com

Buy brand Kamagra online

Get quality medication online. Brand Kamagra delivered to your door for 2 USD per pill.

http://www.viagramedic.com/?product=kamagra

Certified Canadian Pharmacy - kamagra

Our products it's Hight Quality Medications! No prescription needed. We
Attackers signed malware with certificates.

Some certs were stolen with malware. Some were obtained through identity theft.

See http://j.mp/9HbPLC
Certificate Information

This certificate is intended for the following purpose(s):
- Ensures software came from software publisher
- Protects software from alteration after publication

* Refer to the certification authority’s statement for details.

Issued to: C-Media Electronics Incorporation

Issued by: VeriSign Class 3 Code Signing 2009-2 CA

Valid from 8/2/2009 to 8/2/2012

Source: Websense http://j.mp/ICjrsS
Malicious websites presented a security warning to the users, asking to download an update.
Reported Attack Page!

This web page has been reported as an attack page and has been blocked based on your security preferences.

Attack pages try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack pages intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

Download Updates!

The page at http://firelovers.com says:

This web page has been blocked based on your security preferences. Click 'OK' to download and install Firefox secure updates.

See http://j.mp/ITLj9g
So What?
Social engineering works.

It seems to tap into psychological factors that are part of the human nature.
Discuss recent social engineering approaches with employees, partners and customers.
Alternative Channels

Personally-Relevant Messaging

Social Compliance

Reliance on Security Mechanisms
Assume some social engineering will work anyway.
Focus on... internal segmentation, least privilege, need-to-know and monitoring.
Lenny Zeltser
blog.zeltser.com
twitter.com/lennyzeltser
About The Author:

Lenny Zeltser is a seasoned IT professional with a strong background in information security and business management. As a director at NCR Corporation, he focuses on safeguarding IT environments of small and midsize businesses worldwide. Before NCR, he led an enterprise security consulting team at a major IT hosting provider. Lenny's most recent work has focused on malware defenses and cloud-based services. He teaches how to analyze and combat malware at the SANS Institute, where he is a senior faculty member. He also participates as a member of the board of directors at the SANS Technology Institute and volunteers as an incident handler at the Internet Storm Center.

Lenny frequently speaks on security and related business topics at conferences and industry events, writes articles, and has co-authored books on forensics, network security, and malicious software. He is one of the few individuals in the world who have earned the highly-regarded GIAC Security Expert (GSE) designation. Lenny has an MBA degree from MIT Sloan and a computer science degree from the University of Pennsylvania.