Social Engineering

Module 9

Engineered by Hackers. Presented by Professionals.
Chinese attacks 'Byzantine Candor' penetrated federal agencies, says leaked cable

Cyber espionage by Chinese military-linked hackers, part of a series of attacks code-named "Byzantine Candor," extracted at least 50 megabytes of email messages from a federal agency along with a complete list of that agency’s user names and passwords, states a newly-available leaked State Department cable.

According to the cable, which is labeled SECRET//NOFORN and is dated Nov. 3, 2008, Byzantine Candor has existed since late 2002. Its hackers have compromised multiple systems, including one U.S. commercial Internet service provider, in part through social engineering attacks, the cable states.

According to Air Force Office of Special Investigations findings referenced in the cable, hackers in Shanghai with ties to the Chinese military intelligence penetrated "at least three separate systems" at the U.S. ISP from which they were able to download the email, attachments, usernames and passwords from the unnamed federal agency during a period from April 2008 through Oct. 13, 2008.

http://www.fiercegovernmentit.com
Module Objectives

- What is Social Engineering?
- Why is Social Engineering Effective?
- Phases in a Social Engineering Attack
- Common Targets of Social Engineering
- Types of Social Engineering
- Common Intrusion Tactics and Strategies for Prevention
- Social Engineering Through Impersonation on Social Networking Sites
- Risks of Social Networking to Corporate Networks
- Identify Theft
- How to Steal Identity?
- Social Engineering Countermeasures
- Social Engineering Pen Testing
There is No Patch to Human Stupidity
What is Social Engineering?

- Social engineering is the art of **convincing people** to reveal confidential information.
- Social engineers depend on the fact that people are **unaware of their valuable information** and are careless about protecting it.
Behaviors Vulnerable to Attacks

Human nature of trust is the basis of any social engineering attack.

Ignorance about social engineering and its effects among the workforce makes the organization an easy target.

Social engineers might threaten severe losses in case of non-compliance with their request.

Targets are asked for help and they comply out of a sense of moral obligation.

Social engineers lure the targets to divulge information by promising something for nothing.
Factors that Make Companies Vulnerable to Attacks

- Insufficient Security Training
- Lack of Security Policies
- Easy Access of Information
- Several Organizational Units

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Why is Social Engineering Effective?

- Security policies are as strong as their weakest link, and humans are the most susceptible factor.
- It is difficult to detect social engineering attempts.
- There is no specific software or hardware for defending against a social engineering attack.
- There is no method to ensure complete security from social engineering attacks.
Warning Signs of an Attack

Internet attacks have become a business and attackers are constantly attempting to invade networks.

- Show inability to give valid callback number
- Make informal requests
- Claim authority and threaten if information is not provided
- Show haste and drop the name inadvertently
- Unusually compliment or praise
- Show discomfort when questioned
Phases in a Social Engineering Attack

- **Research on target company**
  - Dumpster diving, websites, employees, tour company, etc.

- **Select victim**
  - Identify the frustrated employees of the target company

- **Research**

- **Develop relationship**
  - Develop relationship with the selected employees

- **Develop**

- **Exploit**
  - Collect sensitive account information, financial information, and current technologies

- **Exploit the relationship**
Impact on the Organization

- Economic Losses
- Dangers of Terrorism
- Loss of Privacy
- Damage of Goodwill
- Temporary or Permanent Closure
- Lawsuits and Arbitrations

---

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Command Injection Attacks

Online
Internet connectivity enables attackers to approach employees from an anonymous Internet source and persuade them to provide information through a believable user.

Telephone
Request information, usually through the imitation of a legitimate user, either to access the telephone system itself or to gain remote access to computer systems.

Personal Approaches
In Personal Approaches, attackers get information by directly asking for it.
“Rebecca” and “Jessica”

Attakers use the term “Rebecca” and “Jessica” to denote social engineering victims

Rebecca and Jessica means a person who is an easy target for social engineering, such as the receptionist of a company

Example:

- “There was a **Rebecca** at the bank and I am going to call her to extract the privileged information.”
- “I met **Ms. Jessica**, she was an easy target for social engineering.”
- “Do you have a **Rebecca** in your company?”
Common Targets of Social Engineering

- Receptionists & Help Desk Personnel
- Technical Support Executives
- Users and Clients
- System Administrators
- Vendors of the Target Organization
Common Targets of Social Engineering: Office Workers

Attacker making an attempt as a valid employee to **gather information** from the staff of a company.

The victim employee gives information back assuming the attacker to be a **valid employee**.

Despite having the best firewall, intrusion-detection, and antivirus systems, you are still hit with security breaches.

Attackers can attempt social engineering attacks on office workers to extract the sensitive data, such as:
- Security policies
- Sensitive documents
- Office network infrastructure
- Passwords
Module Flow

- Social Engineering Concepts
- Social Engineering Techniques
- Impersonation on Social Networking Sites
- Identity Theft
- Social Engineering Countermeasures
- Penetration Testing
Types of Social Engineering

**Human-based**
Gathers sensitive information by interaction
Attacks of this category exploit trust, fear, and helping nature of humans

**Computer-based**
Social engineering is carried out with the help of computers
Human-Based Social Engineering

1. **Posing as a legitimate end user**
   
   Give identity and ask for the *sensitive information*
   
   “Hi! This is John, from Department X. I have forgotten my password. Can I get it?”

2. **Posing as an important user**
   
   Posing as a VIP of a target company, valuable customer, etc.
   
   “Hi! This is Kevin, CFO Secretary. I’m working on an urgent project and lost my system password. Can you help me out?”

3. **Posing as technical support**
   
   Call as technical support staff and request IDs and passwords to retrieve data
   
   “Sir, this is Mathew, Technical support, X company. Last night we had a system crash here, and we are checking for the lost data. Can you give me your ID and password?”
A man calls a company’s help desk and says he has forgotten his password. He adds that if he misses the deadline on a big advertising project, his boss might fire him. The help desk worker feels sorry for him and quickly resets the password, unwittingly giving the attacker clear entrance into the corporate network.
Hi, I am John Brown. I'm with the external auditors Arthur Sanderson. We've been told by corporate to do a surprise inspection of your disaster recovery procedures.

Your department has 10 minutes to show me how you would recover from a website crash.
"Hi I'm Sharon, a sales rep out of the New York office. I know this is short notice, but I have a group of prospective clients out in the car that I've been trying for months to get to outsource their security training needs to us. They're located just a few miles away and I think that if I can give them a quick tour of our facilities, it should be enough to push them over the edge and get them to sign up. Oh yeah, they are particularly interested in what security precautions we've adopted. Seems someone hacked into their website a while back, which is one of the reasons they're considering our company."
Hi, I'm with Aircon Express Services. We received a call that the computer room was getting too warm and need to check your HVAC system. Using professional-sounding terms like HVAC (Heating, Ventilation, and Air Conditioning) may add just enough credibility to an intruder's masquerade to allow him or her to gain access to the targeted secured resource.
Human-based Social Engineering

**Eavesdropping**
- Eavesdropping or unauthorized listening of conversations or reading of messages.
- Interception of any form such as audio, video, or written.
- It can also be done using communication channels such as telephone lines, email, instant messaging, etc.

**Shoulder Surfing**
- Shoulder surfing is the name given to the procedure that thieves use to find out passwords, personal identification number, account numbers, etc.
- Thieves look over your shoulder—or even watch from a distance using binoculars, in order to get those pieces of information.
Human-based Social Engineering: Dumpster Diving

- Dumpster diving is looking for treasure in someone else's trash.
Human-based Social Engineering

Tailgating
An unauthorized person, wearing a fake ID badge, enters a secured area by closely following an authorized person through a door requiring key access.

In Person
Survey a target company to collect information on:
- Current technologies
- Contact information

Third-Party Authorization
Refer to an important person in the organization and try to collect data
“Mr. George, our Finance Manager, asked that I pick up the audit reports. Will you please provide them to me?”
**Reverse Social Engineering**

- This is when the attacker creates a persona who appears to be in a position of authority so that employees will ask him for information, rather than the other way around.
- Reverse social engineering attack involves sabotage, marketing, and tech support.

**Piggybacking**

- "I forgot my ID badge at home. Please help me."
- An authorized person provides access to an unauthorized person by keeping the secured door open.
In the 2003 movie “Matchstick Men”, Nicolas Cage plays a con artist residing in Los Angeles and operates a fake lottery, selling overpriced water filtration systems to unsuspecting customers, in the process collecting over a million dollars.

This movie is an excellent study in the art of social engineering, the act of manipulating people into performing actions or divulging confidential information.
Computer-Based Social Engineering

- Pop-up Windows: Windows that suddenly pop up while surfing the Internet and ask for users’ information to login or sign-in.
- Hoax Letters: Hoax letters are emails that issue warnings to the user on new viruses, Trojans, or worms that may harm the user’s system.
- Chain Letters: Chain letters are emails that offer free gifts such as money and software on the condition that the user has to forward the mail to the said number of persons.
- Instant Chat Messenger: Gathering personal information by chatting with a selected online user to get information such as birth dates and maiden names.
- Spam Email: Irrelevant, unwanted, and unsolicited email to collect the financial information, social security numbers, and network information.
Computer-Based Social Engineering: Pop-Ups

Pop-ups trick users into clicking a hyperlink that redirects them to fake web pages asking for personal information, or downloads malicious programs such as keyloggers, Trojans, or spyware.
Computer-Based Social Engineering: Phishing

- An illegitimate email falsely claiming to be from a legitimate site attempts to acquire the user’s personal or account information.

- Phishing emails or pop-ups redirect users to fake webpages of mimicking trustworthy sites that ask them to submit their personal information.

Example email:

**CITIBANK Update**

We recently have discovered that multiple computers have attempted to log into your CITIBANK Online Account, and multiple password failures were presented before the logons. We now require you to re-validate your account information to us.

If this is not completed by Sep 14, 2010, we will be forced to suspend your account indefinitely, as it may have been used fraudulent purposes.

To continue please **Click Here** or on the link below to re-validate your account information:

http://www.citibank.com/update

Sincerely,
The CITIBANK Team

**Fake Bank Webpage**
Dear Valued Customer,
Our new security system will help you to avoid frequently fraud transactions and to keep your Credit/Debit Card details in safety. Due to technical update we recommend you to reactivate your card. Please click on the link below to proceed: Update MasterCard
We appreciate your business. It’s truly our pleasure to serve you.
MasterCard Customer Care.
This email is for notification purposes only.
msg-id: 1248471

Dear HSBC Online user,
As part of our security measures, the HSBC Bank, has developed a security program against the fraudulent attempts and account thefts. Therefore, our system requires further account information. We request information from you for the following reason. We need to verify your account information in order to insure the safety and integrity of our services. Please follow the link below to proceed.
Proceed to Account Verification
Once you login, you will be provided with steps to complete the verification process. For your safety, we have physical, electronic, procedural safeguards that comply with federal regulations to protect the information you to provide to us.

Your online banking is blocked
We are recently reviewed your account, and suspect that your Natwest Bank online Banking account may have been accessed by an unauthorized third party.
Protecting the security of your account is our primary concern. Therefore, as a preventative measure, we have temporarily limited access to sensitive account features.
To restore your account access, we need you to confirm your identity, to do so we need you to follow the link below and proceed to confirm your information
https://www.natwest.co.uk
Thanks for your patience as we work together to protect your account.
Sincerely,
Natwest Bank Online Bank Customer Service
*Important*
Please update your records on or before 48 hours, a failure to update your records will result in a temporal hold on your funds.

Dear Sir/Madam,
Barclays Bank PLC always looks forward for the high security of our clients. Some customers have been receiving an email claiming to be from Barclays advising them to follow a link to what appear to be a Barclays web site, where they are prompted to enter their personal Online Banking details. Barclays is in no way involved with this email and the web site does not belong to us.
Barclays is proud to announce about their new updated secure system. we updated our new SSL servers to give our customer better fast and secure online banking service. Due to the recent update of the server, you are requested to please update your account into the following link.
https://update.barclays.co.uk/en/ln/LoginMember.do
*Important*
We have asked for additional information which is going to be the part of secure login process. These additional information will be asked during your future login security so, please provide all these info completely and correctly otherwise due to security reasons we may have to close your account temporarily.
Tracy received an **SMS** text message, ostensibly from the security department at XIM Bank. It claimed to be urgent and that Tracy should call the included phone number immediately. Worried, she called to check on her account.

She called thinking it was a XIM Bank customer service number, and it was a recording asking to provide her credit card or debit card number.

Unsurprisingly, Jonny revealed the sensitive information due to the fraudulent texts.
Social Engineering by a "Fake SMS Spying Tool"

- The users are enticed to download an application that will permit them to view other people's SMS messages online.
- The download file uses alternating filenames, including sms.exe, freetrial.exe, and smstrap.exe.

[Image: Screenshot of a spammed email]

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Insider Attack

Spying

- If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization.

Revenge

- It takes only one disgruntled person to take revenge and your company is compromised.

- 60% of attacks occur behind the firewall
- An inside attack is easy to launch
- Prevention is difficult
- The inside attacker can easily succeed
Most cases of insider abuse can be traced to individuals who are introverted, incapable of dealing with stress or conflict, and frustrated with their job, office politics, and lack of respect or promotion etc.

Disgruntled employees may pass company secrets and intellectual property to competitors for monetary benefits.
Preventing Insider Threats

Separation and rotation of duties
Archive critical data

Least privilege

Legal policies

Controlled access

Logging and auditing

There is no single solution to prevent an insider threat
### Common Intrusion Tactics and Strategies for Prevention

<table>
<thead>
<tr>
<th>Area of Risk</th>
<th>Attacker’s Tactics</th>
<th>Combat Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone (help desk)</td>
<td>Impersonation and persuasion</td>
<td>Train employees/help desk to never reveal passwords or other information by phone</td>
</tr>
<tr>
<td>Building entrance</td>
<td>Unauthorized physical access</td>
<td>Tight badge security, employee training, and security officers</td>
</tr>
<tr>
<td>Office</td>
<td>Shoulder surfing</td>
<td>Do not type in passwords with anyone else present (or if you must, do it quickly!)</td>
</tr>
<tr>
<td>Phone (help desk)</td>
<td>Impersonation on help desk calls</td>
<td>Assign a PIN to all employees to help desk support</td>
</tr>
<tr>
<td>Office</td>
<td>Wandering through halls looking for open offices</td>
<td>Escort all guests</td>
</tr>
<tr>
<td>Mail room</td>
<td>Insertion of forged memos</td>
<td>Lock and monitor mail room</td>
</tr>
<tr>
<td>Machine room/Phone closet</td>
<td>Attempting to gain access, remove equipment, and/or attach a protocol analyzer to grab the confidential data</td>
<td>Keep phone closets, server rooms, etc. locked at all times and keep updated inventory on equipment</td>
</tr>
<tr>
<td>Phone and PBX</td>
<td>Stealing phone toll access</td>
<td>Control overseas and long-distance calls, trace calls, and refuse transfers</td>
</tr>
</tbody>
</table>
Module Flow

- Social Engineering Concepts
- Impersonation on Social Networking Sites
- Social Engineering Techniques
- Social Engineering Countermeasures
- Identity Theft
- Penetration Testing
Social Engineering Through Impersonation on Social Networking Sites

Impersonation means **imitating** or copying the behavior or actions of others.

Malicious users **gather confidential information** from social networking sites and create accounts in others’ names.

Attackers can also use collected information to carry out other forms of **social engineering attacks**.

Attackers use others’ profiles to create large networks of friends and **extract information** using social engineering techniques.
Social Engineering Example: LinkedIn Profile

Chris Stone
UX Designer at Nitobi
Vancouver, Canada Area
What are you working on?

Current
- UX Designer at Nitobi

Past
- Principal/Designer at SeaStone Designs (Solo Proprietorship)
- Information Architect, UI Designer at Clarius Systems
- Manager, Product Marketing at Clarius Systems

Education
- University of California, Davis

Recommended
- 4 people have recommended you
  1 manager, 3 co-workers

Connections
- 64 connections

Industry
- Computer Software

Websites
- My Website

Public Profile
- http://www.linkedin.com/in/chrisstone

Profile Completeness
100%

Profile Settings
Social Engineering on Facebook

- Attackers create a **fake user group** on Facebook identified as "Employees of" the company.
- Using a **false identity**, attacker then proceeds to "friend," or invite, employees to the fake group, "Employees of the company.
- Users join the group and **provide their credentials** such as date of birth, educational and employment backgrounds, spouses names, etc.
- Using the details of any one of the employee, an attacker can **compromise** a secured facility to **gain access** to the building.

![Facebook profile screen capture]

---

**Basic Information**

- **Sex**: Male
- **Interested In**: Men
- **Relationship Status**: Single

**Contact Information**

- **Phone**: +64 50800000 (Mobile), +64 5080111 (Other)
- **Address**: XXXXXXXX, Auckland, CA 700017
- **Screen Name**: John (Skype)
- **Website**: [http://www.juguyboy.com/](http://www.juguyboy.com/)

**John James**

- **College**: The University of Auckland, Class of 2002
- **High School**: Mt Roskill Grammar, Class of 1999
Social Engineering on Twitter

Twitter settings for John Attacker

- Use Twitter with Text Messaging
  Twitter is more fun when used through your mobile phone. Set yours up! It's easy!
  Twitter does not charge for this service. Standard message and data rates may apply.

1. Choose your country/region
   United States

2. Enter your mobile phone number
   +1 [redacted]
   Let others find me by my phone number

3. Verify your phone
   Start

- Text Messaging on Twitter
  Setting up your phone allows you to:
  - Send tweets with text messaging on your phone.
  - Receive texts for DMs and the tweets from users you want to be notified about.
  - Clicking the phone icon on a user's profile page or your followers page sets Tweet notifications for that user.

- Twitter commands
  Do more than Tweet! Send these commands to Twitter:
  - FOLLOW username
  - Start following a user
  - UNFOLLOW username
  - Stop following a user
Social Engineering on Orkut
Social Engineering on MySpace
Risks of Social Networking to Corporate Networks

A social networking site is an enormous database accessed by many individuals, increasing the risk of information exploitation.

In the absence of a strong policy, employees may unknowingly post sensitive data about their company on social networking.

Information on social networking sites could be used for preliminary reconnaissance in a targeted attack.

All social networking sites are subject to flaws and bugs that may lead to vulnerabilities in the company’s network.
Module Flow

- Social Engineering Concepts
- Social Engineering Techniques
- Impersonation on Social Networking Sites
- Identity Theft
- Social Engineering Countermeasures
- Penetration Testing
Identity Theft
“One bit of personal information is all someone needs to steal your identity.”
How to Steal an Identity?

Original identity – Steven Charles
Address: San Diego CA 92130
STEP 1

Get hold of Steven’s telephone bill, water bill, or electricity bill using dumpster diving, stolen email, or onsite stealing.
STEP 2

- Go to the Department of Motor Vehicles and tell them you lost your driver’s license
- They will ask you for proof of identity such as a water bill and electricity bill
- Show them the stolen bills
- Tell them you have moved from the original address
- The department employee will ask you to complete two forms—one for the replacement of the driver’s license and the second for a change in address
- You will need a photo for the driver’s license
- Your replacement driver’s license will be issued to your new home address
- Now you are ready to have some serious fun
Comparison

Original

Same name: Steven Charles

Identity Theft
**STEP 3**

Go to a bank in which the original Steven Charles has an account and tell them you would like to apply for a **new credit card**

Tell them you **do not remember** the account number and ask them to look it up using Steven’s name and address

The bank will ask for your ID: Show them your **driver’s license as ID**, and if the ID is accepted, your credit card will be issued and ready for use

**Now you are ready for shopping**

**Fake Steven is Ready to:**

- Make purchases worth thousands of USD
- Apply for a car loan
- Apply for a new passport
- Apply for a new bank account
- Shut down your utility services
Real Steven Gets Huge Credit Card Statement

<table>
<thead>
<tr>
<th>ACCOUNT NUMBER</th>
<th>NAME</th>
<th>STATEMENT DATE</th>
<th>PAYMENT DUE DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>4125-239-412</td>
<td>Stevens Charles</td>
<td>2/13/01</td>
<td>3/09/01</td>
</tr>
</tbody>
</table>

**NEW BALANCE**

<table>
<thead>
<tr>
<th>CREDIT LINE</th>
<th>CREDIT AVAILABLE</th>
<th>MINIMUM PAYMENT DUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1200.00</td>
<td>$1074.76</td>
<td>$20.00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REFERENCE</th>
<th>SOLED</th>
<th>POSTED</th>
<th>ACTIVITY / STATEMENT</th>
<th>AMOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>463094392</td>
<td>1/26</td>
<td>1/26</td>
<td>FOR LUNA'S DINNER</td>
<td>$168.80</td>
</tr>
<tr>
<td>32P3468ER3</td>
<td>1/16</td>
<td>1/16</td>
<td>Recorder Rent</td>
<td>$125.24</td>
</tr>
<tr>
<td>8490000880</td>
<td>1/13</td>
<td>1/13</td>
<td>Bomberman Rest</td>
<td>$120.92</td>
</tr>
<tr>
<td>849012321</td>
<td>1/18</td>
<td>1/18</td>
<td>Great Expectations BIG CITY USA</td>
<td>$1230.65</td>
</tr>
<tr>
<td>873253321</td>
<td>2/09</td>
<td>2/09</td>
<td>Dino-Go Petroleum</td>
<td>$923.90</td>
</tr>
<tr>
<td>873253321</td>
<td>2/09</td>
<td>2/09</td>
<td>Shirt 'n Such</td>
<td>$540.10</td>
</tr>
</tbody>
</table>

Previous Balance: $168.80
Current Amount Due: $40,000
Amount Over Credit Line: $40,000
Minimum Payment Due: $20.00

Somebody stole my identity!
Identity Theft - Serious Problem

- Identity theft is a serious problem
- The number of violations has increased
- Securing personal information in the workplace and at home and looking over credit card reports are just a few of the ways to minimize the risk of identity theft

Welcome to the FTC's Identity Theft Site

This website is a one-stop national resource to learn about the crime of identity theft. It provides detailed information to help you deter, detect, and defend against identity theft.

On this site, consumers can learn how to avoid identity theft — and learn what to do if their identity is stolen. Businesses can learn how to help their customers deal with identity theft, as well as how to prevent problems in the first place. Law enforcement can get resources and learn how to help victims of identity theft.

Read on to find out more about identity theft and what you can do about it.

If your information has been stolen and used by an identity thief

If your information may have been stolen, but may or may not have been used by an identity thief

Learn more about identity theft

http://www.consumer.gov

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Module Flow

- Social Engineering Concepts
- Social Engineering Techniques
- Impersonation on Social Networking Sites
- Identity Theft
- Social Engineering Countermeasures
- Penetration Testing

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Social Engineering Countermeasures: Policies

- Good policies and procedures are ineffective if they are not taught and reinforced by the employees.
- After receiving training, employees should sign a statement acknowledging that they understand the policies.

Password Policies:
- Periodic password change
- Avoiding guessable passwords
- Account blocking after failed attempts
- Length and complexity of passwords
- Secrecy of passwords

Physical Security Policies:
- Identification of employees by issuing of ID cards, uniforms, etc.
- Escorting the visitors
- Accessing area restrictions
- Proper shredding of useless documents
- Employing security personnel
Social Engineering Countermeasures

Training
An efficient training program should consist of all security policies and methods to increase awareness on social engineering.

Operational Guidelines
Ensure security of the sensitive information and authorized use of resources.
Social Engineering Countermeasures

Classification of Information
- Categorize the information as top secret, proprietary, for internal use only, for public use, etc.
- Insiders with a criminal background and terminated employees are easy targets for procuring information

Access Privileges
- There should be administrator, user, and guest accounts with proper authorization

Background Check of Employees and Proper Termination Process
- There should be proper guidelines for reacting in case of a social engineering attempt

Proper Incidence Response Time
Social Engineering Countermeasures

Two-Factor Authentication

- Instead of fixed passwords, use two-factor authentication for high-risk network services such as VPNs and modern pools.

Anti-Virus/Anti-Phishing Defenses

- Use multiple layers of anti-virus defenses such as at end-user desktops and at mail gateways to minimize social engineering attacks.

Change Management

- A documented change-management process is more secure than the ad-hoc process.
How to Detect Phishing Emails?

- It includes links that lead to spoofed websites asking to enter personal information when clicked.
- The phishing email seems to be from a bank, financial institution, company, or social networking site.
- Seems to be from a person who is listed in your email address book.
- Directs to call a phone number in order to give up account number, personal identification number, password, or confidential information.
- Includes official-looking logos and other information taken directly from legitimate websites convincing you to disclose your personal details.

![Phishing Email Example]

Dear HSBC Online User,

As part of our security measures, the HSBC Bank, has developed a security program against the fraudulent attempts and account thefts. Therefore, our system requires further account information. We request information from you for the following reason. We need to verify your account information in order to insure the safety and integrity of our services.

Please follow the link below to proceed.


Once you login, you will be provided with steps to complete the verification process. For your safety, we have physical, electronic, procedural safeguards that comply with federal regulations to protect the information you to provide us.

Thanks and Regards,

![Link to Spoofed Website]

Link that seems to be legitimate but leads to spoofed website.
Anti-Phishing Toolbar: Netcraft

http://www.netcraft.com
Anti-Phishing Toolbar: PhishTank

Join the fight against phishing

Submit suspected phishes, Track the status of your submissions, Verify other users' submissions, Develop software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:
http://

Recent Submissions
You can help! Sign in or register (free! fast!) to verify these suspected phishes.

<table>
<thead>
<tr>
<th>ID</th>
<th>URL</th>
<th>Submitted by</th>
</tr>
</thead>
<tbody>
<tr>
<td>983960</td>
<td><a href="http://www.msnfotovriend.nl/">http://www.msnfotovriend.nl/</a></td>
<td>Harm222</td>
</tr>
<tr>
<td>983959</td>
<td><a href="http://natureorganisme.linemeweb.com/paypal%20full%20c">http://natureorganisme.linemeweb.com/paypal%20full%20c</a>...</td>
<td>PhishReporter</td>
</tr>
<tr>
<td>983958</td>
<td><a href="http://server1.p7hosting.de/sitekey_bankofamer">http://server1.p7hosting.de/sitekey_bankofamer</a>...</td>
<td>mepkerl</td>
</tr>
<tr>
<td>983957</td>
<td><a href="http://grebfamily.us/latest/consum/management/fin">http://grebfamily.us/latest/consum/management/fin</a>...</td>
<td>PhishReporter</td>
</tr>
<tr>
<td>983956</td>
<td><a href="http://alwan.net23.net/cgi-bin/webscr/">http://alwan.net23.net/cgi-bin/webscr/</a></td>
<td>PhishReporter</td>
</tr>
<tr>
<td>983955</td>
<td><a href="http://user26974.vs.easily.co.uk/connexion/">http://user26974.vs.easily.co.uk/connexion/</a>...</td>
<td>PhishReporter</td>
</tr>
<tr>
<td>983954</td>
<td><a href="http://user25945.vs.easily.co.uk/img/www.PayPal.co">http://user25945.vs.easily.co.uk/img/www.PayPal.co</a>...</td>
<td>PhishReporter</td>
</tr>
<tr>
<td>983953</td>
<td><a href="http://www.bonsaitreesite.com/articles/PayPal.fr/">http://www.bonsaitreesite.com/articles/PayPal.fr/</a>...</td>
<td>PhishReporter</td>
</tr>
<tr>
<td>983951</td>
<td><a href="http://www.metzgerie-pauleser.de/administrator/mod">http://www.metzgerie-pauleser.de/administrator/mod</a>...</td>
<td>PhishReporter</td>
</tr>
</tbody>
</table>
Identity Theft Countermeasures

- Secure or shred all documents containing private information
- To keep your mail secure, empty the mailbox quickly
- Ensure your name is not present in the marketers’ hit lists
- Suspect and verify all the requests for personal data
- Review your credit card reports regularly
- Never let your credit card out of your sight
- Protect your personal information from being publicized
- Never give any personal information on the phone
- Do not display account/contact numbers unless mandatory
Module Flow

Social Engineering Concepts

Social Engineering Techniques

Impersonation on Social Networking Sites

Identity Theft

Social Engineering Countermeasures

Penetration Testing
The objective of social engineering pen testing is to test the strength of human factors in a security chain within the organization. Social engineering pen testing is often used to raise the level of security awareness among employees. Tester should demonstrate extreme care and professionalism for social engineering pen test as it might involve legal issues such as violation of privacy and may result in an embarrassing situation for the organization.
Obtain management’s explicit **authorization** and details that will help in defining scope of pen-test such as list of departments, employees that need to be tested, or level of physical intrusion allowed.

Collect **email addresses and contact details** of target organization and its human resources (if not provided) using techniques such as dumpster diving, email guessing, USENET and web search, email spider tools like Email Extractor.

Try to **extract as much information as possible** about the identified targets using footprinting techniques.

Create a script based on the collected information considering both positive and negative results of an attempt.
Email employees asking for personal information such as their user names and passwords by disguising as network administrator, senior manager, tech support, or anyone from a different department on pretext of an emergency.

Send emails to targets with malicious attachments and monitor their treatment with attachments using tools such as ReadNotify.

Send phishing emails to targets as if from a bank asking about their sensitive information (you should have requisite permission for this).
Social Engineering Pen Testing: Using Phone

- Call a target posing as a colleague and ask for the sensitive information
- Call a target user posing as an important user
- Call a target posing as technical support and ask for the sensitive information
- Refer to an important person in the organization and try to collect data
- Call a target and offer them rewards in lieu of personal information
- Threaten the target with dire consequences (for example, account will be disabled) to get information
- Use reverse social engineering techniques so that the targets yield information themselves
Social Engineering Pen Testing: In Person

- Befriend employees in cafeteria and try to extract information
- Try to tailgate wearing a fake ID badge or piggyback
  - Success of any social engineering technique depends on how well a tester can enact the testing script and his interpersonal skills

- Try to enter facility posing as an external auditor
- Try eavesdropping and shoulder surfing on systems and users
  - There could be countless other social engineering techniques based on available information and scope of test. Always scrutinize your testing steps for legal issues

- Try to enter facility posing as a technician
- Document all the findings in a formal report
Module Summary

- Social engineering is the art of convincing people to reveal confidential information.
- Social engineering involves acquiring sensitive information or inappropriate access privileges by an outsider.
- Human-based social engineering refers to person-to-person interaction to retrieve the desired information.
- Computer-based social engineering refers to having computer software that attempts to retrieve the desired information.
- A successful defense depends on having good policies and their diligent implementation.
If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology.

- Bruce Schneier,
  Security Technologist and Author