

Social Engineering

Module 08

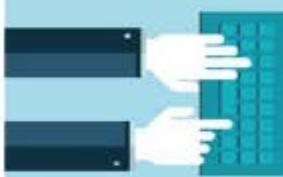
Unmask the Invisible Hacker.



Social Engineering Statistics

CEH
Certified Ethical Hacker

Phishing



88%

Clicking links within email of all reported phishing

Most common phishing attacks mimicking financial institutions



How much email is sent?

107 Trillion annually

294 Billion each day



77% Percentage of phishing of all socially based attacks

Vishing



2.4 M customers targeted for phone fraud for all of 2012

2.3 M customers targeted for phone fraud for first half of 2013

Average loss for targeted business \$42,546 per account

60% of US adults who send and receive text messages received mobile spam in 2012

What do Smishers ask for?

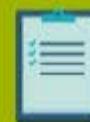


Impersonation



1.8 Million victims of medical theft in 2013 due to websites impersonating medical providers

88% of reported stolen assets were personal data



Average Victims of impersonation

41.7 year old

\$4,187 lost



Top place for thief is work area

According to the survey conducted by Social-Engineer.Org <http://www.social-engineer.org>

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

Module Objectives

CEH
Certified Ethical Hacker

- Overview of Social Engineering Concepts
- Understanding various Social Engineering Techniques
- Understanding Insider Threats
- Understanding Impersonation on Social Networking Sites



- Understanding Identity Theft
- Social Engineering Countermeasures
- Identity Theft Countermeasures
- Overview of Social Engineering Pen Testing



Module Flow



1

Social Engineering Concepts

2

Social Engineering Techniques

3

Impersonation on Social Networking Sites

4

Identity Theft

5

Social Engineering Countermeasures

6

Penetration Testing

What is Social Engineering?

CEH
Certified Ethical Hacker



Social engineering is the art of **convincing people** to reveal confidential information. Common targets of social engineering include help desk personnel, technical support executives, system administrators, etc.



Social engineers depend on the fact that people are **unaware of their valuable information** and are careless about protecting it

Impact of Attack on Organization



Economic Losses



Lawsuits and Arbitrations



Temporary or Permanent Closure



Loss of Privacy



Damage of Goodwill



Dangers of Terrorism

Behaviors Vulnerable to Attacks

CEH
Certified Ethical Hacker

I

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



II

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



III

Fear of severe losses in case of non-compliance to the social engineer's request



IV

Social engineers lure the targets to divulge information by **promising something for nothing (greediness)**



V

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



Factors that Make Companies Vulnerable to Attacks

CEH
Certified Ethical Hacker

01



Insufficient Security Training

02



Unregulated Access to the Information

03



Several Organizational Units

04



Lack of Security Policies

Why is Social Engineering Effective?



01

Security policies are as strong as their weakest link, and **humans** are the most **susceptible factor**



02

It is **difficult to detect social engineering attempts**



03

There is **no method to ensure complete security** from social engineering attacks



04

There is **no specific software or hardware** for defending against a social engineering attack



Phases in a Social Engineering Attack

CEH
Certified Ethical Hacker



Research on Target Company

Dumpster diving, websites, employees, tour company, etc.



Select Victim

Identify the frustrated employees of the target company



Develop Relationship

Develop relationship with the selected employees



Exploit the Relationship

Collect sensitive account and financial information, and current technologies

Module Flow



1

Social Engineering Concepts

2

Social Engineering Techniques

3

Impersonation on Social Networking Sites

4

Identity Theft

5

Social Engineering Countermeasures

6

Penetration Testing

Types of Social Engineering



Human-based Social Engineering

Gathers sensitive information by **interaction**



Computer-based Social Engineering

Social engineering is carried out with the help of **computers**



Mobile-based Social Engineering

It is carried out with the help of **mobile applications**



Human-based Social Engineering: Impersonation



It is most common human-based social engineering technique where attacker **pretends to be someone legitimate or authorized person**

1

Attackers may **impersonate** a legitimate or authorized person either personally or using a **communication medium** such as phone, email, etc.

2

Impersonation helps attackers in **tricking a target** to reveal **sensitive information**

3

Human-based Social Engineering: Impersonation (Cont'd)



Posing as a legitimate end user

- Give identity and ask for the sensitive information

"Hi! This is John, from finance department. I have forgotten my password. Can I get it?"



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?"



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 u give me your ID and password?"

Impersonation Scenario: Over-Helpfulness of Help Desk



- Help desks are mostly vulnerable to social engineering as they are in place **explicitly to help**
- Attacker calls a company's help desk, pretends to be someone in a **position of authority** or relevance and tries to **extract sensitive information** out of the help desk



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

Impersonation Scenario: Third-party Authorization



Attacker obtains the name of the authorized employee of target organization who has access to the information he/she wants



Attacker then call to the target organization where information is stored and claims that particular employee has requested that information be provided



Impersonation Scenario: Tech Support



- Attacker **pretends to be technical support staff** of target organization's software vendors or contractors
- He/she may then **claims user ID and password** for troubleshooting problem in the organization



Attacker: "Hi, this is Mike with tech support. We have had some folks in your office report slowdowns in logging in lately. Is this true?"

Employee: "Yes, it has seemed slow lately."

Attacker: "Well, we have moved you to a new server, so your service should be much better. If you want to give me your password, I can check your service. Things should be better for you now."

Impersonation Scenario: Repairman



- Attacker may pretend to be **telephone repairman** or **computer technician** and enters into target organization
- He/she may then **plant a snooping device** or gain hidden passwords during activities associated with their duties



Impersonation Scenarios: Trusted Authority Figure



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 and Shoulder Surfing



Eavesdropping



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

Shoulder Surfing



- Shoulder surfing uses direct observation techniques such as **looking over someone's shoulder** to get information such as passwords, PINs, account numbers, etc.
- Shoulder surfing can also be done from a longer distance with the aid of **vision enhancing devices** such as binoculars to obtain sensitive information

Human-based Social Engineering: Dumpster Diving

CEH
Certified Ethical Hacker

Dumpster Diving

Dumpster diving is **looking for treasure** in someone else's **trash**



Human-based Social Engineering: Reverse Social Engineering, Piggybacking, and Tailgating



Reverse Social Engineering

- A situation in which an attacker presents himself as an **authority** and the target seeks his advice offering the information that he needs
- Reverse social engineering attack involves **sabotage**, **marketing**, and **tech support**

Piggybacking

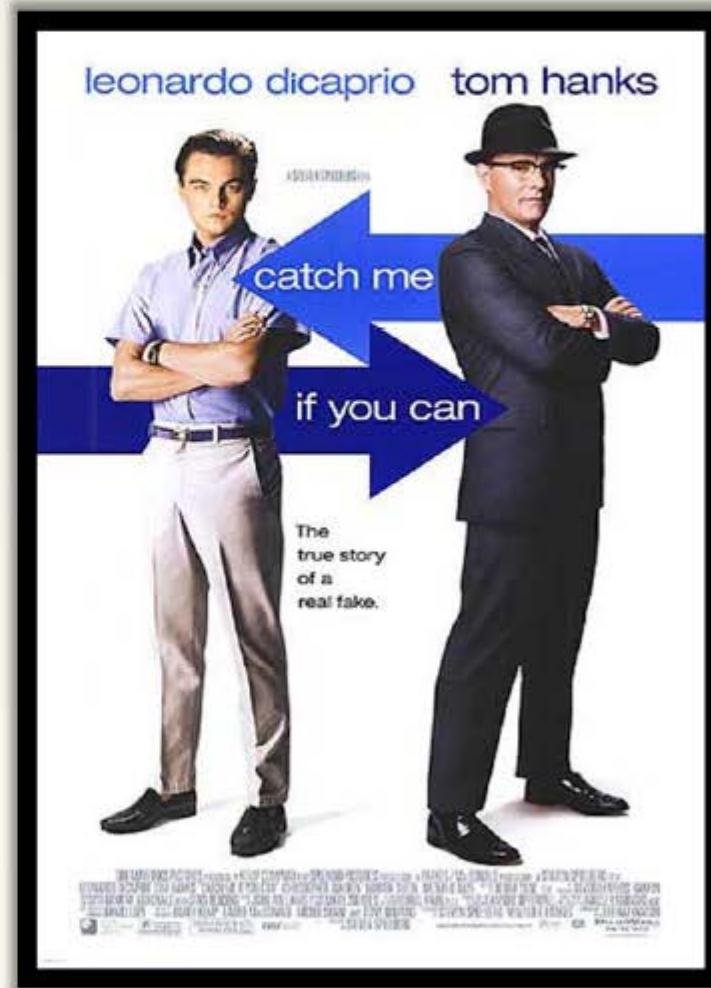
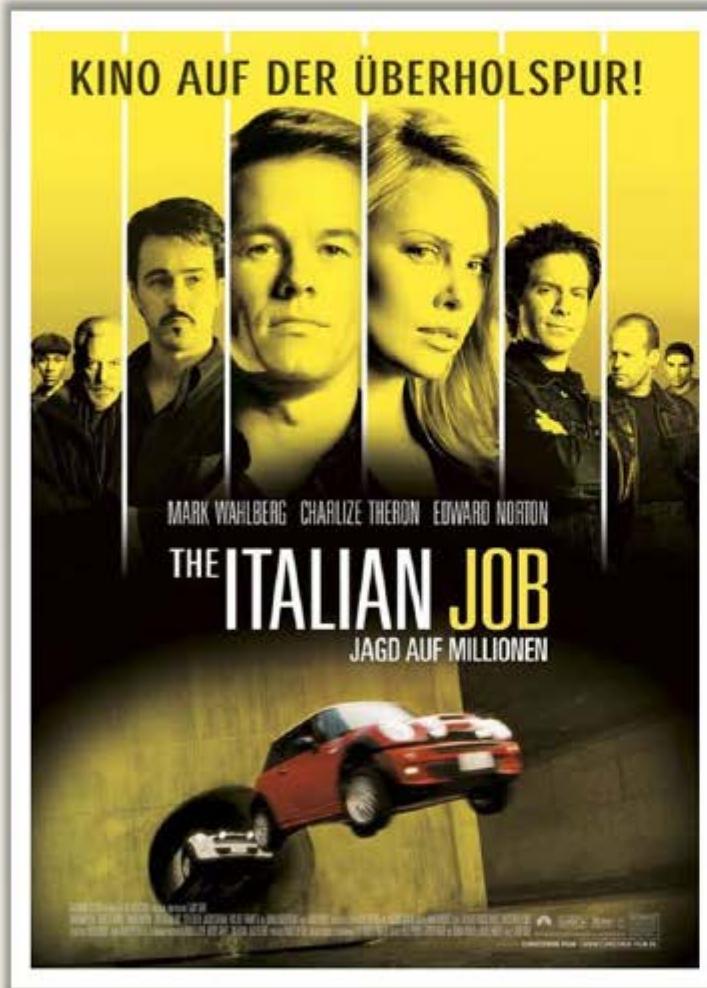
- "I forgot my ID badge at home. Please help me."
- An authorized person allows (intentionally or unintentionally) an **unauthorized person** to pass through a secure door

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

Watch these **Movies**

CEH
Certified Ethical Hacker



Watch this Movie

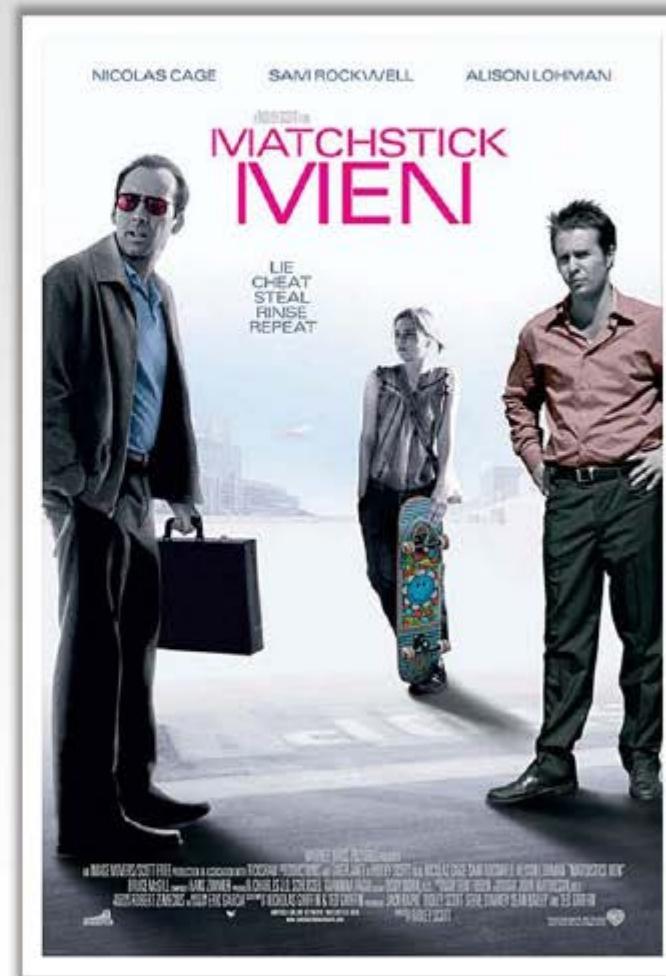
CEH
Certified Ethical Hacker

Social Engineering

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

Manipulating People

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**



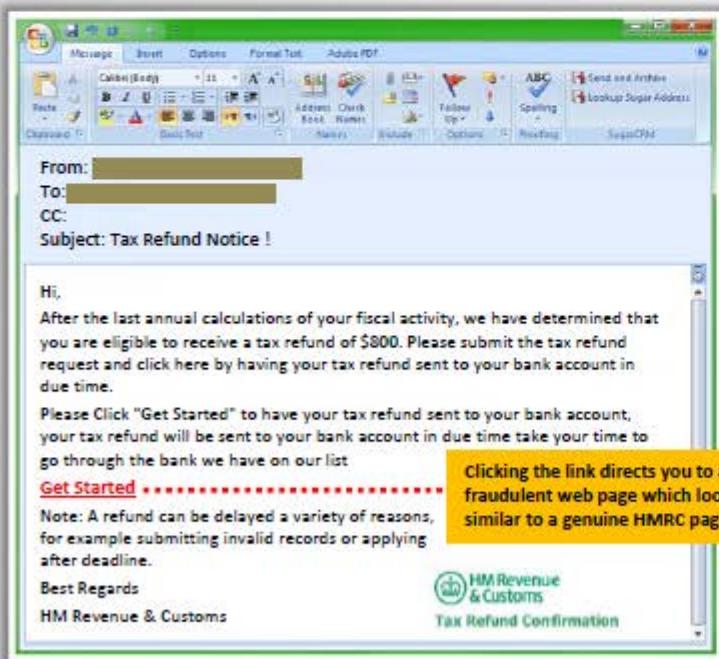
Computer-based Social Engineering: Phishing



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



HM Revenue & Customs

Address Information - Please enter your name and address as you have it listed for your credit card.

Cardholder Name: _____
Date of Birth: Day Month Year
Mother Maiden Name: _____
Address: _____
Town/City: _____
Postal Code: _____
Phone Number: _____

Credit Card Information - Please enter your Credit or Debit Card where refunds will be made.

Bank Name: _____
Debit / Credit Card Number: _____
Expiration Date: Month Year
Card Verification Number: _____
Sort Code: _____ (If Shown On Card)
Submit Information

<http://www.hmrc.gov.uk>

Computer-based Social Engineering: Spear Phishing



Spear phishing is a direct, targeted phishing attack aimed at **specific individuals within an organization**

In contrast to normal phishing attack where attackers send out hundreds of generic messages to random email addresses, attackers use spear phishing to send a message with specialized, **social engineering content** directed at a **specific person or a small group of people**



Spear phishing **generates higher response rate** when compared to normal phishing attack



Mobile-based Social Engineering: Publishing Malicious Apps

CEH
Certified Ethical Hacker



Attackers create **malicious apps** with attractive features and **similar names** to that of popular apps, and publish them on major **app stores**



Unaware **users download these apps** and get infected by malware that sends **credentials to attackers**



Mobile-based Social Engineering: Repackaging Legitimate Apps

CEH
Certified Ethical Hacker



Mobile-based Social Engineering: Fake Security Applications



- 01 Attacker infects the **victim's PC**
- 02 The victim logs onto his/her **bank account**
- 03 Malware in PC **pop-ups a message** telling the victim to **download an application** onto his/her phone in order to receive security messages
- 04 Victim **downloads the malicious application** on his/her phone
- 05 Attacker can now access **second authentication factor** sent to the victim from the bank via SMS



Mobile-based Social Engineering: Using SMS

CEH
Certified Ethical Hacker

1 Tracy received an **SMS** text message, ostensibly from the security department at XIM Bank

2 It claimed to be **urgent** and that Tracy should call the phone number in the SMS immediately. Worried, she called to check on her account.

3 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

4 Predictably, Tracy **revealed the sensitive information** due to the fraudulent texts



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

Insider Attack

- An inside attack is easy to launch
- Prevention is difficult
- The inside attacker can easily succeed



Disgruntled Employee

CEH
Certified Ethical Hacker

1

An employee may become **disgruntled towards the company** when he/she is disrespected, frustrated with their job, having conflicts with the management, not satisfied with employment benefits, issued an employment termination notice, transferred, demoted, etc.

2

Disgruntled employees may **pass company secrets** and **intellectual property** to competitors for monetary benefits



Preventing Insider Threats

CEH
Certified Ethical Hacker

01

Separation and rotation of duties

Logging and auditing

04



02

Least privilege

Legal policies

05

03

Controlled access

Archive critical data

06



There is no single solution to **prevent** an insider threat

Common Social Engineering Targets and Defense Strategies



Social Engineering Targets	Attack Techniques	Defense Strategies
Front office and help desk	Eavesdropping, shoulder surfing, impersonation, persuasion, and intimidation	Train employees/help desk to never reveal passwords or other information by phone
Perimeter security	Impersonation, fake IDs, piggy backing, etc.	Implement strict badge, token or biometric authentication, employee training, and security guards
Office	Shoulder surfing, eavesdropping, Ingratiation, etc.	Employee training, best practices and checklists for using passwords Escort all guests
Phone (help desk)	Impersonation, Intimidation, and persuasion on help desk calls	Employee training, enforce policies for the help desk
Mail room	Theft, damage or forging of mails	Lock and monitor mail room, employee training
Machine room/ Phone closet	Attempting to gain access, remove equipment, and/or attach a protocol analyzer to grab the confidential data	Keep phone closets, server rooms, etc. locked at all times and keep updated inventory on equipment

Module Flow



1

Social Engineering Concepts

2

Social Engineering Techniques

3

Impersonation on Social Networking Sites

4

Identity Theft

5

Social Engineering Countermeasures

6

Penetration Testing

Social Engineering Through Impersonation on Social Networking Sites



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

Attackers use others' profiles to create large networks of friends and **extract information** using social engineering techniques

Attackers try to join the target **organization's employee groups** where they share personal and company information

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

Social Engineering on Facebook



The screenshot shows John Legend's Facebook profile. The 'About' section includes his official page link (<http://www.facebook.com/johnlegend>), biography, and artists he likes. The 'Basic Info' section provides details like founded year (2000), genre (R&B/Soul), and influences (Stevie Wonder, Ne-Yo, Al Green, Jeff Buckley). The 'Contact Info' section lists websites, booking agent (Creative Artists Agency), and life events (2011 Grammy Awards, 2010 Ebony Magazine's 65th Anniversary Tribute Cover).

Attackers create a **fake user group** on Facebook identified as "Employees of" the target 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

<http://www.facebook.com>

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

Social Engineering on LinkedIn and Twitter



The image displays two screenshots side-by-side. On the left is a LinkedIn profile for Christopher Stone, a Columnist and Author. His profile picture shows him wearing sunglasses and a dark shirt. Below the picture, his name and title are listed, along with his current position at United Kingdom Writing and Editing. He has 222 connections. On the right is a Twitter feed for Novak Djokovic (@DjokerNole). The feed shows several tweets, including one from him about his new book. The Twitter interface includes sections for Tweets, Following, Followers, Favorites, and Lists. A sidebar on the left of the Twitter screen shows a blurred profile picture of another user. At the bottom of the image, the URLs <http://www.linkedin.com> and <http://twitter.com> are displayed.

Attackers scan details in **profile pages**. They use these details for spear phishing, impersonation, and identity theft.

Risks of Social Networking to Corporate Networks



Data Theft



A social networking site is an **information repository** accessed by many users, enhancing the risk of information exploitation

Involuntary Data Leakage



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

Targeted Attacks



Attackers use the **information** available on **social networking sites** to perform a targeted attack

Network Vulnerability



All social networking sites are subject to **flaws** and **bugs** that in turn could cause vulnerabilities in the organization's network

Module Flow



1

Social Engineering Concepts

2

Social Engineering Techniques

3

Impersonation on Social Networking Sites

4

Identity Theft

5

Social Engineering Countermeasures

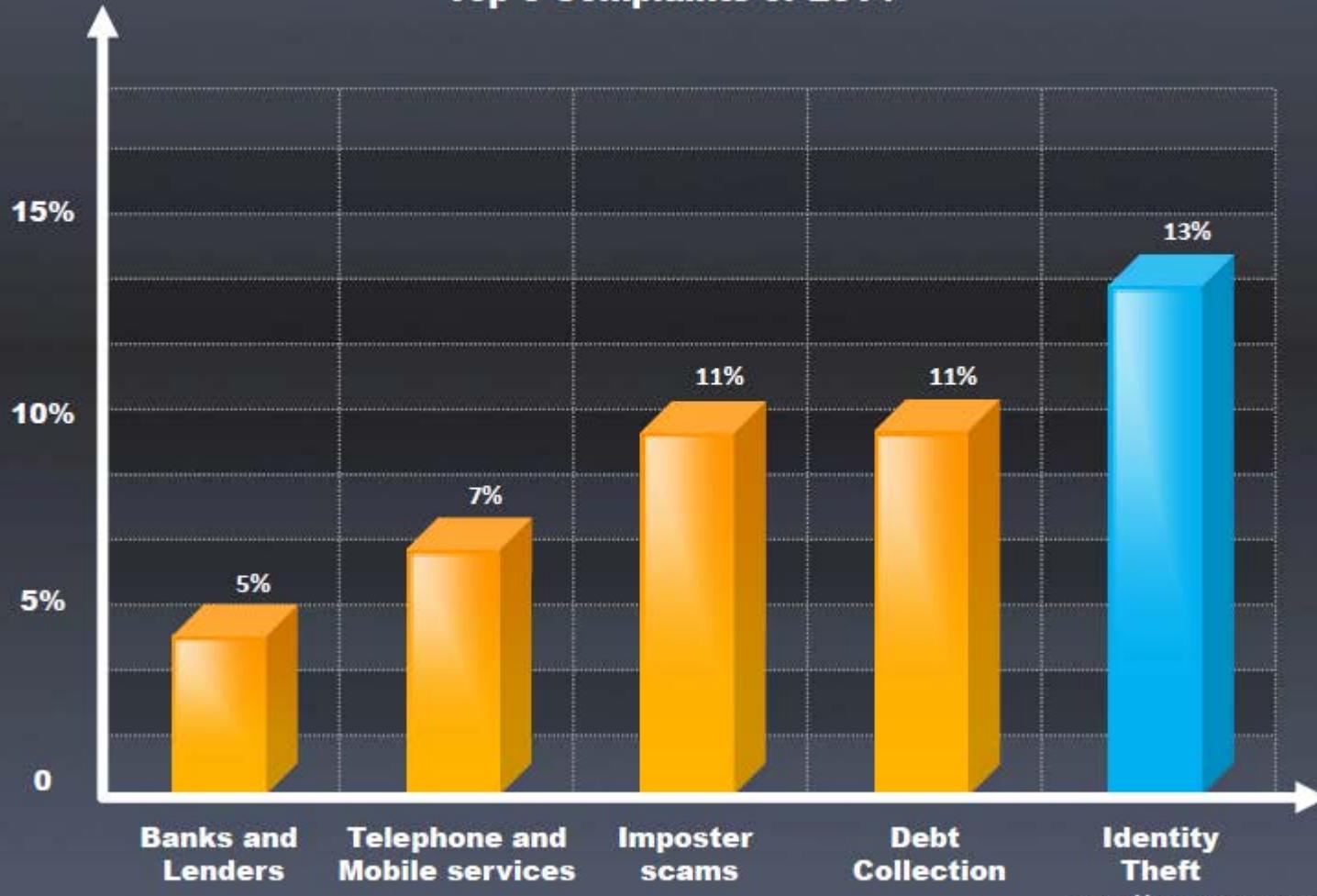
6

Penetration Testing

Identity Theft Statistics

CEH
Certified Ethical Hacker

Top 5 Complaints of 2014



<http://money.cnn.com>

Identify Theft



1.

Identity theft occurs when **someone steals your personally identifiable information** for fraudulent purposes

2.

It is a crime in which an imposter obtains personal identifying information such as **name, credit card number, social security or driver license numbers**, etc. to commit fraud or other crimes

3.

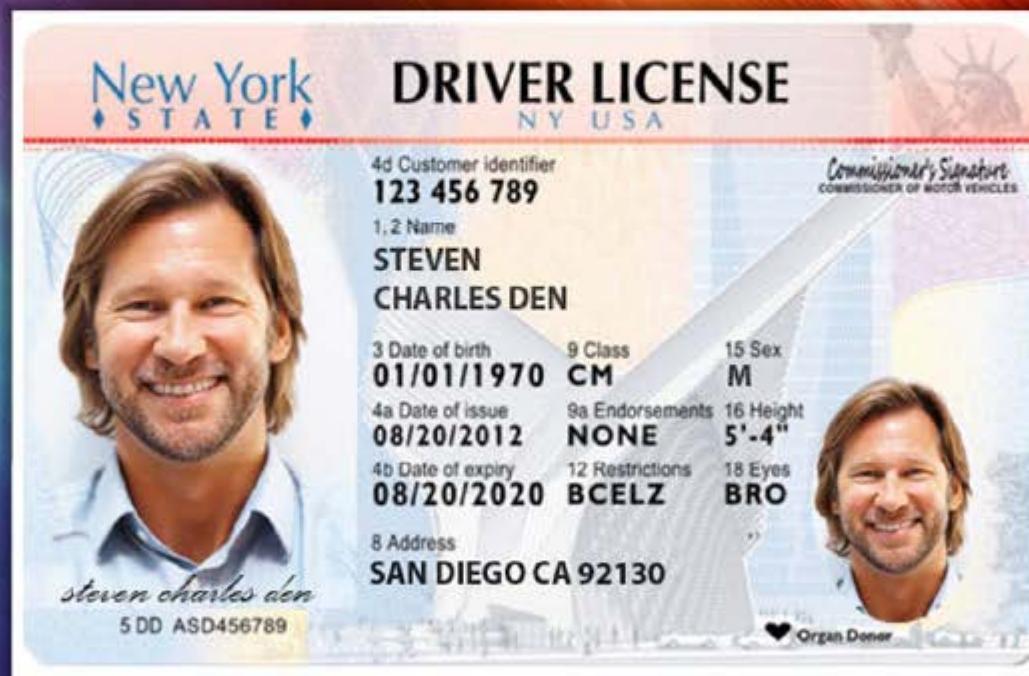
Attackers can use identity theft to **impersonate employees of a target organization** and physically access the facility

How to Steal an Identity

CEH
Certified Ethical Hacker

Original identity – Steven Charles

Address: San Diego CA 92130



Note: The identity theft illustration presented here is for demonstrating a typical identity theft scenario. It may or may not be used in all location and scenarios.

STEP 1



- Search for Steven's address on **social networking sites** (Facebook, Twitter, etc.) or on **people search sites**
- Get hold of Steven's telephone bill, water bill, or electricity bill using **dumpster diving, stolen email, or onsite stealing**



Steven Charles

Steven Charles Map

STEVEN CHARLES DEN BESTE
SAN DIEGO CA 92130

Phone: 1800-411-7343

Steven's Address

pipl

STEVEN CHARLES

California, US

Search By: Steven Charles, 36 Pages, 33 Locations, 15 Related

Sponsored Shortcuts: Contact Details, Address History, Vital Records, Social Profile

SDGE San Diego Gas & Electric

ACCOUNT NUMBER: 123456
SERIAL#:

STEVEN CHARLES DEN BESTE
SAN DIEGO CA 92130

DATE MAILED: Jun 24, 2013 Page 1 of 4

SDG&E offers programs and services that can help you save energy and money. Call 1-800-411-7343 or visit www.sdge.com.

Account Summary

Previous Balance	06/09/13	THANK YOU	\$10.04
Payment Received			- \$0.04
Current Charges			+ \$0.76
Total Amount Due			\$10.76

Summary of Current Charges (See page 2 for details)

Billing Period	Start Date	End Date	Usage	Amount
May 18, 2013 - Jun 17, 2013	May 18, 2013	Jun 17, 2013	16 Therms	\$17.92
			420 kWhs	\$0.64
			Total Charges this Month	\$18.56

Your payment of \$18.56 will be paid by "Automatic Pay" on July 9, 2013.

Gas Usage History (Total Therms used)



Total Therms used: 16 Daily average: 1.06 Change in daily average last month: 0.00% Change in daily average from last year: 0.00%

Electric Usage History (Total kWhs used)



Total kWhs used: 420 Daily average: 10.5 Change in daily average last month: 0.00% Change in daily average from last year: 0.00%

Steven's Electricity Bill

WATER & WASTEWATER SERVICES PUBLIC UTILITIES

ACCOUNT NUMBER: 1234567890
SERVICE ADDRESS: STEVEN CHARLES DEN BESTE SAN DIEGO CA 92130

Mailed on: Oct 07 2013 PAYMENT BY DATE: Oct 22 2013

RETURN THIS PORTION
MAKE CHECK PAYABLE TO CITY TREASURER

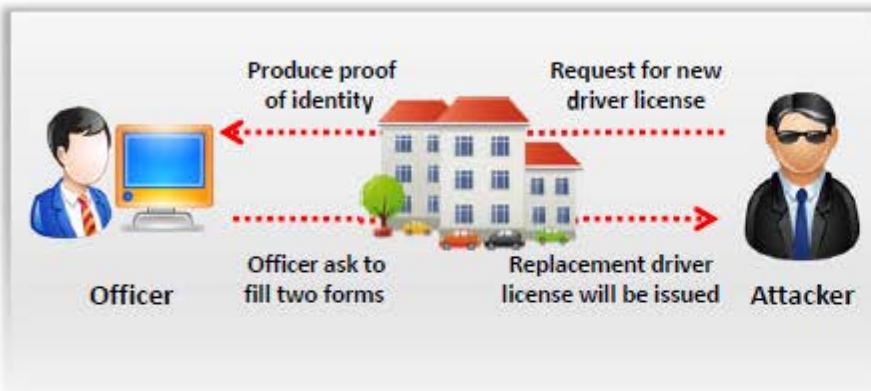
Steven's Water Bill

Oct 22 2013	\$160.57	TOTAL AMOUNT DUE
PAYMENT DUE DATE		
AMOUNT		
CODE		

DETAILS

TYPE OF SERVICE	METER	SERVICE PERIOD	DAY	METER READING	USAGE HCF*	AMOUNT	CODE	
Water Base Fee	1234567890	09-06-13 - 10-03-13	59	Meter size: 3/4 inch	210	12.00 HCF @ \$3.6117 =	\$43.34	38.85
Water Used		09-06-13 - 10-03-13	59		230			43.34
Sewer Base Fee		09-06-13 - 10-03-13	59					30.66
Sewer Service Charge		09-06-13 - 10-03-13	59					45.21
Storm Drain								1.00
Current Charges								160.57
TOTAL AMOUNT DUE								\$160.57

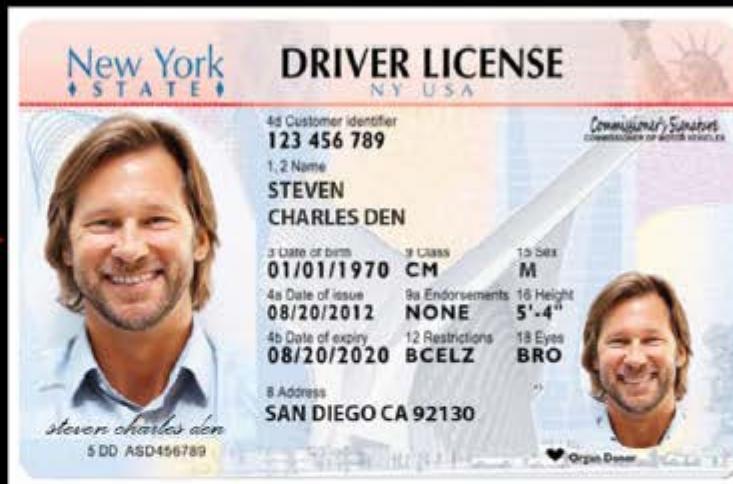
STEP 2



- 01 Go to the **Department of Motor Vehicles** and tell them you lost your driver license
- 02 They will ask you for **proof of identity** such as a water bill and electricity bill
- 03 Show them the **stolen bills**
- 04 Tell them you have **moved from the original address**
- 05 The department employee will ask to complete **replacement of the driver license form** and **change in address form**
- 06 You will need a **photo for the driver license**
- 07 Your replacement driver license will be issued to your **new home address**
- 08 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 license as ID**, and if the ID is accepted, your credit card will be issued and ready for
- Now you are ready for **shopping**



Fake Steven is Ready to:

Make purchases worth thousands of USD



Apply for a new passport



Apply for a new bank account



Shut down your utility services



Apply for a car loan



Real Steven Gets Huge Credit Card Statement

CEH
Certified Ethical Hacker



Somebody stole my identity!

Statement of Personal Credit Card Account

Check here if address or telephone number has changed. Please note changes on reverse side.

Account Number	Statement Closing Date	Current Amount Due
1234-567-890	01-31-14	\$40,000

MAIL PAYMENT TO :
EA BANK
1234 FAIRFIELD STREET
ANYTOWN, USA 12345

872919345 00176255000000000000

Detach here and return upper portion with check or money order. Do not staple or fold.

Statement of Personal Credit Card Account

Retain this portion for your files.

Cardmember Name	Account Number	Statement Closing Date
STEVEN CHARLES	1234-456-890	01-31-14

Statement Date: 02-01-14 Payment Due Date: 03-01-14
Closing Date: 01-31-14
Credit Limit: \$50,000 Credit Available: \$10,000
New Balance: \$40,000 Minimum Payment Due: \$8,000

Account Summary

Previous Balance:	+0	Transaction Fees:	+0
Purchases:	+40,000	Annual Fees:	+0
Cash Advances:	+0	Current Amount Due:	+40,000
Payments:	+0	Amount Past Due:	+0
Finance Charge:	+0	Amount Over Credit Line:	+0
Late Charge:	+0	NEW BALANCE:	+40,000

Reference Number	Sold	Posted	Activity Since Last Statement	Amount
43210987	01-03	01-13	Payment, Thank You	-\$74.25
01234567	01-12	01-13	Wings 'N' Things Anytown, USA	\$25.25
78901234	01-14	01-17	Record Release Anytown, USA	\$40.00
45678901	01-14	01-17	Sports Stadium Anytown, USA	\$75.25
3210987	01-22	01-23	Tie Tack Anytown, USA	\$8,850
76543210	01-29	01-30	Electronic World Anytown, USA	\$30,000

PAGE 1 OF 1



Identity Theft - Serious Problem



- Identity theft is a **serious problem and number of violations** are increasing rapidly
- Some of the ways **to minimize the risk of identity theft** include checking the credit card reports periodically, safeguarding personal information at home and in the workplace, verifying the legality of sources, etc.



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

The screenshot shows the official website of the Federal Trade Commission (FTC). The header features the FTC logo and the tagline "Protecting America's Consumers". Navigation links include Home, News, Competition, Consumer Protection, Economics, General Counsel, Actions, Congressional, Policy, International, About the FTC, Commissioners, Offices & Bureaus, Inspector General, Jobs, Diversity, FOIA, and Budget & Performance. A search bar is located in the top right corner. The main content area includes a banner for the "10th Anniversary of the Do Not Call Registry", news about a "Record Civil Penalty in Do Not Call Case", and links for "Get Your Free Credit Report", "REGISTER TO VOTE", "FIGHTING BACK AGAINST IDENTITY THIEF", and "CONSUMER COMPLAINTS REPORT IT TO THE FTC". A "FTC NEWS" section highlights the approval of Kinder Morgan's acquisition of El Paso Corp. A "FEATURED TOPICS" sidebar lists various consumer protection issues such as Administrative Law Judge Cases, Advertising & Marketing, Antitrust & Mergers, Clothing & Textiles Information, Commission Actions, Conferences & Workshops, Consumer Resources, and Getting Your Money Back.

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

<http://www.ftc.gov>

Module Flow



1

Social Engineering Concepts

2

Social Engineering Techniques

3

Impersonation on Social Networking Sites

4

Identity Theft

5

Social Engineering Countermeasures

6

Penetration Testing

Social Engineering Countermeasures



- 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

- 1 Periodic password change
- 2 Avoiding guessable passwords
- 3 Account blocking after failed attempts
- 4 Length and complexity of passwords
- 5 Secrecy of passwords

Physical Security Policies

- 1 Identification of employees by issuing ID cards, uniforms, etc.
- 2 Escorting the visitors
- 3 Access area restrictions
- 4 Proper shredding of useless documents
- 5 Employing security personnel

Social Engineering Countermeasures (Cont'd)



1

Training



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

2

Operational Guidelines



Make sure sensitive information is secured and resources are accessed only by authorized users

3

Access Privileges



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

4

Classification of Information



Categorize the information as top secret, proprietary, for internal use only, for public use, etc.

5

Proper Incidence Response Time



There should be proper guidelines for reacting in case of a social engineering attempt

6

Background Check and Proper Termination Process



Insiders with a criminal background and terminated employees are easy targets for procuring information

Social Engineering Countermeasures (Cont'd)



Anti-Virus/Anti-Phishing Defenses

Use **multiple layers** of anti-virus defenses at end-user and mail gateway levels to minimize social engineering attacks

Two-Factor Authentication

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

Change Management

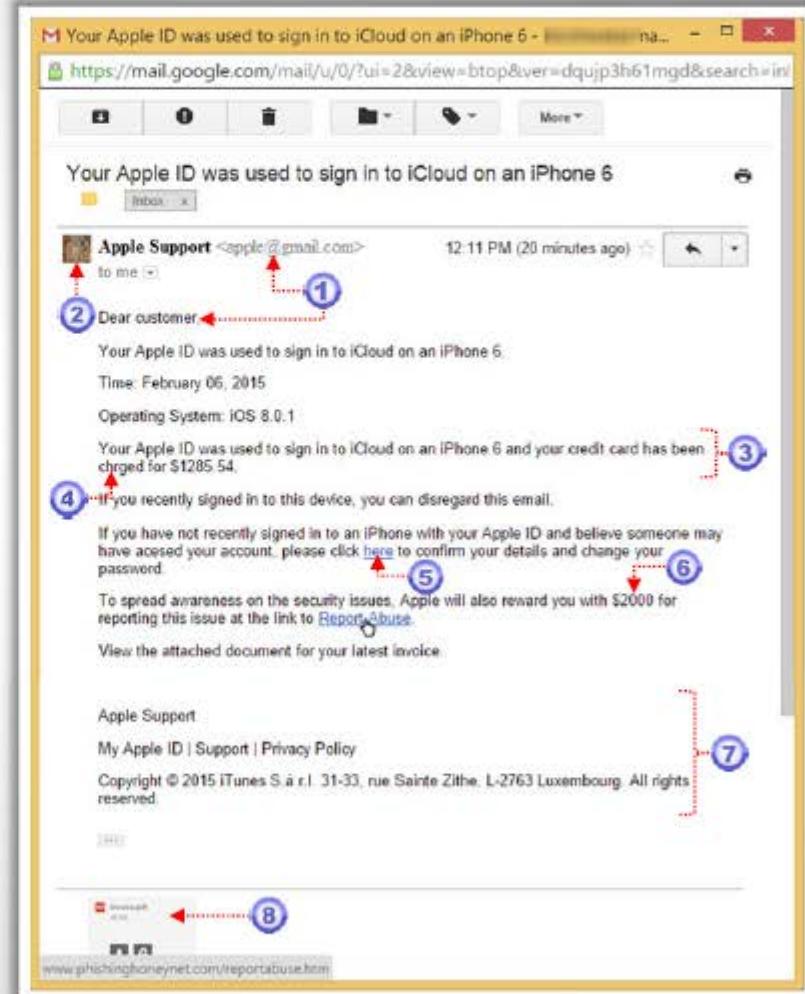
A **documented change-management** process is more secure than the ad-hoc process



How to Detect Phishing Emails

CEH
Certified Ethical Hacker

- 1 Seem to be from a **bank, company, or social networking site** and have a **generic greeting**
- 2 Seem to be from a person listed in your **email address book**
- 3 Gives a sense of **urgency** or a **veiled threat**
- 4 May contain **grammatical/spelling mistakes**
- 5 Includes links to **spoofed websites**
- 6 May contain **offers that seem to be too good to believe**
- 7 Includes **official-looking logos** and other information taken from legitimate websites
- 8 May contain a **malicious attachment**



Anti-Phishing Toolbar: Netcraft



The image shows two browser windows demonstrating the Netcraft Toolbar. The left window is the EC-Council website, and the right window is the Netcraft Most Visited Web Sites page.

EC-Council Website: A screenshot of the EC-Council homepage. It features a large banner with a man in a suit at a starting line, the text "Hire a CEH. He can Protect your network from", and several navigation links like Home, Certification, Training, Services, Store, and Support. A sidebar on the left offers "Weekly Monday Presentations" and "Selling Secrets of Phishers to Advertisers".

Netcraft Toolbar: An orange callout box points to the toolbar icon in the browser's address bar of both windows. The toolbar icon is a blue arrow pointing down next to a yellow disc.

Netcraft Most Visited Web Sites: A screenshot of the Netcraft toolbar extension's interface. It shows a dropdown menu with options like "Tell a Friend", "Frequently Asked Questions", "Glossary", "Phishing Blocking & Phishing Site", "Phished Countries", and "Phished Hosts". The "Most Visited Web Sites" option is highlighted. Below the menu, a table lists the top 23 most visited websites with their first seen date, last block date, and country. The table includes rows for Google, Facebook, YouTube, and Twitter.

Rank	Website	Last Seen	Last Block	Country
1	www.google.com	May 2002	Google Inc.	US
2	http://www.facebook.com	November 2007	Facebook, Inc.	US
3	http://www.youtube.com	September 1998	Google Inc.	US
4	http://mail.google.com	August 2003	Google Inc.	US
5	http://www.wikipedia.org	April 2005	Wikimedia Foundation, Inc.	US
6	http://www.facebook.com	May 1997	Facebook, Inc.	US
7	http://accounts.google.com	March 2003	Google Inc.	US
8	http://www.google.de	April 1999	Google Inc.	DE
9	http://www.google.de	January 2013	Google Inc.	DE
10	https://www.google.it	January 2013	Google Inc.	IT
11	http://www.google.it	November 2001	Google Inc.	IT
12	https://twitter.com	June 2007	Twitter Inc.	US
13	http://www.google.it	March 2000	Google Inc.	IT
14	https://en.wikipedia.org	November 2005	Wikimedia Foundation, Inc.	IT
15	https://aws.amazon.com	October 2013	Amazon Web Services, Inc.	US
16	https://www.youtube.com	April 2013	Google Inc.	US
17	http://www.google.it	January 2013	Google Inc.	IT
18	https://www.google.co.uk	January 2013	Google Inc.	GB
19	http://www.google.co.uk	April 1999	Google Inc.	GB
20	https://apps.facebook.com	February 2013	Facebook, Inc.	US
21	http://www.amazon.com	October 1995	Amazon.com, Inc.	US
22	https://accounts.netflix.com	April 2013	Netflix, Inc.	US
23	http://www.googleadservices.com	September 2003	Google Inc.	US

The Netcraft **anti-phishing community** is effectively a giant neighborhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing attacks.

<http://toolbar.netcraft.com>

Anti-Phishing Toolbar: PhishTank



- PhishTank is a collaborative clearing house for data and information about **phishing** on the Internet
- It provides an **open API** for developers and researchers to integrate **anti-phishing data** into their applications



The screenshot shows the PhishTank homepage with a search bar for suspected phishing sites. Below it, a table lists 20 recent submissions, each with a unique ID, URL, and the user who submitted it. A sidebar on the right explains what phishing is and what PhishTank does.

ID	URL	Submitted by
2085837	http://www.caiaut-total.my/include/s/B14D1TQ/RB1...	bearminical
2085838	http://www3.vpxg.vnet.com.br/images/bg-input-login...	deanmo
2085839	http://www.eeasyjerseys.com/contact_us.html	newwin
2085840	http://www.sendmailbox.biz/tl.php?p=s8/s8/rs/1lq3/...	newwin
2085841	http://www.eeasyjerseys.com/nike-pittsburgh-steeler...	newwin
2085842	http://www.sendmailbox.biz/tl.php?p=s8/s8/rs/1lq3/...	newwin
2085843	http://www.eeasyjerseys.com/nike-houston-texans-99...	newwin
2085844	http://www.sendmailbox.biz/tl.php?p=s8/s8/rs/1lq3/...	newwin
2085845	http://www.eeasyjerseys.com/nike-denver-broncos-18...	newwin
2085846	http://www.sendmailbox.biz/tl.php?p=s8/s8/rs/1lq3/...	newwin
2085847	http://www.eeasyjerseys.com/nike-san-francisco-49er...	newwin
2085848	http://www.sendmailbox.biz/tl.php?p=s8/s8/rs/1lq3/...	newwin
2085849	http://www.eeasyjerseys.com/nike-seattle-seahawks-3...	newwin
2085850	http://www.sendmailbox.biz/tl.php?p=s8/s8/rs/1lq3/...	newwin
2085851	http://www.eeasyjerseys.com/nike-washington-redskin...	newwin

<http://www.phishtank.com>

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 and never let it go out of 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



1

Social Engineering Concepts

2

Social Engineering Techniques

3

Impersonation on Social Networking Sites

4

Identity Theft

5

Social Engineering Countermeasures

6

Penetration Testing

Social Engineering Pen 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 level of security awareness** among employees

Tester should **demonstrate extreme care and professionalism** for social engineering pen test as it might involve legal issues

01

Good Interpersonal Skills



02

Good Communication Skills



03

Creative



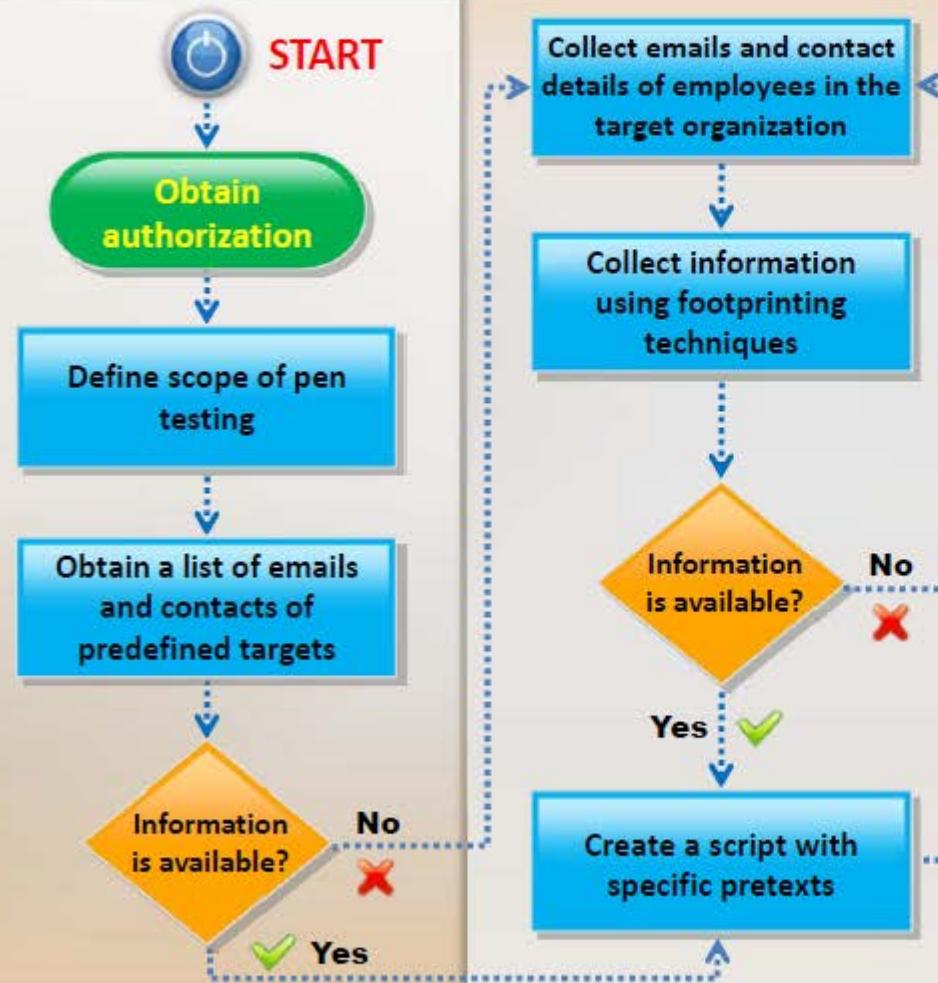
04

Talkative and Friendly Nature



Social Engineering Pen Testing

(Cont'd)

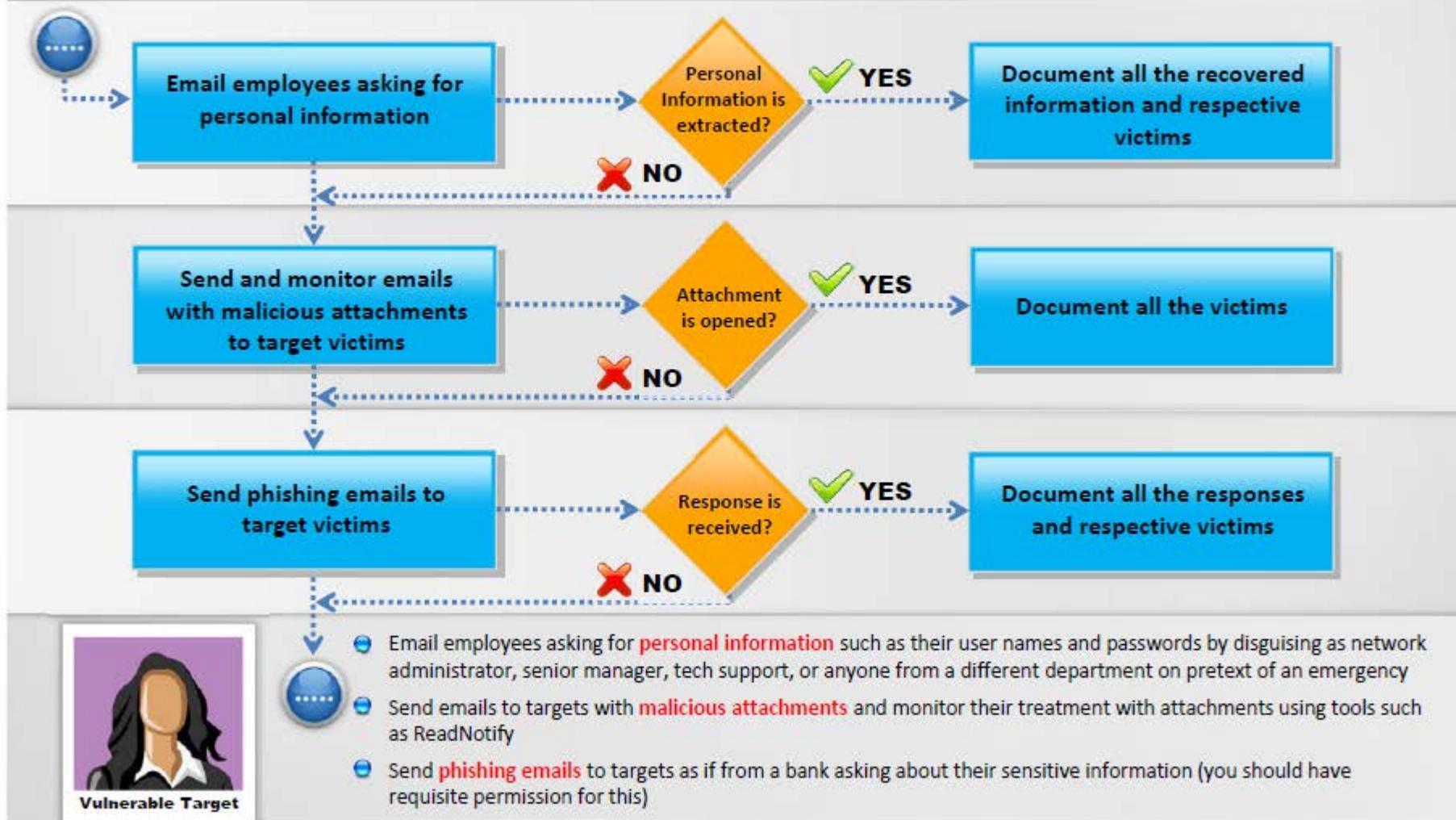


- Obtain management's explicit **authorization** and details that will help in **defining scope** of pen-test such as list of departments, employees that need to be tested, or level of physical intrusion allowed
- Collect **email addresses and contact details** of target organization and its human resources (if not provided) using techniques such as **dumpster diving**, email guessing, USENET and web search, and email spiders
- 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

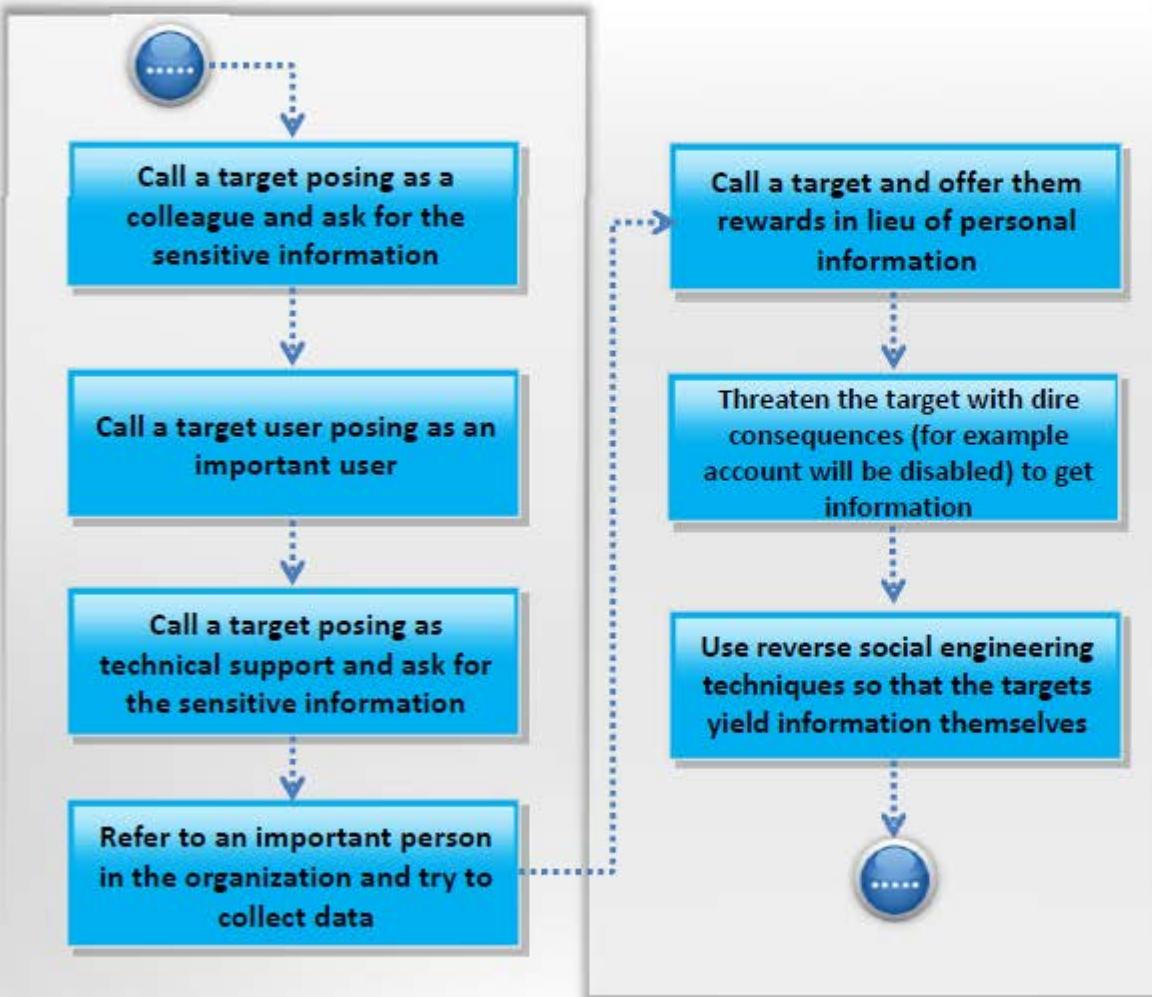


Social Engineering Pen Testing: Using Emails

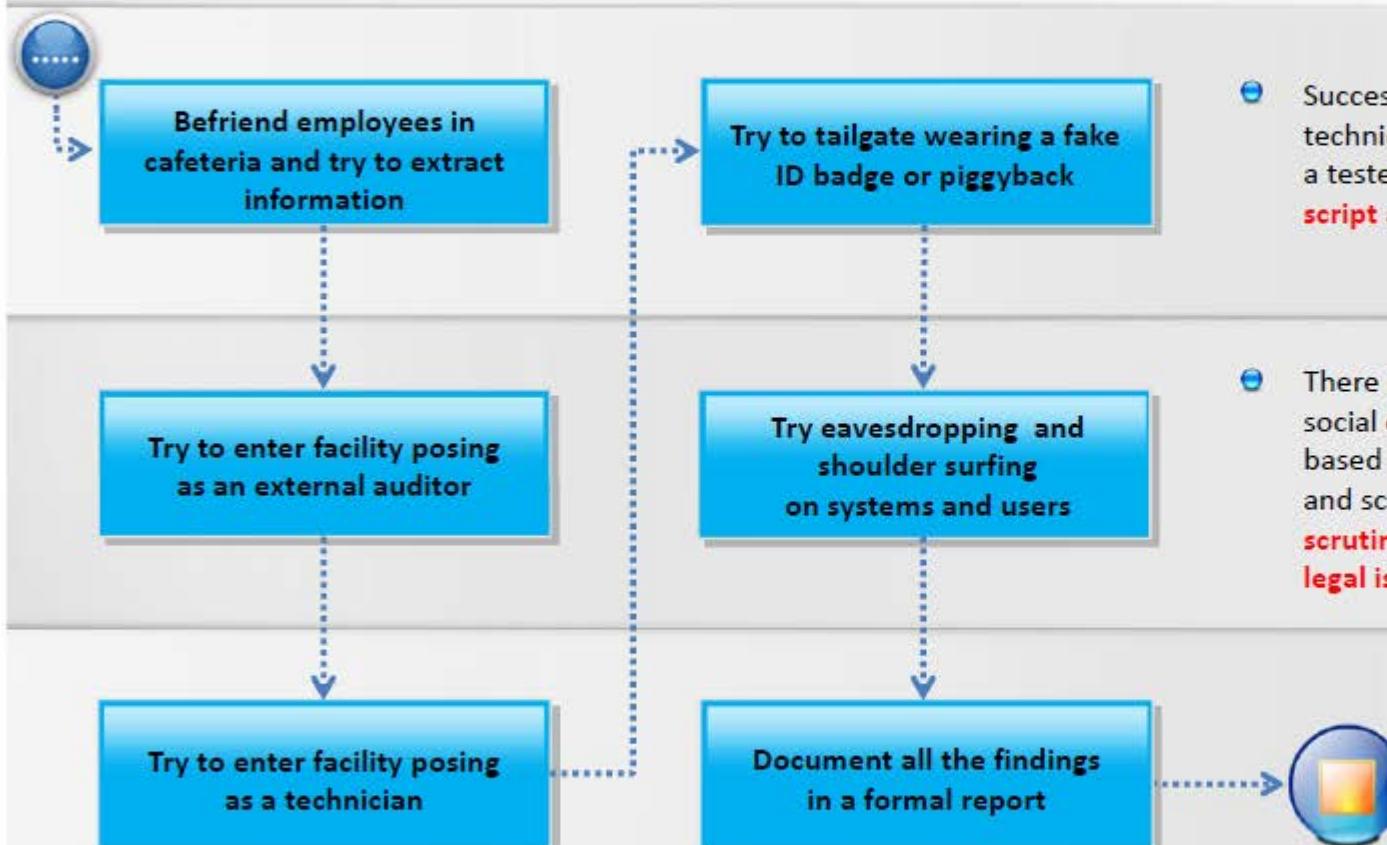
CEH
Certified Ethical Hacker



Social Engineering Pen Testing: Using Phone



Social Engineering Pen Testing: In Person



- Success of any social engineering technique depends on how well a tester can **enact the testing script** and his **interpersonal skills**
- There could be countless other social engineering techniques based on available information and scope of test. **Always scrutinize your testing steps for legal issues**

Social Engineering Pen Testing: Social Engineering Toolkit (SET)



```
root@kali: /usr/share/set
File Edit View Search Terminal Help
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:
[1] Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Metasploit Framework
5) Update the Social-Engineer Toolkit
6) Update SET configuration
7) Help, Credits, and About

99) Exit the Social-Engineer Toolkit
set> 1
```

```
root@kali: /usr/share/set
File Edit View Search Terminal Help
Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Powershell Attack Vectors
11) Third Party Modules

99) Return back to the main menu.
set> 1
```

<https://www.trustedsec.com>

- The Social-Engineer Toolkit (SET) is an open-source **Python-driven tool** aimed at penetration testing around social engineering

```
root@kali: /usr/share/set
File Edit View Search Terminal Help
root@kali: # cd /usr/share/set
root@kali:/usr/share/set# ./setoolkit
[-] New set_config.py file generated on: 2014-01-07 17:37:33.498403
[-] Verifying configuration update...
[*] Update verified, config timestamp is: 2014-01-07 17:37:33.498403
[*] SET is using the new config, no need to restart

0101100101101110101001000000011100
1001100101010000101101100011011000111
10010010000001101000011000010111011001
100101001000000011101000011000011011100100000
011011010110100001011010000010000001000000
000111010001010010101100110011001100110010
000001011101011011000100000000111100101
10111101101011011010001000000001101000000
011000010110110011001000111001100100000000
0000011010001010100101001000100000000101
010001101000001100001011011100110181101
1100110010000000110011001101110011018110
0010000001110101011100110110100010100010
10010011100100000011101000101000000110
010100100000010100110110111101100001101
1010010110000010101010000101010101010101
```



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
- ❑ Attackers attempt social engineering attacks on office workers to extract sensitive data
- ❑ 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
- ❑ Identity theft occurs when someone steals your name and other personal information for fraudulent purposes
- ❑ A successful defense depends on having good policies and their diligent implementation