

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

90% of all email
is spam or virus



77% Percentage of
phishing of all socially
based attacks

13.3 Million user
reported phishing
attacks in 2013



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?

26%
Call a
number



14% Reply
to text

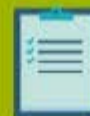
60% Click
on a link

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 **EG-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Objectives

- 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?



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



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

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



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.

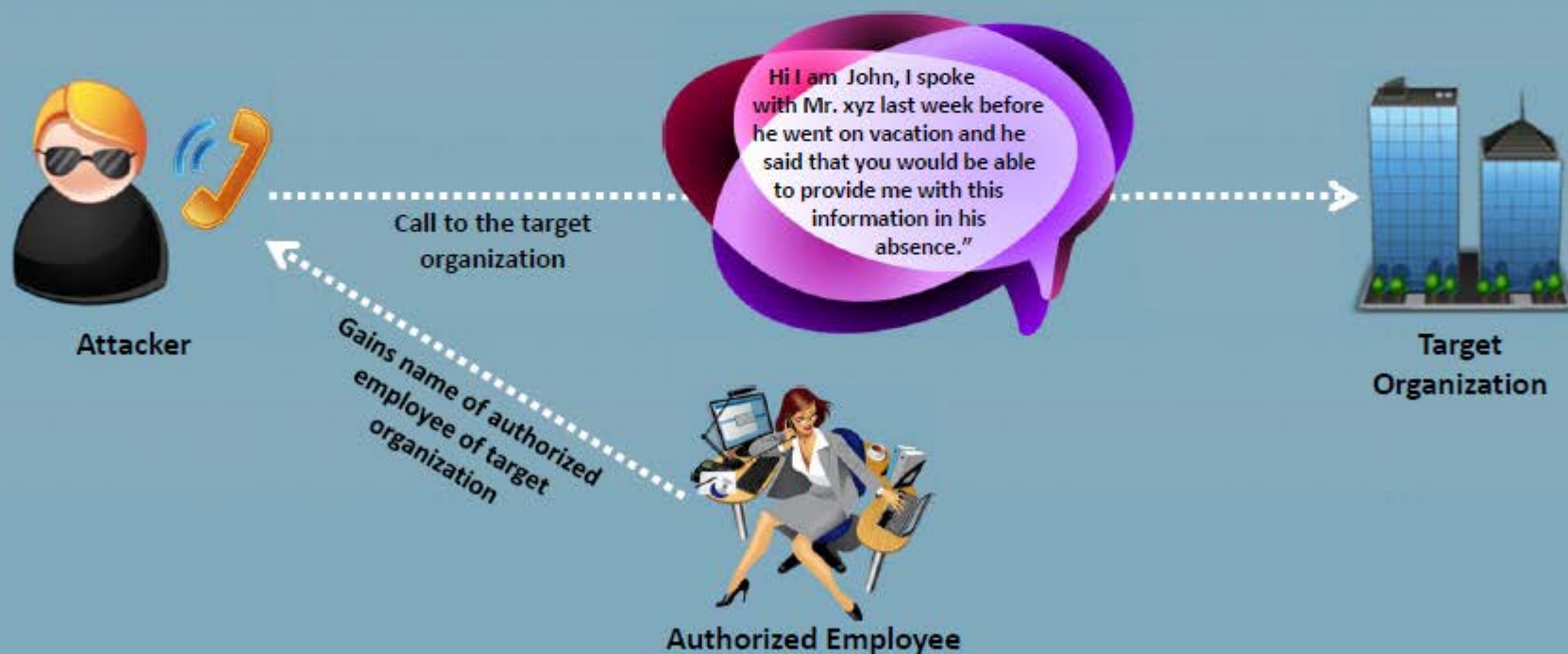
The help desk worker feels sorry for him and quickly resets the password, unwittingly giving the attacker clear entrance into the corporate network ”

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**

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

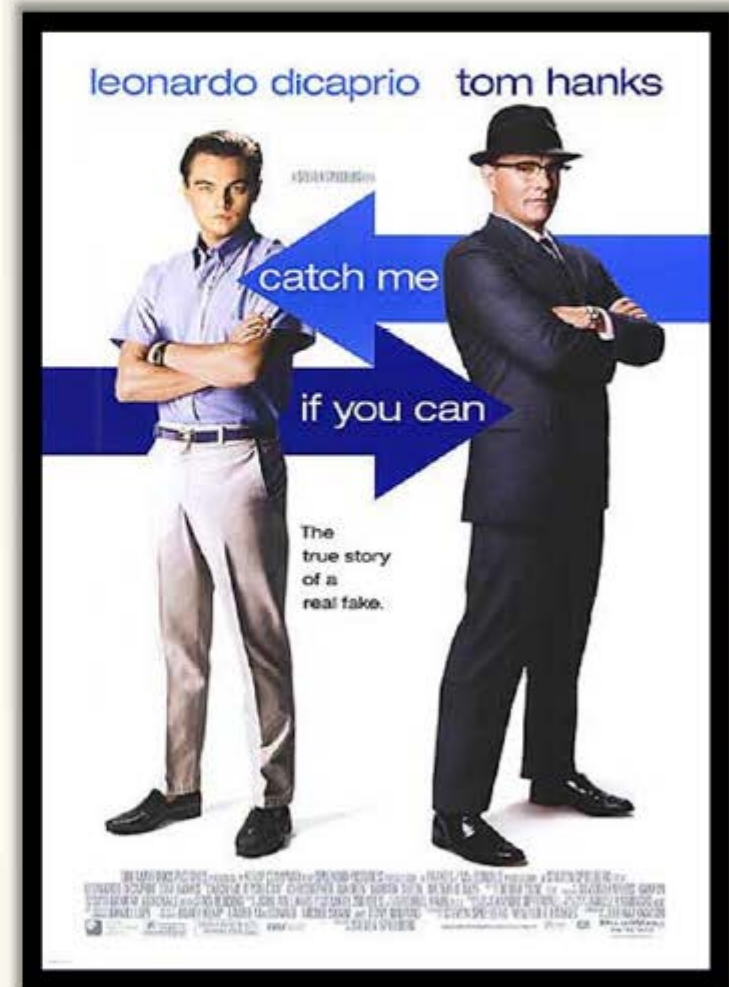
- "I forgot my ID badge at home. Please help me."
- An authorized person allows (intentionally or unintentionally) an **unauthorized person** to pass through a secure door

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

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**



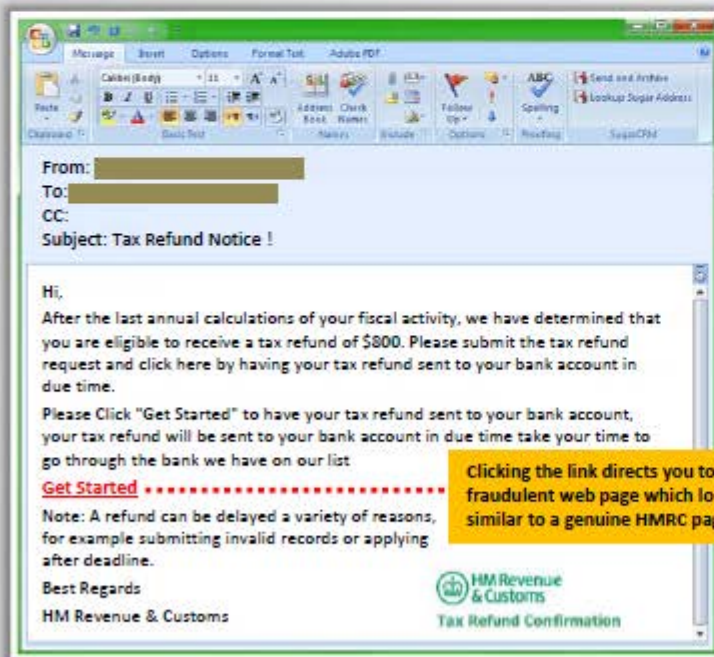
Computer-based Social Engineering: Phishing



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



Clicking the link directs you to a fraudulent web page which looks similar to a genuine HMRC page

<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



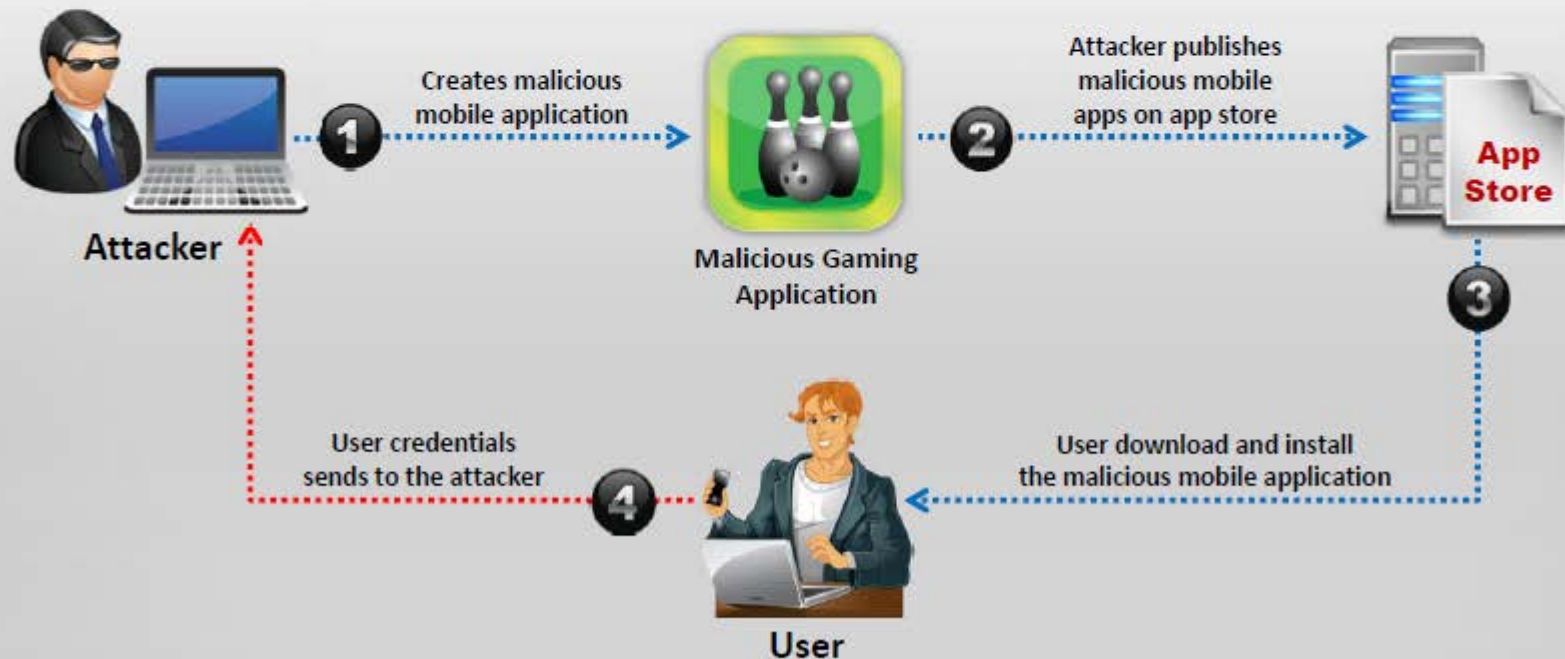
Mobile-based Social Engineering: Publishing Malicious Apps



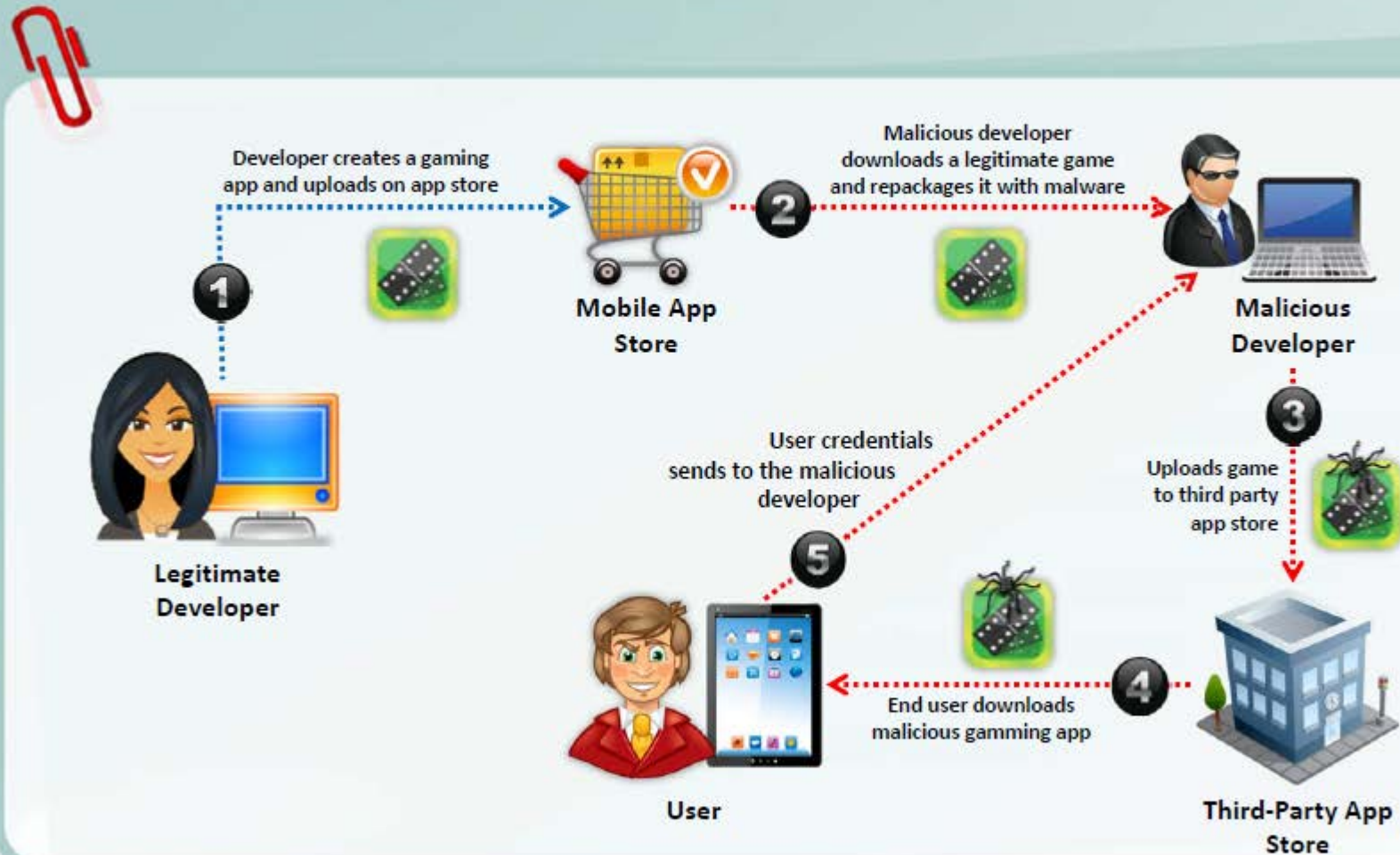
Attackers create **malicious apps** with attractive features and **similar names** to that of popular apps, and publish them on major **app stores**



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



Mobile-based Social Engineering: Repackaging Legitimate Apps



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

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



Attacker

Sends a **SMS**



Thinking it is XIM Bank customer service number



Tracy calling to 08-7999-433

It was a **recording** asking to provide her credit card or debit card number. Tracy **revealed sensitive information**

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

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



Disgruntled Employee



Company's Secrets



Company Network

Sends the data to competitors using **steganography**



Competitors

Preventing Insider Threats

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



Organization Details

Professional Details

Contacts and Connections

Personal Details

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

About

The Official John Legend Facebook Page
Get #LoveInTheFuture now <http://smarturl.it/LoveInTheFutureDX>
<http://johnlegend.tumblr.com/>
www.johnlegend.com

Biography

John Legend is a nine-time Grammy Award winning recording artist, critically-acclaimed concert performer, philanthropist/social activist, and was named one of Time magazine's 100 most influential people. Legend's debut album, Get Lifted (2004) sold more than three million copies worldwide and earned an astounding eight Grammy nominations with three wins for Best New Artist, Best Male R&B Vocal Per... See More

Artists We Also Like

Estelle, Vaughn Anthony, Kanye West, Good Music

Basic Info

Founded 2000

Genre R&B/Soul

Members John Legend

Hometown Springfield, OH

Record Label GOOD Music- Sony/Columbia

General Manager Atom Factory / Troy Carter

Influences Stevie Wonder, Ne-Yo, Al Green, Jeff Buckley

Current Location New York

Contact Info

Website <http://www.johnlegend.com>
<http://www.showme.campaign.org>
<http://www.twitter.com/johnlegend>
<http://www.twitter.com/showme.campaign>
<http://www.myspace.com/johnlegend>
<http://www.youtube.com/johnlegend>

Booking Agent Creative Artists Agency

Life Events

2011 🎵 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

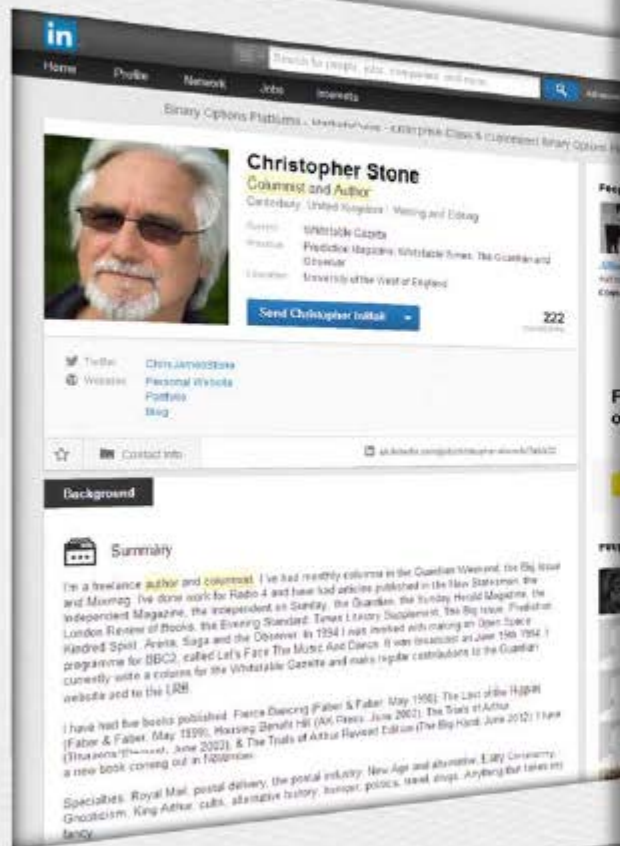
Using a **false identity**, attacker then proceeds to "friend," or invite, employees to the fake group, "Employees of the company"

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>

Social Engineering on LinkedIn and Twitter



<http://www.linkedin.com>



<http://twitter.com>

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

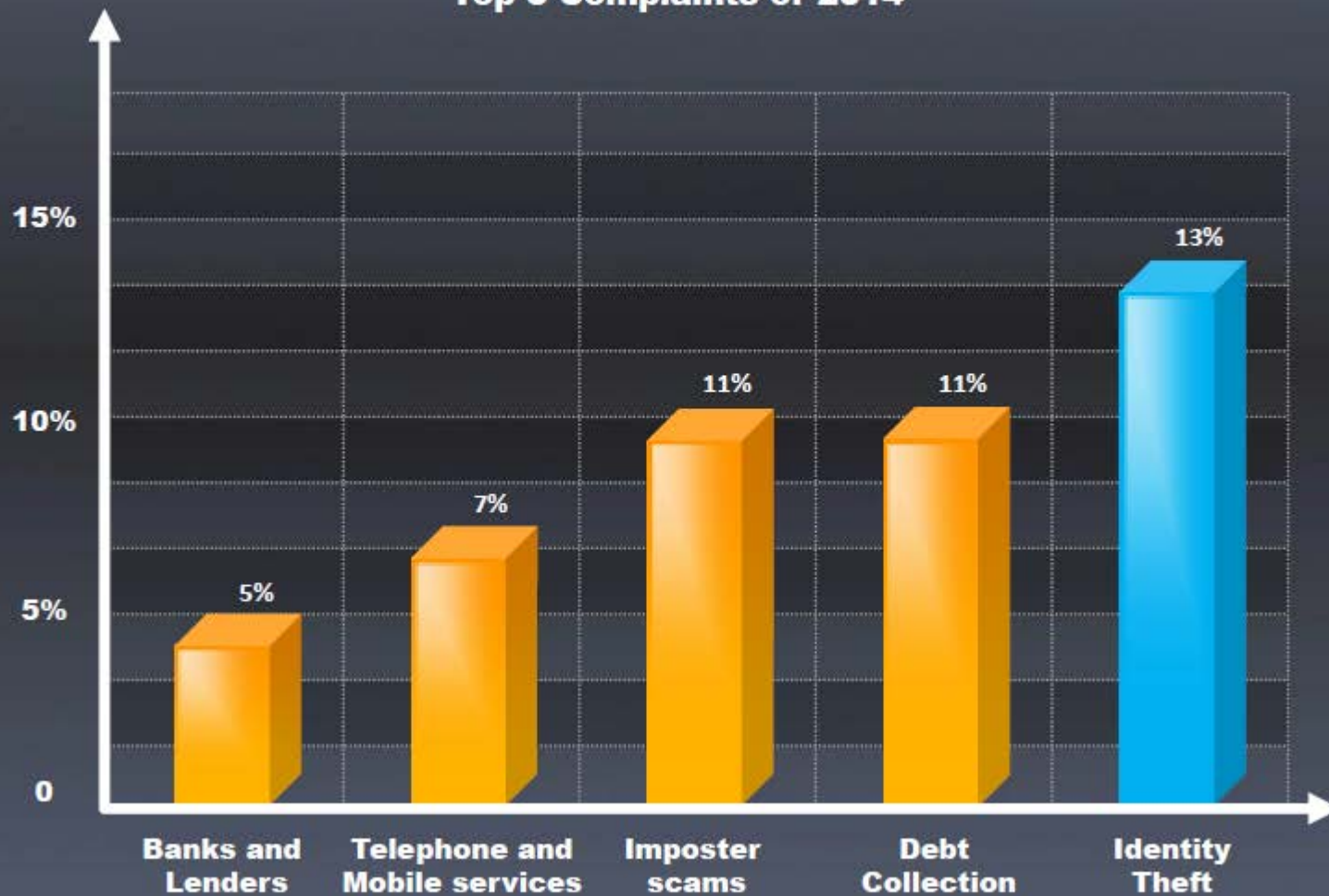
**Social Engineering
Countermeasures**

6

Penetration Testing

Identity Theft Statistics

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

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.

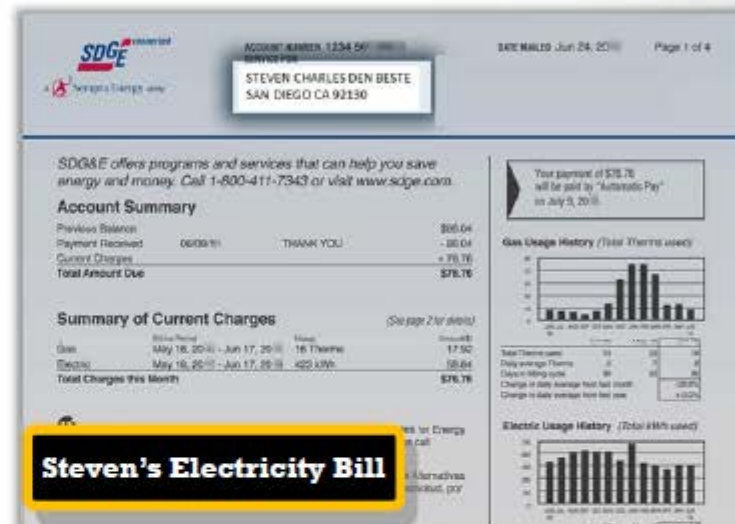
STEP 1

CEH
Certified Ethical Hacker

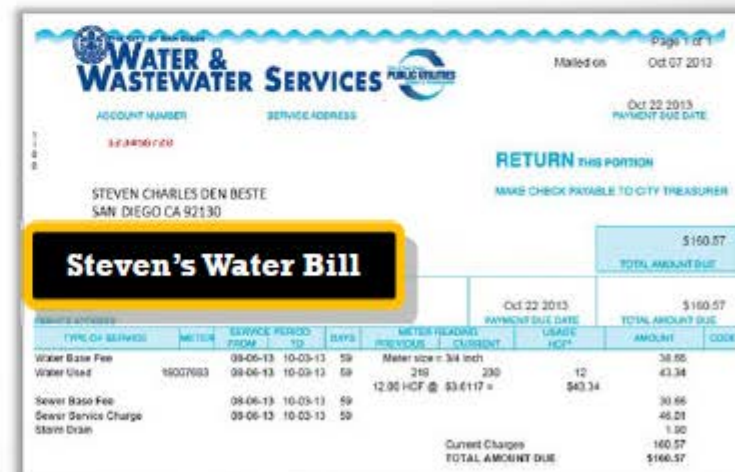
- Search for Steven's address on **social networking sites** (Facebook, Twitter, etc.) or on **people search sites**
- Get hold of Steven's telephone bill, water bill, or electricity bill using **dumpster diving**, **stolen email**, or **onsite stealing**



Steven's Address

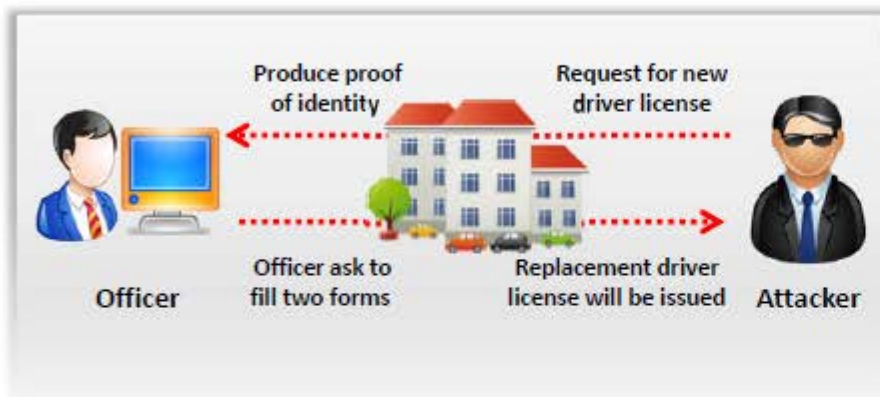


Steven's Electricity Bill



Steven's Water Bill

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

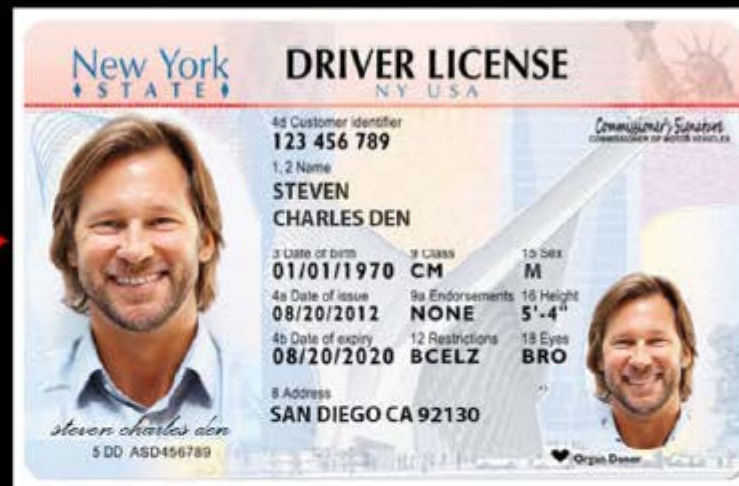
Your replacement driver license will be issued to your **new home address**

08

Now you are ready to have some serious fun

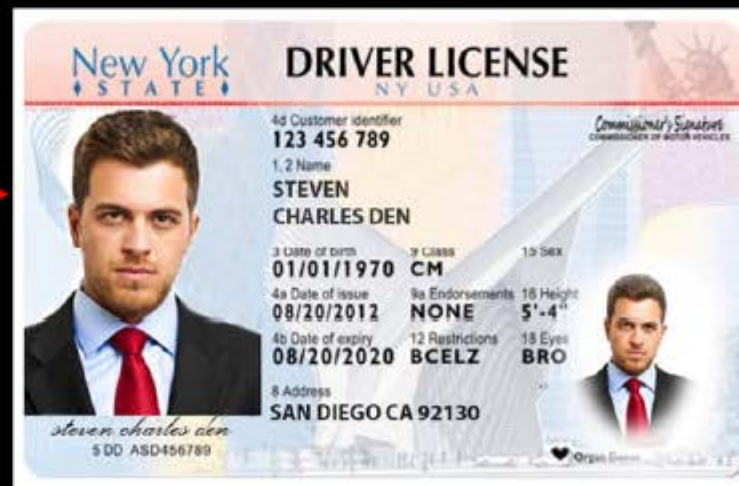
Comparison

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



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

STEVEN CHARLES DEN BESTE
SAN DIEGO CA 92130
872919345 00176255000000003

MAIL PAYMENT TO:
EA BANK
100 BANK STREET
ANYTOWN, USA 92101-1000

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 STEVEN CHARLES	Account Number 1234-456-890	Statement Closing Date 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	\$9,850
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

Home | News | Competition | Consumer Protection | Economics | General Counsel | Actions | Congressional | Policy | International
About the FTC | Commissioners | Offices & Bureau | Inspector General | Jobs | Diversity | FOIA | Budget & Performance

10 Years of Do Not Call
Announcing a Record Civil Penalty

Record Civil Penalty in Do Not Call Case
Announced on the Registry's 10 Year Anniversary

Payday Lender Settles FTC Debt Collection Charges

Do Not Call Registry
On 10th anniversary, a record civil penalty for violating Do Not Call

Timeshare Rescale Scams
FTC, multinational partners act to halt travel fraud

Competition Counts
How Consumers Win When Businesses Compete

Get Your Free Credit Report
more

REGISTER TO IMPROVE YOUR CREDIT
more

FIGHTING BACK AGAINST IDENTITY THEFT
more

CONSUMER COMPLAINT: REPORT IT TO THE FTC
more

FTC NEWS
More News

For Your Information: October 31, 2013
FTC Approves Kinder Morgan, Inc.'s Request to Modify Final Decision and Order, Divestiture Agreement Related to 2012 Acquisition of El Paso Corp.
The Federal Trade Commission has approved a request by Kinder Morgan, Inc. that the Commission modify the final FTC order and approve a change to a related divestiture agreement.

Tips For Consumers: October 31, 2013
FTC Poses Eight Questions to Ask When Choosing a College After Military Service

FEATURED TOPICS

- Administrative Law Judge Cases
- Advertising & Marketing
- Antitrust & Mergers
- Clothing & Textiles Information
- Complaint Actions
- Conferences & Workshops
- Consumer Resources
- Getting Your Money Back

<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 Incident 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

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**

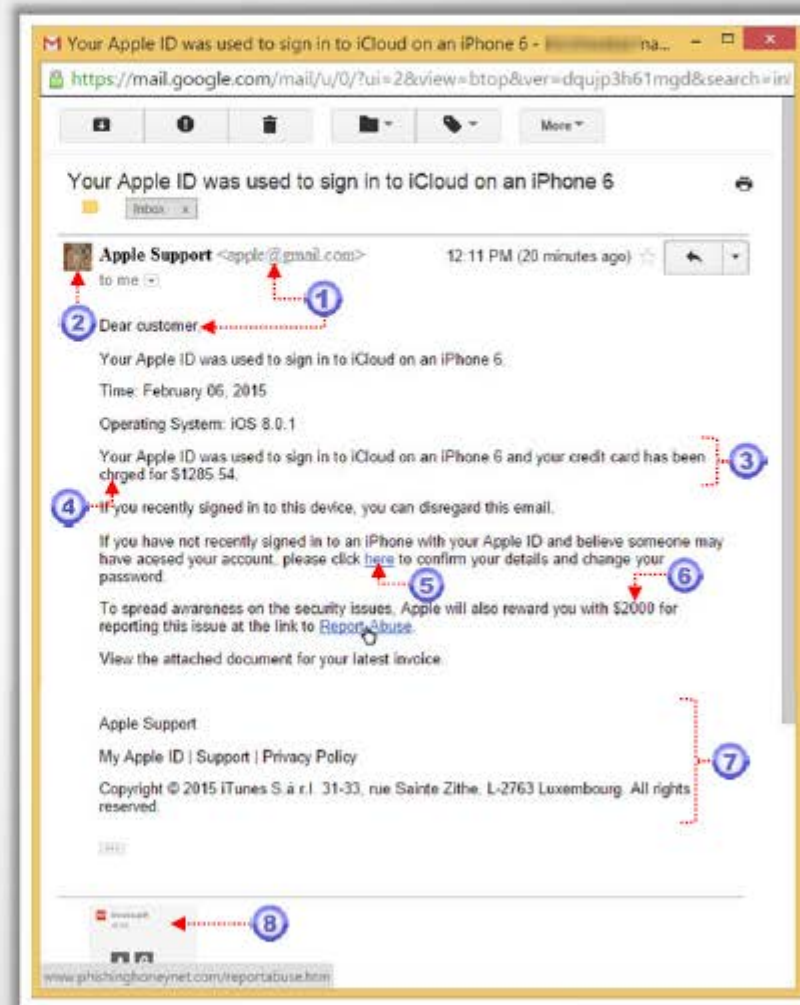
4 May contain **grammatical/spelling mistakes**

5 Includes links to **spoofed websites**

6 May contain **offers that seem to be too good to believe**

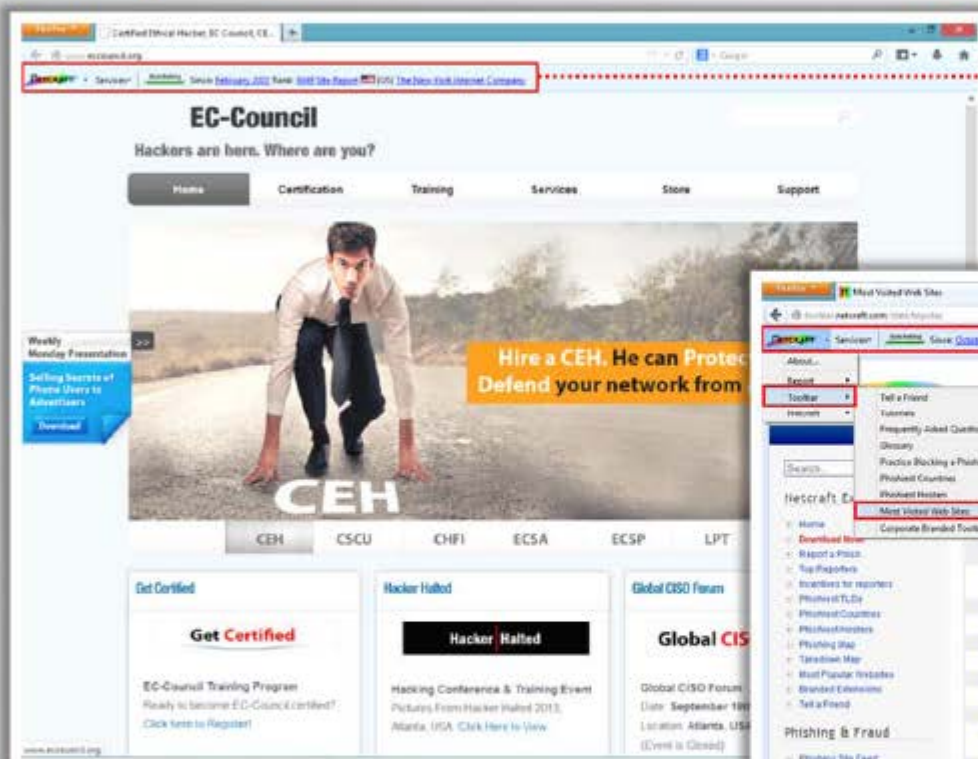
7 Includes **official-looking logos** and other information taken from legitimate websites

8 May contain a **malicious attachment**

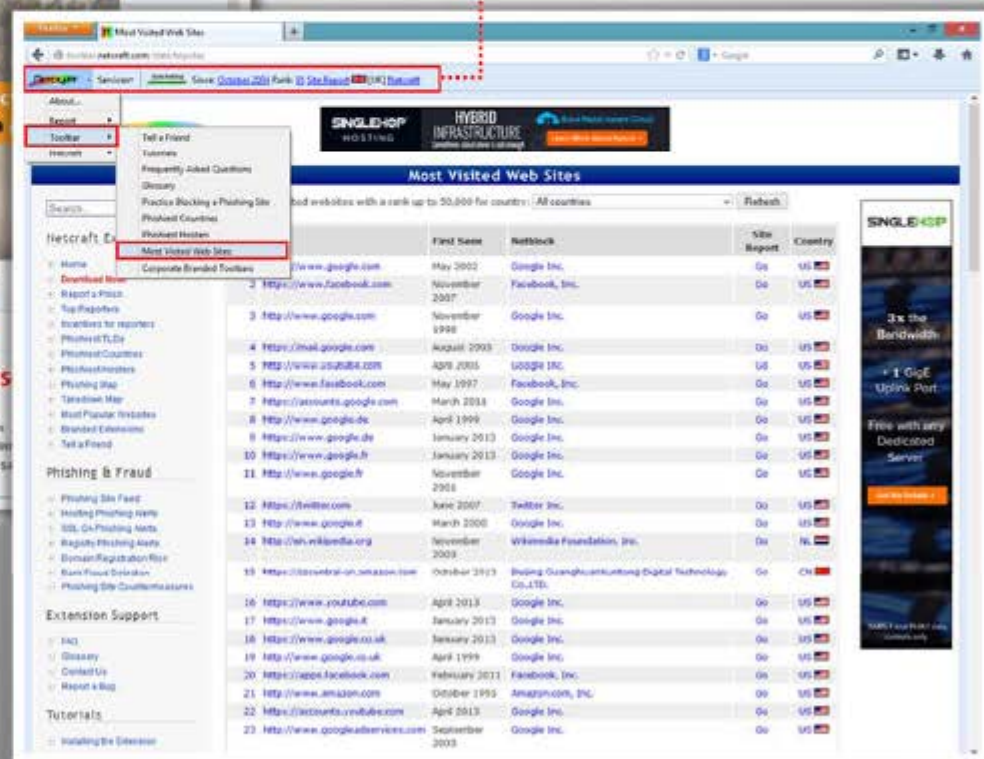


Anti-Phishing Toolbar: Netcraft

CEH
Certified Ethical Hacker



Netcraft Toolbar



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>

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

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



PhishTank | Join the Fight

PhishTank is operated by [OpenDNS](#), a free service that makes your Internet safer, faster, and smarter. [Get started today!](#)

PhishTank Out of the Net, into the Tank.

username: password: [Sign In](#)
[Register](#) | [Forgot Password](#)

[Home](#) [Add A Phish](#) [Verify A Phish](#) [Phish Search](#) [Stats](#) [FAQ](#) [Developers](#) [Helping Links](#) [My Account](#)

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:

[Is it a phish?](#)

Recent Submissions

You can help! [Sign in](#) or [register](#) (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
2085832	http://www.safad-total.org/includes/PB14D16D/PB1...	hsaspirat
2085830	http://www3.xpg.ua1.com.br/images/bg-input-login...	cleans
2085829	http://www.easyjerseys.com/contact_us.html	jocwin
2085828	http://www.sendmailbox.biz/tl.php?p=s8/s8/rs/1/q3/...	jocwin
2085827	http://www.easyjerseys.com/nike-pittsburgh-steelers...	jocwin
2085826	http://www.sendmailbox.biz/tl.php?p=s8/s8/rs/1/q3/...	jocwin
2085825	http://www.easyjerseys.com/nike-houston-texans-99...	jocwin
2085824	http://www.sendmailbox.biz/tl.php?p=s8/s8/rs/1/q3/...	jocwin
2085823	http://www.easyjerseys.com/nike-danver-broncos-18...	jocwin
2085822	http://www.sendmailbox.biz/tl.php?p=s8/s8/rs/1/q3/...	jocwin
2085821	http://www.easyjerseys.com/nike-san-francisco-49er...	jocwin
2085820	http://www.sendmailbox.biz/tl.php?p=s8/s8/rs/1/q3/...	jocwin
2085819	http://www.easyjerseys.com/nike-seattle-seahawks-3...	jocwin
2085818	http://www.sendmailbox.biz/tl.php?p=s8/s8/rs/1/q3/...	jocwin
2085817	http://www.easyjerseys.com/nike-washington-redskin...	jocwin

[See more suspected phishes...](#)

What is phishing?

Phishing is a fraudulent attempt, usually made through email, to steal your personal information. [Learn more...](#)

What is PhishTank?

PhishTank is a collaborative clearing house for data and information about phishing on the Internet. Also, PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge. [Read the FAQ...](#)

<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

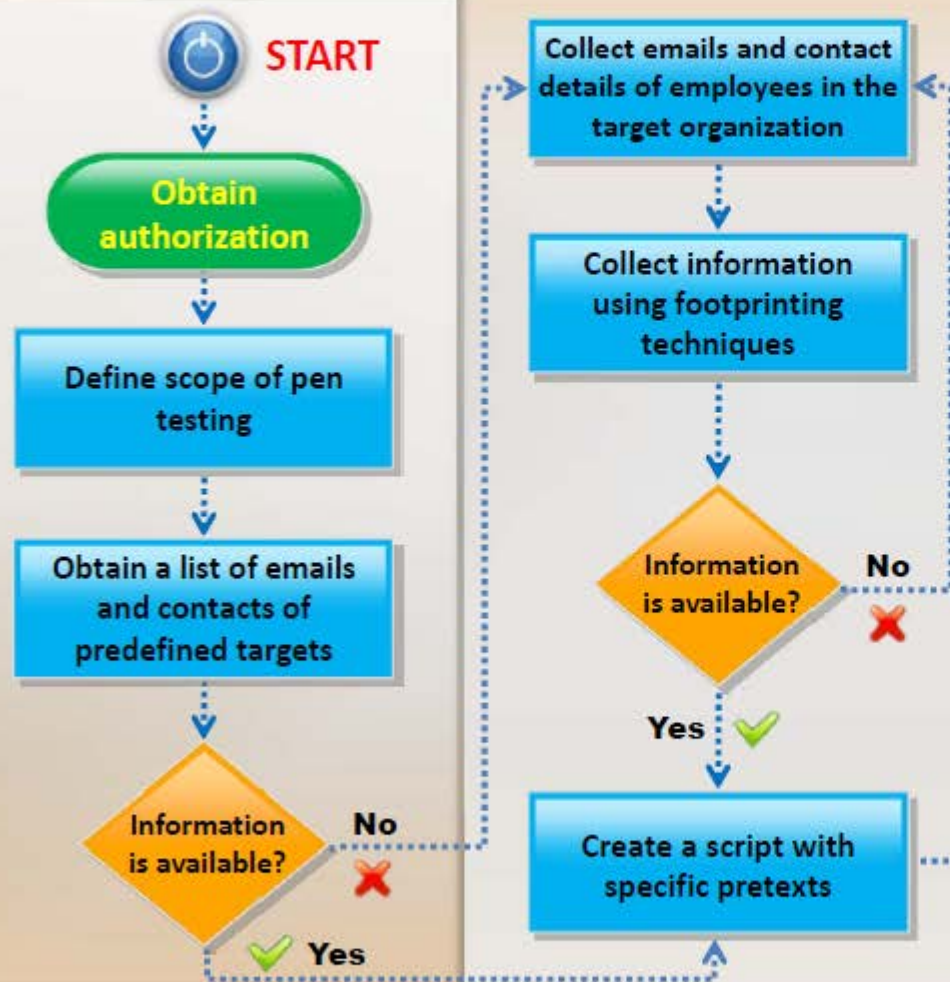


04

Talkative and Friendly Nature

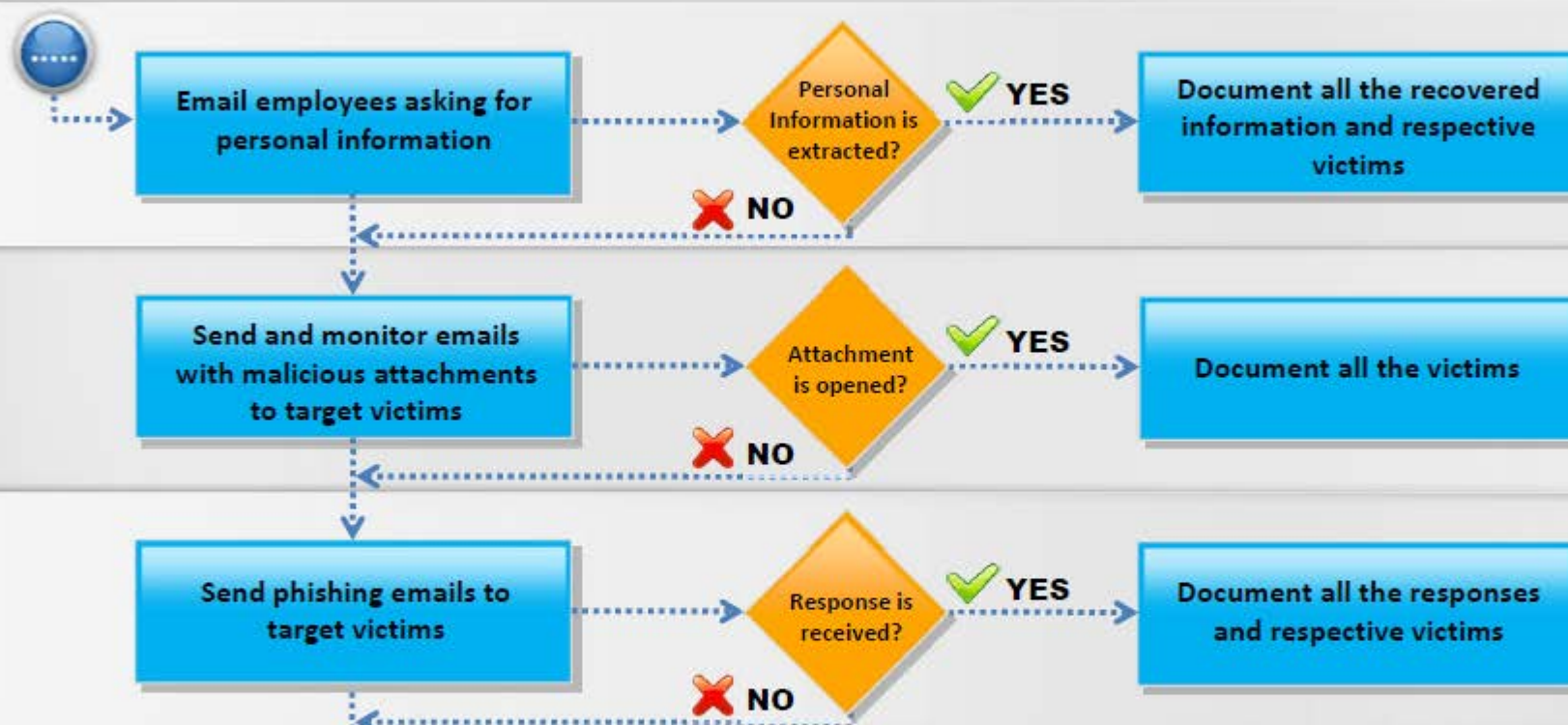


Social Engineering Pen Testing (Cont'd)



- 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

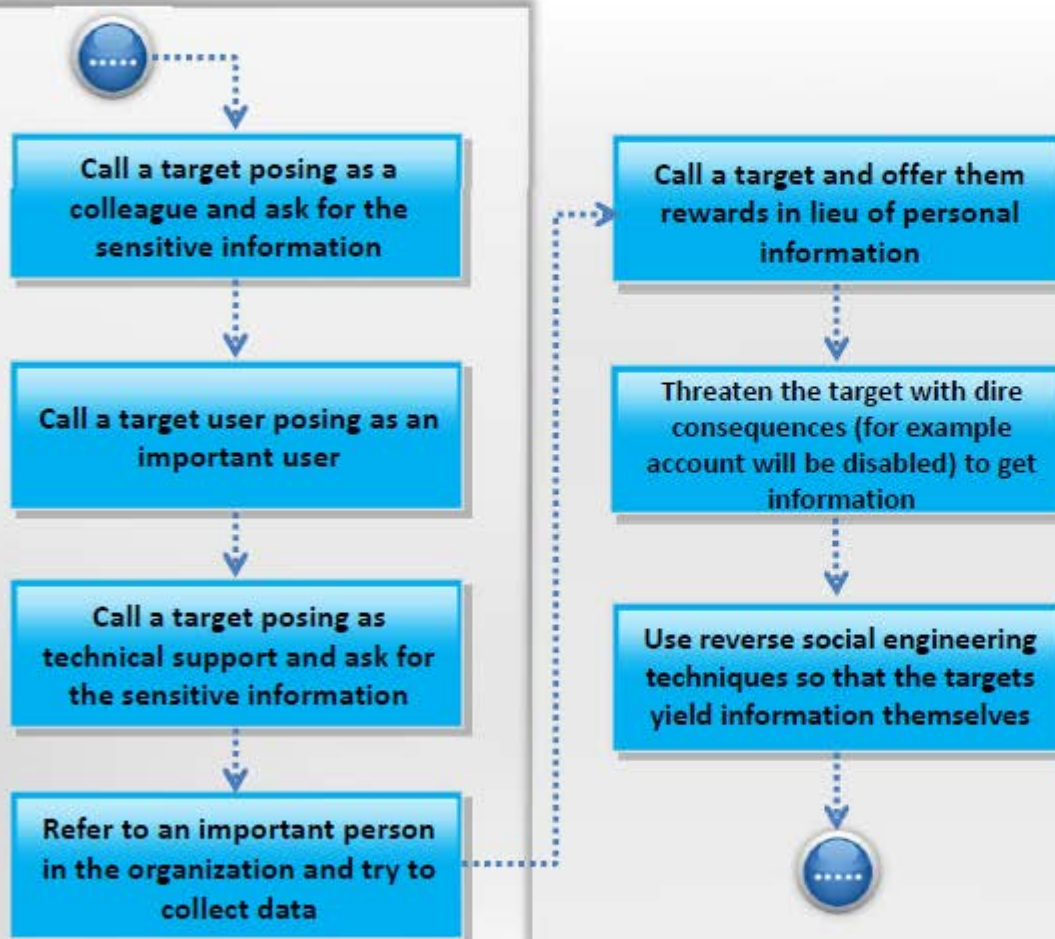
Social Engineering Pen Testing: Using Emails



Vulnerable Target

- 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



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



Social Engineering Pen Testing: Social Engineering Toolkit (SET)



- 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
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> 
```

```
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

0101100101101111011101010010000011100
1001100101011000010110110001011000111
1001001000000110100001100001011011001
100101001000000110100011011100100000
0110110101110101011000110110100001000
0001110100011010010110101011001010010
0000011011110110111000100000011100101
10111101110101011100100010000001101000
01100001011011100110010001110011001000
0001110100010110100101001001000000101
10001101000011000010110111001101101
1100110010000001100110011011101110010
0010000001101010111001101101001011011
10011001110010000001110100011010000100
0101001000000101001101101110110001101
10100101100001011011000010110101000101
```

<https://www.trustedsec.com>



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