



Don't fall in the trap

Arwa Alhamad | Cyber Security Sector

Table of content

• Introduction	4
• SE Backdoors	12
• SE Channels	20
• How to prevent from SE	28
• Summary	32

“War is based on deception.”

Sun-tzu, (~400 BC), The Art of War, Strategic Assessments



Introduction

Don't fall in the trap

SE - Introduction

Movie: Catch me if you can



Don't fall in the trap

SE - Introduction

Kevin Mitnick



Kevin Mitnick

Famous Social Engineer & Hacker

- Went to prison for hacking
- Became ethical hacker

“You could spend a fortune purchasing technology and services... and your network infrastructure **could still remain vulnerable to old-fashioned manipulation.**”

-Kevin Mitnick

SE - Introduction

Kevin Mitnick



- "People are generally helpful, especially to someone who is nice, knowledgeable or insistent."

"People inherently want to be helpful and therefore are easily duped"

"It's all about gaining access to information that people think is innocuous when it isn't"

-Kevin Mitnick

SE - Introduction

Social Engineering definition

Dictionary:

The application of sociological principles to specific social problems.



Information Security context:

Psychological manipulation of people into performing actions or divulging confidential information.

SE attacks can be both **technical** and **non-technical** in nature

SE - Introduction

Gartner Research

Gartner



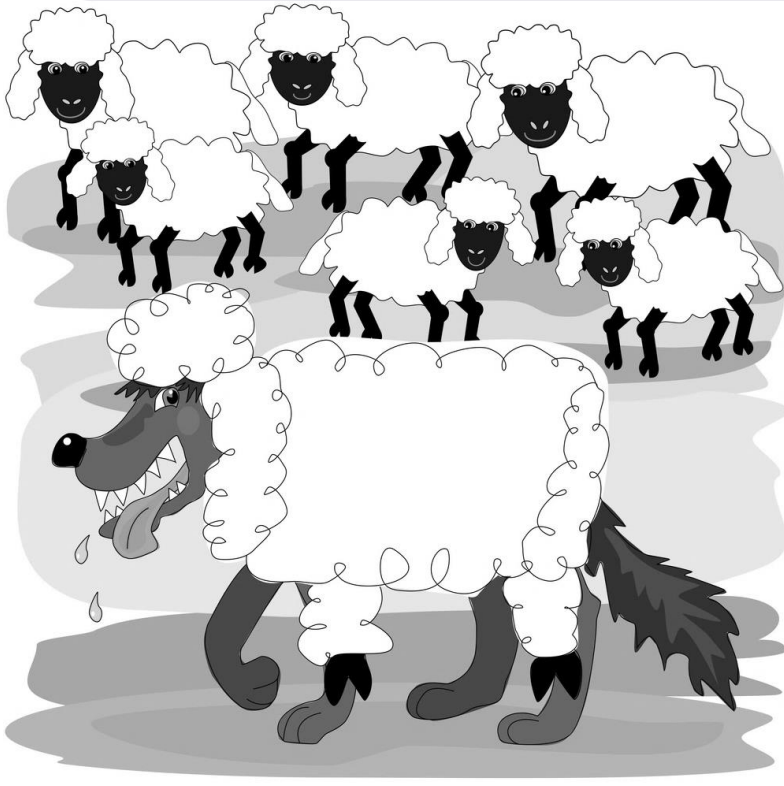
Gartner advised that the greatest security risk facing large companies and individual Internet users over the next 10 years will be the increasingly sophisticated use of social engineering to bypass IT security defenses

“We believe social engineering is the single greatest security risk in the decade ahead.”

Rich Mogull, Research VP, Gartner

SE - Introduction

Who Are Social Engineers?



Social Engineers are:

- Malicious hackers.
- Competitive intelligence.
- Cybercriminals.
- Terrorists.
- Scam artists.
- Disgruntled employees.

SE - Introduction

Why Do They Do It?

The goals of the social engineer are the same as any malicious hacker.
Social engineers are after:



Your
information.



Your
trade secrets.



Your
money.



Your
IT resources.

SE - Introduction

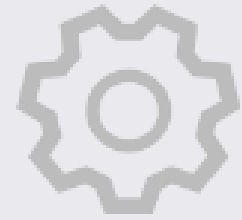
Why Social Engineering?

**Because It's
Easy...**



Easier to bypass human nature than multiple layers of technical defenses

**Because It
Works...**



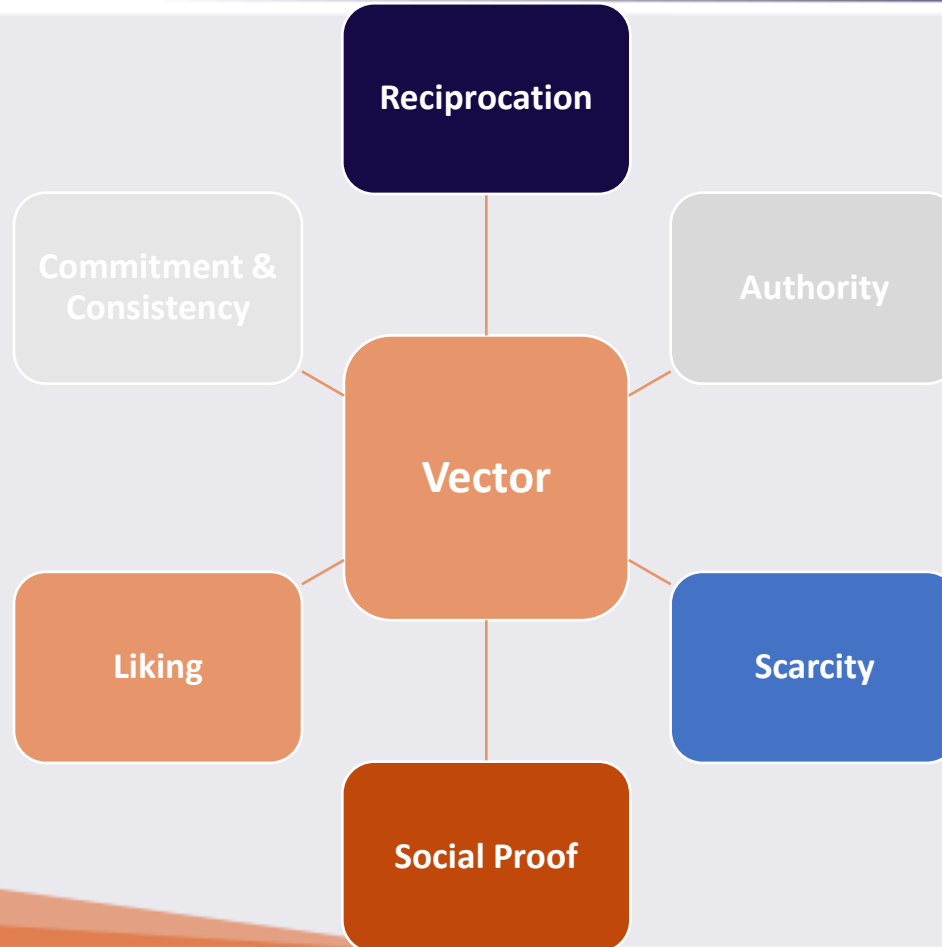
Results are predictable because humans are “engineered” to respond automatically to certain psychological triggers



Social Engineering Backdoors

Don't fall in the trap

SE Backdoors



SE Backdoors

Reciprocation



What is it?''''''

“Taking advantage of human desire to respond in kind to perceived favors.”

Example:''''''

Cup of coffee for your password?



Methods of Attack

- Offer false information to “help” user which forms an underlying obligation (reverse social engineering).

SE Backdoors

Authority



What is it?''''''

“Once we take a stand or commit, we need to be (and appear) consistent with what we have already said and done”

Example:

- The gym membership



Methods of Attack

- Give a new employee a false security policy then request their password to verify against policy.

SE Backdoors

Commitment and Consistency



What is it?''''''

People generally tend to conform to the dictates of authority figures'

Example:

- Milgram psychology experiments



Methods of Attack

- **Telephone:** Call to obtain a forgotten password or other information.
- **In Person:** Clothing, falsified badges.

SE Backdoors

Social Proof



What is it?.....

“Pressure to follow the crowd”

Example:

- Celebrity endorsements
- Canned laughter



Methods of Attack

- **Telephone:** Call to obtain a forgotten password or other information.
- **In Person:** Clothing, falsified badges.

SE Backdoors

Liking



What is it?.....

“Humans naturally tend to associate with those who like the same things, or are similar to them in some way”



Methods of Attack

- Through conversation, attacker probes for a personal connection to establish rapport
- “You like football? So do I! How about those Nassir Players!”

SE Backdoors

Scarcity



What is it?.....

“People tend to comply when they believe that an object is in short supply, highly sought after, or is available only in scarce quantities”



Methods of Attack

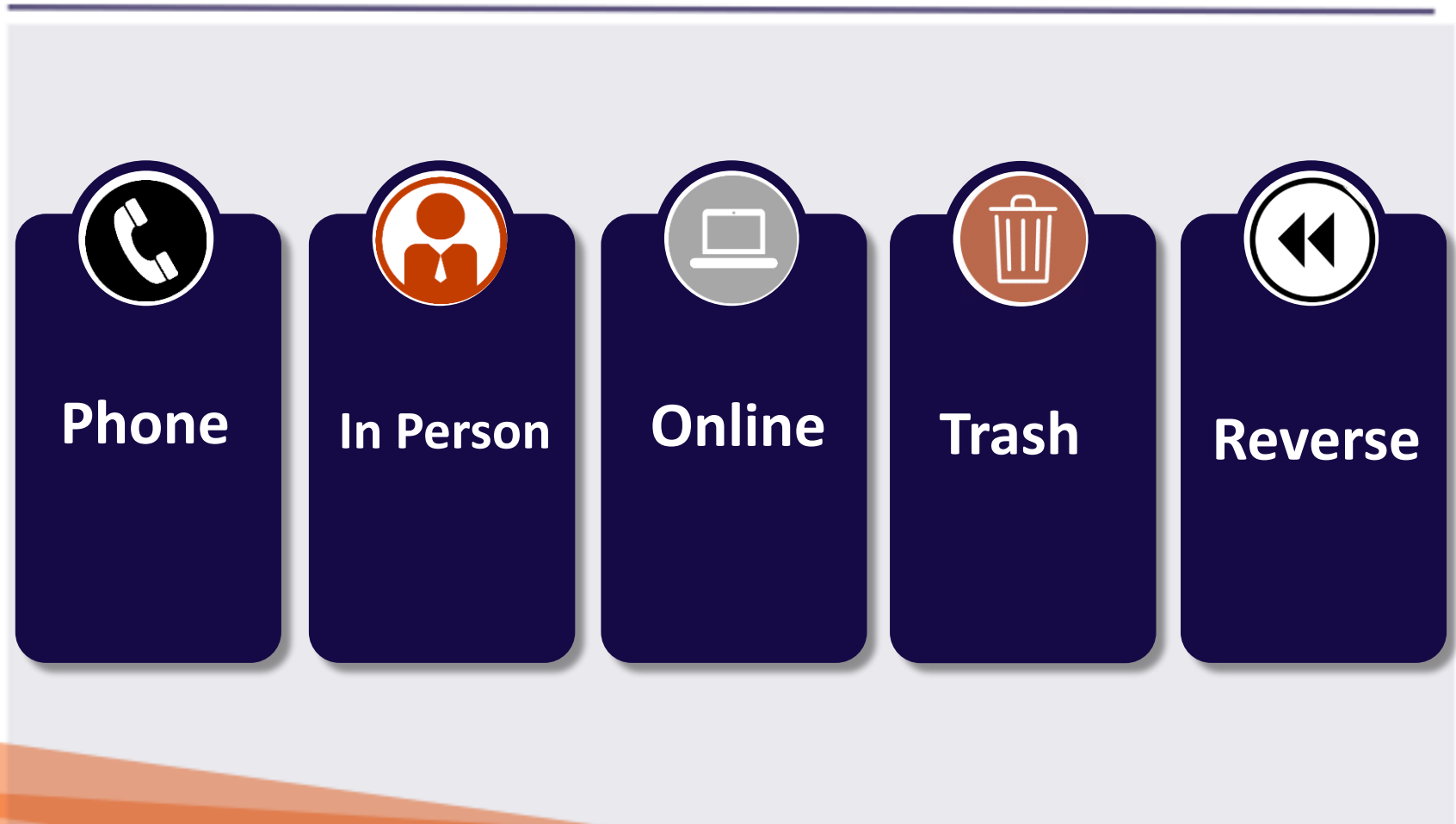
- Phishing emails



Social Engineering Channels

Don't fall in the trap

SE Channels



Phone

In Person

Online

Trash

Reverse

SE Channels

Phone

Why Do They Use It?

- Low risk, high reward
- Can be used from remote locations
- Easy to hide SE's true identity
- Hard to arrest "a voice"
- Universal target, everyone has a phone
- Easier to deceive people over phone than in person.



How is it Used?

- Find "weakest link" to gather intelligence.
- Gather various pieces of seemingly innocuous information.
- Establish a relationship to use in the future.

Target Examples

- **Front Line/Administrative**
- **Staff** Receptionist, shipping/receiving, etc.
- **Help Desk** Desire to help and resolve user problems may override the need for security.
- **Anyone with Information** Budget, Financial, Marketing, and Personnel Departments.

SE Channels

In person

Why Do They Use It?

- Social engineer physically enters premises and interacts with personnel.
- Manipulates to get information or further access.
- Yields information but at a high risk.
- Can lead to identification and possible arrest.
- Usually a last resort.



How is it Used?

Employed by highly skilled SE's

- Experts in use of psychological triggers as well as: Spying.
- Piggybacking
- Shoulder surfing
- Eavesdropping

Target Examples

Vulnerable building areas:

- Reception.
- Smoking area.
- Open office areas.

SE Channels

Online



Emails


- Phishing emails appear as legitimate requests
- Low-risk
- beyond legal bounds
- Can be distributed to Mass audience

Road Apples

- USB devices loaded with malware to capture information.
- Left in a location sure to be found (bathroom, elevator, sidewalk)
- Can appear to be legitimate corporate device or a vendor giveaway
- Once connected, a Trojan collects passwords, login's and machine-specific information emailing the findings back to the attacker

SE Channels

Online



DON'T GET HOOKED!

WHAT IS PHISHING?

Phishing is a psychological attack used by cyber criminals to trick you into giving up information or taking an action. Phishing originally described email attacks that would steal your online username and password. However, the term has evolved and now refers to almost any message-based attack. These attacks begin with a cyber criminal sending a message pretending to be from someone or something you know, such as a friend, your bank or a well-known store.

These messages then entice you into taking an action, such as clicking on a malicious link, opening an infected attachment, or responding to a scam. Cyber criminals craft these convincing-looking emails and send them to millions of people around the world. The criminals do not know who will fall victim, they simply know that the more emails they send out, the more people they will have the opportunity to hack. In addition, cyber criminals are not limited to just email but will use other methods, such as instant messaging or social media posts.

WHAT IS SPEAR PHISHING?

The concept is the same as phishing, except that instead of sending random emails to millions of potential victims, cyber attackers send targeted messages to a very few select individuals. With spear phishing, the cyber attackers research their intended targets, such as by reading the intended victims' LinkedIn or Facebook accounts or any messages they posted on public blogs or forums. Based on this research, the attackers then create a highly customized email that appears relevant to the intended targets. This way, the individuals are far more likely to fall victim.

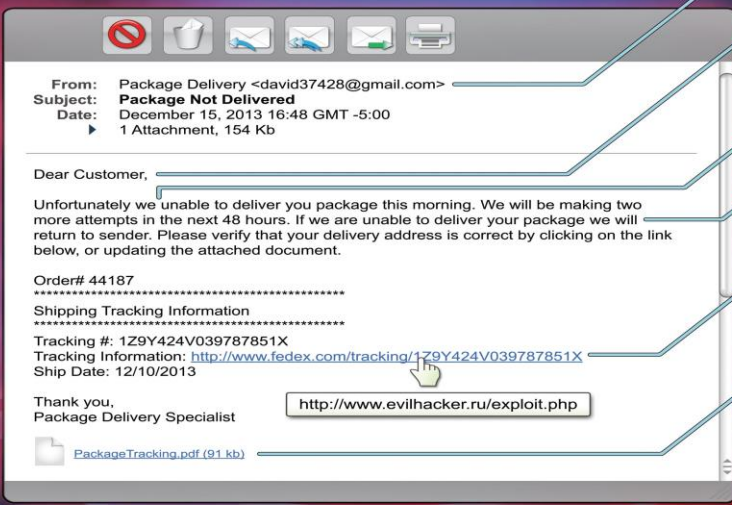
This poster was developed as a community project. Contributors include: Cheryl Conley (Lockheed Martin), Tim Harwood (BP), Tonia Dudley (Honeywell), Ellen Powers (MITRE Corporation), Shanah Johnson (Reserve Bank of Atlanta) and Terri Chihota.

WHY SHOULD I CARE?

You may not realize it, but you are a phishing target at work and at home. You and your devices are worth a tremendous amount of money to cyber criminals, and they will do anything they can to hack them. YOU are the most effective way to detect and stop phishing. If you identify an email you think is a phishing attack, or you are concerned you may have fallen victim, contact your help desk or security team immediately. To learn more about phishing or to demo the SANS Securing The Human Phishing testing platform, please visit <http://www.securingthehuman.org/phishing>.

PHISHING INDICATORS

- A** Check the email addresses. If the email appears to come from a legitimate organization, but the "FROM" address is someone's personal account, such as @gmail.com or @hotmail.com, this is most likely an attack. Also, check the "TO" and "CC" fields. Is the email being sent to people you do not know or do not work with?
- B** Be suspicious of emails addressed to "Dear Customer" or that use some other generic salutation. If a trusted organization has a need to contact you, they should know your name and information. Also ask yourself, am I expecting an email from this company?
- C** Be suspicious of grammar or spelling mistakes; most businesses proofread their messages carefully before sending them.
- D** Be suspicious of any email that requires "immediate action" or creates a sense of urgency. This is a common technique to rush people into making a mistake. Also, legitimate organizations will not ask you for your personal information.
- E** Be careful with links, and only click on those that you are expecting. Also, hover your mouse over the link. This shows you the true destination of where you would go if you clicked on it. If the true destination is different than what is shown in the email, this is an indication of an attack.
- F** Be suspicious of attachments. Only click on those you are expecting.
- G** Be suspicious of any message that sounds too good to be true. No, you did not just win the lottery.
- H** Just because you got an email from your friend does not mean they sent it. Your friend's computer may have been infected or their account may be compromised. If you get a suspicious email from a trusted friend or colleague, call them on the phone.



The screenshot shows an email from 'Package Delivery <david37428@gmail.com>' with subject 'Package Not Delivered'. It contains a shipping tracking link that, when hovered over, reveals the true destination: 'http://www.evilhacker.ru/exploit.php'. A red box highlights this link, and a red arrow points from indicator 'E' to it.

© SANS Institute - You are free to print, distribute and post as many copies of this poster as you like, the only limitation is you cannot modify or sell it. For digital copies of this and other security awareness posters, visit www.securingthehuman.org/resources/posters

SE Channels

Trash



Why Do They Use It?

- Organizations throw away sensitive information without shredding.
- Low level of protection –no one is guarding the dumpster.
- Less risky than in-person, but more than phone.
- No reasonable expectation of privacy.

What they can Find?

Trash dumpsters often contain valuable corporate and client information:

- Telephone lists.
- Organization charts.
- Account numbers.
- User IDs.

SE Channels

Reverse



Why Do They Use It?

- Attacker creates situation where victim requests help from the attacker.
- Hacker deletes user files, offers to assist user in recovery.
- Relies upon trust and sense of urgency.

What they can Find?

Pop-ups (Dialog boxes)

- Electronic messages offering help.
- Virus removal.



How to prevent form SE

SE Channels

Summary



- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about internal information.
- Do not provide personal information, information about the company (such as internal network) unless authority of person is verified.
- Before transmitting personal information over the internet, check the connection is secure and check the URL is correct.

SE Channels

Summary



- If unsure if an email message is legitimate, contact the person or company by another means to verify.
- Be paranoid and aware when interacting with anything that needs protection, The smallest information could compromise what you're protecting.
- User Awareness.



Summary

Summary

Lies VS. Truth

Lies

- Successfully conducting SE attacks requires great skill.
- Like malicious hacking, to succeed at SE, you need sophisticated tools (listening devices, micro cameras, etc.).
- Only foolish people are susceptible to SE attacks.



Truth

- Your biggest security threat and vulnerability is people.
- Not just people...maybe even you.
- Your users are vulnerable to social engineers.
- They may also be social engineers.

Summary

Summary

- ✓ Everyone has information -Everyone can be an SE target.
- ✓ Social engineer will choose lowest risk to get information from “weakest link”.
- ✓ Social engineer will use human weaknesses to get pieces of the puzzle.
- ✓ With aggregated information, a social engineer can accomplish their goal.



THANK YOU