Social Engineering

- Online
- Baiting
- persuasion
- Dumpster diving
- Vishing
- Shoulder surfing
- Many More

Objective

- The learning objective of this chapter is
  - Understanding the social engineering
  - Understanding the types of social engineering
  - Do’s and Don'ts

What is Social Engineering?

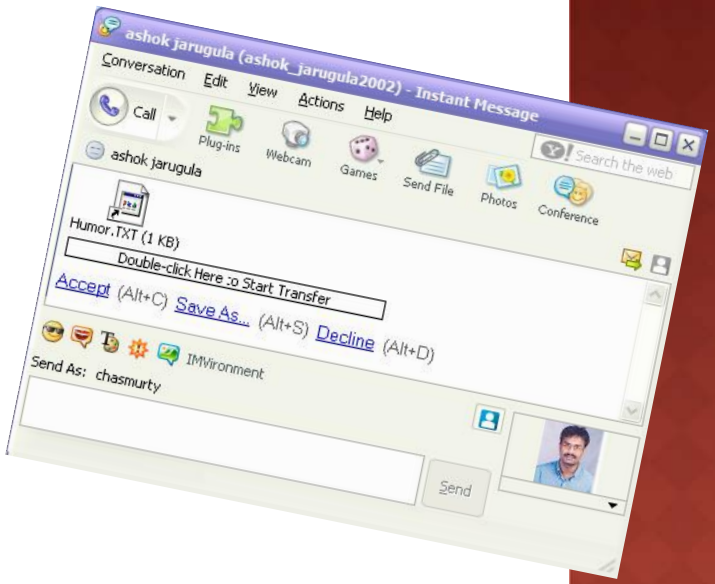
- Social Engineering is an approach or method used to gain access to information through misrepresentation or false identity by using various methods few are as follows
  - Careless talking is one of the reason for social engineering
  - Careless talking about business, the office, home, personal and the people and discussing with those who not authorized to talk.

Social Engineering Methods

- Instant messaging
- E-mails
- Websites
- Gossips
- Personal Pride or Confidence
- Online
- Baiting
- Persuasion
- Through Social Networking sites
- Through Whaling method
- Shoulder surfing
- Vishing
- Dumpster diving

Social Engineering Methods

- Instant messaging
- E-mails
- Websites
- Gossips
- Personal Pride or Confidence
- Online
- Baiting
- Persuasion
- Through Social Networking sites
- Through Whaling method
- Shoulder surfing
- Vishing
- Dumpster diving



Instant Messaging

- Social Engineering can be done through Instant messaging/Internet Relay Chat.
- Users are directed to sites that claim to offer help
- The sites may contain the malware like Trojan
- System may infect with the malware

Social Engineering Methods:

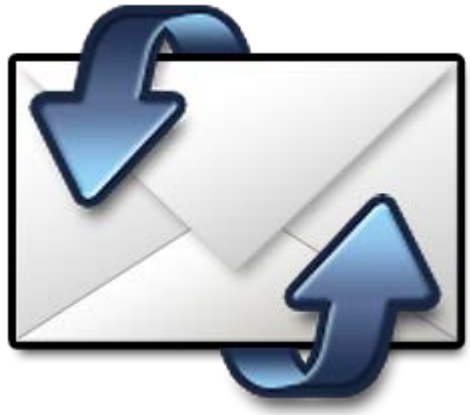
- Instant messaging
- E-mails
- Websites
- Gossips
- Personal Pride or Confidence
- Online
- Baiting
- Persuasion
- Through Social Networking sites
- Through Whaling method
- Shoulder surfing
- Vishing
- Dumpster diving

E-mails

- Social Engineering through e-mails like
  - Phishing e-mails
  - e-mail with attachments
  - e-mail scams
  - Fake e-mails

How???

- Social engineer sends an email to a person who appears to come from a legitimate site, such as
  - Online shopping
  - Banking site
  - New offers
  - Registration
  - Change of account password



Through e-mail attachments

- In email attachments there is a possibility of spreading viruses or cause damage to computer networks.
- These attachments may include malicious software such as viruses, worms and Trojan horses.

E-mail scams

- Email scams are becoming more prevalent
  - *One **recent example** claims that you have won a trip to the America and requests "basic information" from the user so that the prize can be awarded*

One of the example of e-mail Scam

This message has been replied to or forwarded.

From: [redacted]

To: [redacted].in

Cc: [redacted]

Subject: [redacted]

Dear All,

Blackberry is giving away free phones as part of their promotional drive.

All you need to do is send a copy of this email to 8 people; and you will receive your phone in less than 24 hrs.
Please note that if you send to more than 20 people you will receive two phones.
Please do not forget to send a copy to: amanda.lee@blackberry.com

With Regards,

Amanda Lee (Marketing Manager)
Office Number: 0117838512

One more example

New social engineering poll reveals which scam works better

Poll results from social-engineer.org finds most people think sweet talking victims is the best approach for criminal success

By Joan Goodchild, CSO
October 17, 2011 02:50 PM ET

Add a comment Print

Which tactic works best for a scamming social engineer? Acting like an authority figure and requiring a victim to answer questions and give up sensitive information? Or acting like a nice, trustworthy person who strikes up a friendly conversation and just needs the victim to tell them a few things to help them out?

That was the question asked by the team behind the web site social-engineer.org. They have just released results of a several-months long poll that laid out two different scenarios of how a social engineer might try and elicit information from a victim.

[Social engineering: The basics]

The first showed how the principle of endearment and how it may be used by a malicious social engineer. The example given was a social engineer who attempts to get strangers to engage in very personal conversation with him with little effort. Dressed very casually he grabbed a prop that he felt would endear people to him, a small sign that had a funny slogan

Fake Netflix Android app is social engineering scam

An application that looks like the legitimate Netflix app for Android is actually a text-book case of an information- stealing Trojan, according to Symantec

» 1 Comment

By Joan Goodchild, Senior Editor

October 13, 2011 — CSO —

Malware masquerading as a popular Netflix application for Android is actually a social engineering scam that utilizes a classic Trojan to get account information and passwords.

Symantec warned about the malware in a blog post this week, noting it is a clear example of how far mobile malware has come.

[Social engineering: 3 mobile malware techhiques]

The Android.Fakeneflic exploit, according to Symantec's Irfan Asrar, "is a text book case of an information stealing Trojan that targets account information. The malicious app is not too difficult to understand. Despite the fact that there are multiple permissions being requested at the time of installation — identical to the permissions required by the actual app — our analysis shows that this is, in fact, a red herring, probably used to add to the illusion that the end user is dealing with the genuine article."

Social Engineering Methods

- Instant messaging
- E-mails
- Websites
- Gossips
- Personal Pride or Confidence
- Online
- Baiting
- Persuasion
- Through Social Networking sites
- Through Whaling method
- Shoulder surfing
- Vishing
- Dumpster diving

Websites

- A common play is to offer something free or a chance to win a sweepstakes on a Website
- To win the user must enter an email address and a password
- Many employees will enter the same password that they use at work
  - so the through such methods Social Engineer now has a valid user name and password to enter an organization's network.

Hackers tried to bluff RSA customers

By Tom Espiner, 12 October, 2011 17:32

Hackers attempted to get into RSA customers' systems following a breach of RSA SecurID data in March.

The hackers attempted to fool staff of companies that use RSA products in targeted attacks which used the original attack on RSA as bait, RSA president Tom Heiser said on Tuesday. Heiser did not say whether the original hacking group was responsible for the later attempts.

"We did see attempted social engineering attacks against our customers using the RSA attack as a pretext," said Heiser.

Following the RSA attack, many customers felt that RSA was not sharing enough information about the nature of the attack, said Heiser. The reticence was due to an investigation that was being undertaken by the FBI and other law enforcement, Heiser added.

"Many stakeholders felt we could have done more, and we should have done more to let them know. To those customers we inconvenienced, we truly apologise," said Heiser. "I'm often asked why we didn't share more information, and share information sooner. Well... our adversaries were stealthy, but they did leave some information behind that could be used in an ongoing

Social Engineering Methods

- Instant messaging
- E-mails
- Websites
- Gossips
- Personal Pride or Confidence
- Online
- Baiting
- Persuasion
- Through Social Networking sites
- Through Whaling method
- Shoulder surfing
- Vishing
- Dumpster diving

Gossips & Personal Pride or Confidence

- **Gossips**
  - You may talk about some gossip with colleague and may give some information to other colleague who might be a social engineer.
- **Personal Pride or Confidence**
  - you may give sensitive information of your family or organization to boast your achievements, pride, and confidence to unknown persons

Social Engineering Methods

- Instant messaging
- E-mails
- Websites
- Gossips
- Personal Pride or Confidence
- Online
- Baiting
- Persuasion
- Through Social Networking sites
- Through Whaling method
- Shoulder surfing
- Vishing
- Dumpster diving

Online

- Social engineers may obtain information online by pretending to be the Network Administrator
- Sending an e-mail through the network and asking for a user's password or any sensitive information indirectly

Social Engineering Methods

- Instant messaging
- E-mails
- Websites
- Gossips
- Personal Pride or Confidence
- Online
- Baiting
- Persuasion
- Through Social Networking sites
- Through Whaling method
- Shoulder surfing
- Vishing
- Dumpster diving

Baiting

- It is one of the methods of social engineering which uses physical media and relies on the curiosity or greed of the victim

Social Engineering Methods

- Instant messaging
- E-mails
- Websites
- Gossips
- Personal Pride or Confidence
- Online
- Baiting
- Persuasion
- Through Social Networking sites
- Through Whaling method
- Shoulder surfing
- Vishing
- Dumpster diving
-

Persuasion

- Influence someone to give you confidential information either by convincing them you are someone who can be trusted or by just asking for it.

Social Engineering Methods

- Instant messaging
- E-mails
- Websites
- Gossips
- Personal Pride or Confidence
- Online
- Baiting
- Persuasion
- Through Social Networking sites
- Through Whaling method
- Shoulder surfing
- Vishing
- Dumpster diving

Through Facebook

- Social networking sites such as Facebook are a social engineer's paradise
  - A social engineer can find out so much about you from these sites
  - People post information about where they work, what they like to do, what bands they like, and many more

Social Engineering Methods:

- Instant messaging
- E-mails
- Websites
- Gossips
- Personal Pride or Confidence
- Online
- Baiting
- Persuasion
- Through Social Networking sites
- Through Whaling method
- Shoulder surfing
- Vishing
- Dumpster diving

Whaling

- Social Engineering to acquire the details of individual
- Targeting the **individual user** or **higher authority**
  - Another variation of phishing attacks is a ***whaling attack*** which would be used by social engineer.
- Whaling is an attack which targets the specific high profile executives in the businesses or targeting upper management in the corporate
  - In this type of attack the social engineer targets executives and high-profile and targets the complete information about them which is easily accessible on the Internet.

Social Engineering Methods

- Instant messaging
- E-mails
- Websites
- Gossips
- Personal Pride or Confidence
- Online
- Baiting
- Persuasion
- Through Social Networking sites
- Through Whaling method
- Shoulder surfing
- Vishing
- Dumpster diving

Shoulder Surfing

- Shoulder surfing
  - Simply looking over someone's shoulder while they are using a computer.
  - This can be done in close range as well as long range using a pair of binoculars.

Social Engineering Methods

- Instant messaging
- E-mails
- Websites
- Gossips
- Personal Pride or Confidence
- Online
- Baiting
- Persuasion
- Through Social Networking sites
- Through Whaling method
- Shoulder surfing
- Vishing
- Dumpster diving

Vishing

- Vishing is an methods similar to phishing but done through voice i.e over telephone

Social Engineering Methods

- Instant messaging
- E-mails
- Websites
- Gossips
- Personal Pride or Confidence
- Online
- Baiting
- Persuasion
- Through Social Networking sites
- Through Whaling method
- Shoulder surfing
- Vishing
- Dumpster diving

Dumpster Diving

- It is an method where the attacker gets the information from the trash

Do's

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information
- If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company

Do's

- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly
- Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic
- Take advantage of any anti-phishing features offered by your email client and web browser
- Be suspicious don't get influenced by the unknown person and don't give away the confidential information to them

Don'ts

- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in e-mail
- Don't send sensitive information over the Internet before checking a website's security. Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net)

Don'ts

- Don’t get tempted in accessing the devices which left unattended or found at sidewalk, elevator, parking lot etc.
- Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information

What do you do if you think you are a victim?

- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity
- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account
- Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future
- Watch for other signs of identity theft
- Consider reporting the attack to the police, and file a report with the Federal Trade Commission

Always be alert and check out before posting or giving information

References

- http://www.pcworld.com/article/182180/top_5_social_engineering_exploit_techniques.html
- http://en.wikipedia.org/wiki/Voice_phishing
- http://www.informit.com/articles/article.aspx?p=1350956&seqNum=7