Social Engineering

Session overview

- **Social engineering**
- **Vishing**
- **Phishing**
- **Smishing**
- **Best practices**

Social engineering

Concept –

- Many technological defenses out there
- Sometimes bypassing them becomes hard
- Better option: Let the victim help us attack him
- Question: **Why should he do it?**

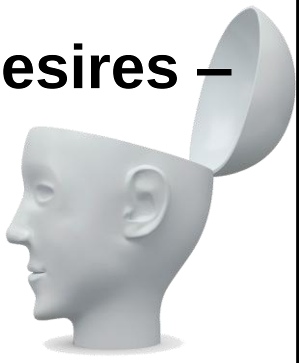
Social engineering

Human psychology –

- We may think we are sophisticated
- We all have our basic desires and fears
- These could be used to manipulate us
- Each has his own “soft spot”

Social engineering

Human psychology – Common desires –



- Being helpful
- Being appreciated
- Feeling like we fit in
- Feeling smart
- Finding great deals
- Finding a suitable mate

Social engineering

Human psychology – Common fears –

- Losing money
- Having our private data stolen
- Fear of technology
- Fear of our boss
- Fear of breaking the law
- Fear for our loved ones

Social engineering

Human psychology – Common Tactics –

- Urgency (Makes us act first and think later)
- Fake facts (Add fake invoice number)
- Raise curiosity (Clickbaits)
- Impersonation (or hacking account of familiar)
- Feelings (Jealousy, fear, hope)
- Blend in with regular content (Lack of attention)

Social engineering

How to make money from SE –

- Obtain victim’s credentials
  - Bank account / credit card information
  - Steal sensitive information and then sell / extort
  - Use account (Netflix, long distance calls)
  - Sell credentials online
- Install profitable malware (Ads, crypto-miners, affiliate)
- Cause victim to send us money directly

Social engineering

Social engineering techniques –

- Various techniques exist
- They share basic concepts
- Difference: method of delivery to target
- Main techniques:
  - Vishing
  - Phishing
  - Smishing

Vishing

Vishing overview –

- Aka Voice phishing
- Social engineering via telephone voice calls
- Benefits:
  - More trusted by victims than phising emails
  - People place trust in caller ID (can be spoofed)
  - Can be automated to scale up
  - Targeted attack: Obtain target’s personal details

Vishing

Vishing examples –

- Automatic credit card blocking alert
- IRS due tax alert
- Microsoft remote support detected malware
- Helpdesk maintenance needs credentials
- Refrigerator warranty about to expire
- Combo attack:
  - #1: ISP needs to verify credit card details
  - #2: Bank calls, and warns about ISP vishing attack

Phishing

Phishing overview –

- Comes from Fishing
- Sub category of the Social engineering world
- Concept: Use bait to convince victim to provide personal information
- Usually sent by Email
- Email contains link to fake site that looks valid

Phishing

Phishing – Common steps –

- The process usually consists of:
  - Creating phishing website
    - Clone existing real page
    - Create new page impersonating known entity
  - Give that site reliable looking address
    - Or use shortening service such as bit.ly
  - Start sending fake emails linking to that site

Phishing

Phishing – Common steps –

- Give that site reliable looking address:

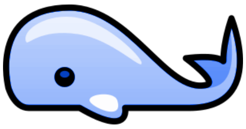
<u>Famous examples:</u>

• **Real:**	**www.steamcommunity.com**
• **Phishing:**	**www.steamcornmunity.com**
• **Real:**	**www.ray-ban.com/israel**
• **Phishing:**	**www.rayban-israel.com**

Phishing

Phishing – Common steps –

- Send fake emails linking to your site
- There are several types of phishing emails:
  - Regular mass phishing attempts
  - Spear Phishing (dox and target specific victims)
    - Raises click chance from ~5% to ~50%
  - Whaling – attacking high profile targets



Phishing

Phishing –

- Common Bait types:
  - Bank warning notice
  - FBI notice of illegal activity on our machine
  - Alert that Credit cards number were stolen
  - Facebook notice about problems with account
  - Congratulations! You’ve won 1M$ in lottery
  - You are entitled to inheritance money

Phishing

Attackers Enhancing efficiency –

- **Base their Emails on real mails from the original site**
- Use fake sender Emails address
  - Several techniques for that
- Make their link look real
  - Easy: Show one address point to another
  - Harder: Use redirect attacks on real site
- Harvest possible victim Email addresses
  - Even using Google dorks

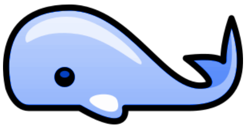
Phishing

Attackers Enhancing efficiency – Spear phishing –

- They target a specific victim
- Increase click probability by:
  - Gathering personal information
  - Incorporating that into the Email
- That could be:
  - Services he registered to
  - Family members details
  - Schools, workplaces, people..

Phishing

Attackers Enhancing efficiency – Whaling –



- Directed at high profile targets
  - Very high value target
  - Usually looks like urgent business email
  - Contains legal warning, customer complaint or financial issue

- Impersonation of company executives (such as CEO)
  - Aka BEC (business email compromise scam)
  - Try to convince employee to transfer funds / sensitive info
  - Accounted for more than $5B in losses between 2013-2016

Phishing

Phishing to install malware –

- Phishing campaigns also used to install malware

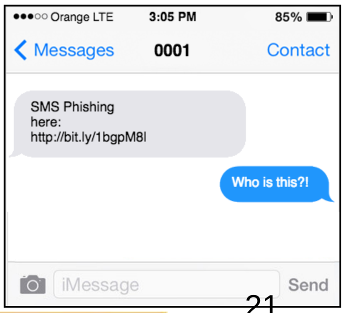
- Common techniques:
  - Rouge AV / computer performance booster
  - Missing Codec to run video
  - Media/Flash player update
  - Install PDF viewer application to open required file
  - Missing fonts update
  - OS update

Phishing

Attackers luring to the phishing site –

- Victim won’t arrive by doing a Google search
  - Nor by typing-in the URL himself

- Common methods:
  - Phishing Email / SMS / social media message
  - Watering hole attack
  - Link in social media (Friend/group post)
  - Online posts in forums
  - Malicious ads (Targeted for our victim)



SMS Phishing here: http://bit.ly/1bgpM8l

Who is this?!

Phishing

Watering hole attack –

- Analyze target behavior
- Choose a web site he frequents
- Insert malware to that website
- When he enters the site he gets infected!
- Very popular (Over 30k sites hijacked daily)

Phishing

Luring to the phishing site using Social media –

- Attackers port link in social media site

- Make sure victim sees the link by:
  - Posting on his wall
  - Tag him in a post
  - Comment on a post he made
  - Post in a group he has joined
  - Create a fake account duplicating one of his friends
  - Post from hacked account of someone he knows

Phishing

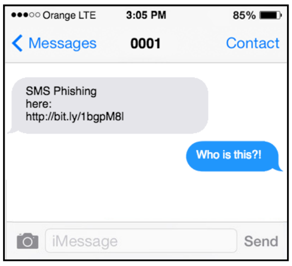
Luring to the phishing site – Malicious Ads –

- Aka: Malvertising
- Attacker paying to put ad on popular sites
  - Regular ad at first
  - After a while change code to infect
  - After successful infection return to regular innocent ad
- User gets infected by:
  - Clicking our ad
  - Drive-by attack
  - Automatic redirect to our website

Smishing

Luring to the phishing site – SMS –

- Sending SMS to a Victim's phone
- The SMS contains a link to attackers site
- Using social engineering techniques to cause a click
  - Topic is related to victim
  - Seems to be from someone he knows
  - Topic is of personal interest to the victim
  - Content is intriguing and irresistible



SMS Phishing here: http://bit.ly/1bgpM8l

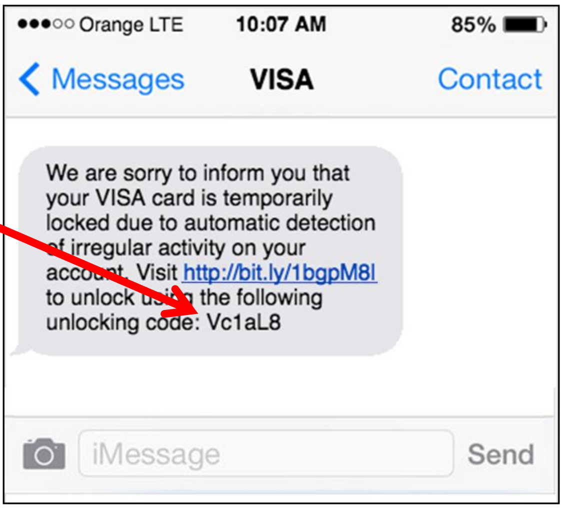
Who is this?!

Smishing

Luring to the phishing site – SMS –

- Adding artifacts
  - Transaction ID
  - Personal code
  - Target's Name or details

- This adds credibility to the message



We are sorry to inform you that your VISA card is temporarily locked due to automatic detection of irregular activity on your account. Visit http://bit.ly/1bgpM8l to unlock using the following unlocking code: Vc1aL8

Best Practices

Best practices to stay safe –

- Who
  - Persona & Name
  - Actual sender address
- What
  - Legitimate content
  - Attachment
  - Phishing techniques (Urgency, sending private info)
- Where
  - Links actual destination

For Questions:
yoav@practis.co.il