



# So you're interested in social engineering?

The very first steps



@k@chaos.social

<https://kirils.org> for more

Mg.sc.comp. Mg.phys. Kirils Solovjovs

Possible Security, ICS



# Contents

- Introduction to social engineering
- Using OSINT to collect initial information
- Creating pretext
- Fundamental principles of human behavior and decision-making
- Leveraging social normativity in persuasive interactions
- Building rapport and trust
- Exploiting trust
- Practical exercises in everyday life

# Social Engineering (SE)

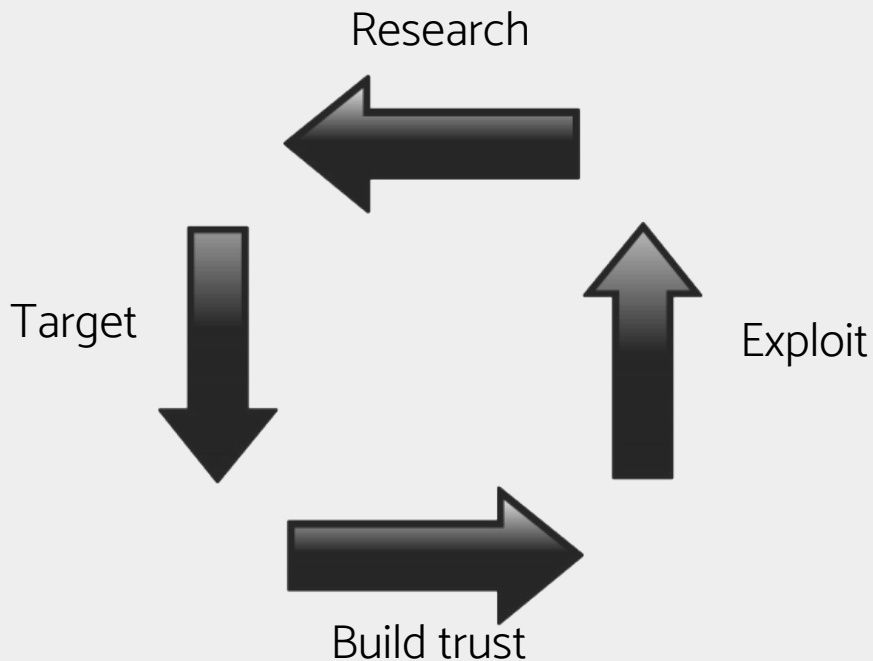


is the use of deception to manipulate individuals into divulging sensitive information that may be used for illegitimate or fraudulent purposes or to further attacks on a larger entity



# SE attack cycle for organisations

- Research
- Target
- Build trust
- Exploit





# SE attack types (in person)

- Impersonation
  - VIP, user, tech
  - appeal to authority
  - reverse social engineering
  - identity theft
- Access
  - tailgating; piggybacking
  - key duplication
- Acquisition
  - eavesdropping
  - shoulder-surfing
  - dumpster-diving



# SE attack types (remote)

- Types
  - phishing, spearphishing
  - vishing
  - app impersonation
  - ...
- Delivery vehicles
  - e-mails
  - phone calls
  - usb drops
  - instant messages, sms
  - social networks
  - traffic injection
  - malware, adware



# Components of a Social Engineer

- Confident
  - „Conman” → Confidence man
- Quick-witted
  - can be partially substituted by A LOT of prep
- Determined
  - „All you have to do is ask” principle

Es pastiepos un dabūju  
Visu kā pēc listes  
Tas mani apbūra  
Vecīt, kaut kas mistisks  
Vienkārši izliekot akcentus uz to, kas svarīgs  
Biku pacenties, skaties un dabū arī

— *There Is Something To It by Brainstorm*

# OSINT



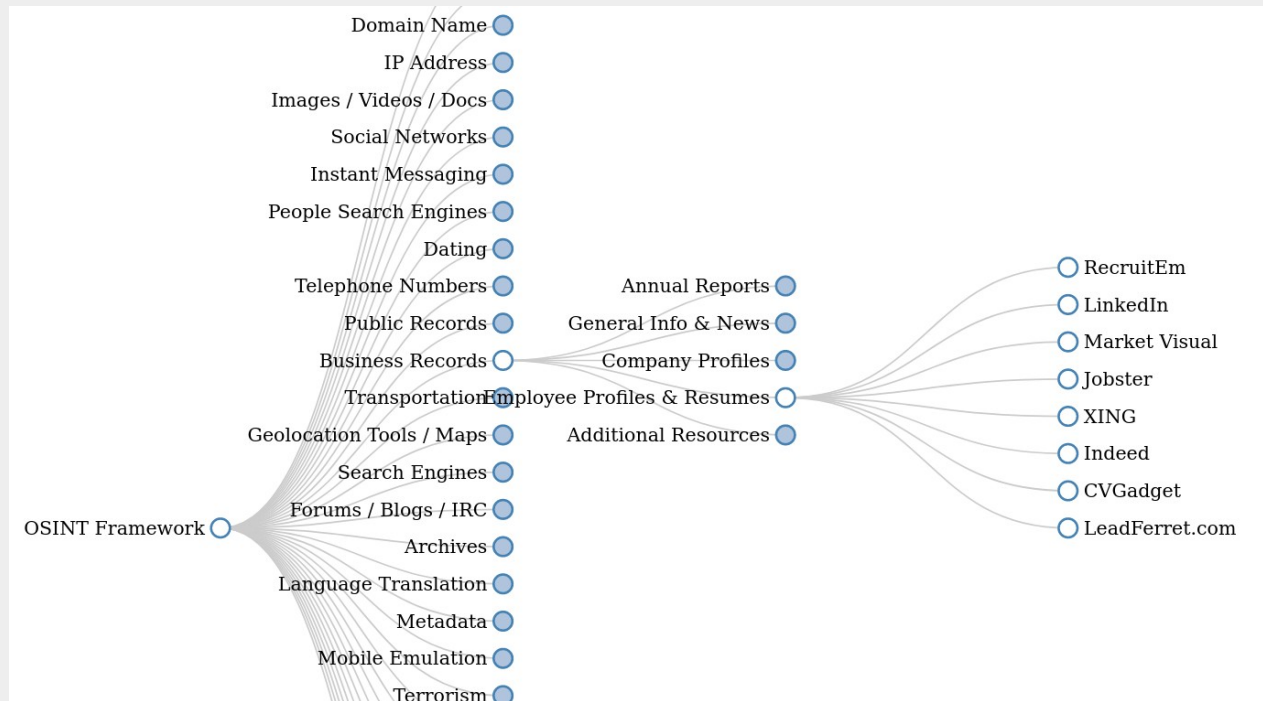
- Open Source intelligence is intelligence collection from openly available sources





# OSINT sources include

- Web & darknet
- Social networks
- Metadata
- Network & service scans
- Fingerprinting
- OSINT “framework”
  - <https://osintframework.com/>





# OSINT: Web

- Google “dorks”
  - filetype:pdf ”COMMERCIAL PROPRIETARY”
  - (google does OCR for you!)
- filetype:sql ”INSERT INTO”
  - SQL dumps
- site:lv ”index of /backup”
  - Public backups
- intitle:r57shell -inurl:r57shell filetype:php
  - Backdoored servers
- cache:example.com
  - Copy of inaccessible webpage



# OSINT: Web

- [pastebin.com](https://pastebin.com)
- online comments on news sites
- Yandex maps, Google Streetview
- webcams
- [web.archive.org](https://web.archive.org)
- [tineye.com](https://tineye.com)
- [blockchain.info](https://blockchain.info)
- [shodan.io](https://shodan.io)
- leaks



# OSINT: Web

- People search engines
  - Honorary mention: sync.me
  - Alternative: google dork
- Public registries
- Online news, etc.
- <https://www.toddington.com/resources/>



# Social networks

- Facebook
  - Twitter/X
  - Instagram
  - Mastodon
  - Tumblr
- 
- Account recovery process sometimes gives info



# OSINT: Social network tools

- <https://inteltechniques.com/tools/index.html>
  - Very valuable OSINT tools, especially for social networks



# Pretext

- What's your role? Who do you wanna play today? :)
  - don't make it too crazy
    - Hello, this is Napoleon Bonaparte and I'm calling you because your password has expired
- Why are you doing this?
  - make sure your role matches your goal
- You have to convince yourself first!
  - challenge yourself
  - look for holes in your story

# Human behavior and decision-making



- Everyone **loves to help**
  - except the hard targets
    - guards
    - people trained to work with external customers
- People generally try to **avoid conflict**
- Some people make consistently good decisions
- Most people make good decision on best-effort basis
- A rare person makes good decision when **rushed**



# Leveraging social normativity in persuasive interactions



- Tailgating with hands full
- Waiting for a „good hair day” and then asking for a favour
- Hint at creating conflict and provide an easy way to avoid it
  - Can't be above the pay grade of whomever you are targeting



# Building rapport and trust

- See my 2017 presentation on lobbying from OpenFest  
<https://kirils.org/sh841>



# Exploiting trust

- Always keep the goal for this interaction in your mind!
- Don't ask for too much at the same time!



# Practical exercises in everyday life



# Non-SE exercises

- talking to people
- improv
- alternative personas
- pretend to be someone else (with a story!) online
- do it with your friends first



# Start with passive acquisition methods

- Dig for some trash
- Eavesdrop on nearby employees
- Shoulder-surf
- Bump into people
  - in a way that is conducive to tag copying & natural
  - at the same time!



# Build some pre-text



# Be uncooperative where you can

- hide your wristband
  - try to talk your way out of it
- smile, be friendly and agreeable
- be vague in your responses
- be dumb





# Continue with simple everyday things



# What NOT to do

- Do not try to „leave with stuff without paying”
- Do not provide a fake identity to government agencies
- Do not damage other’s property
- If you do SE that could result in you getting some financial benefit, make sure that you’ve paid for it as well



# Q&A

Slides are available on <https://kirils.org>

Find me on @k@chaos.social