Ethical Hacking: Hacking Mobile Platforms

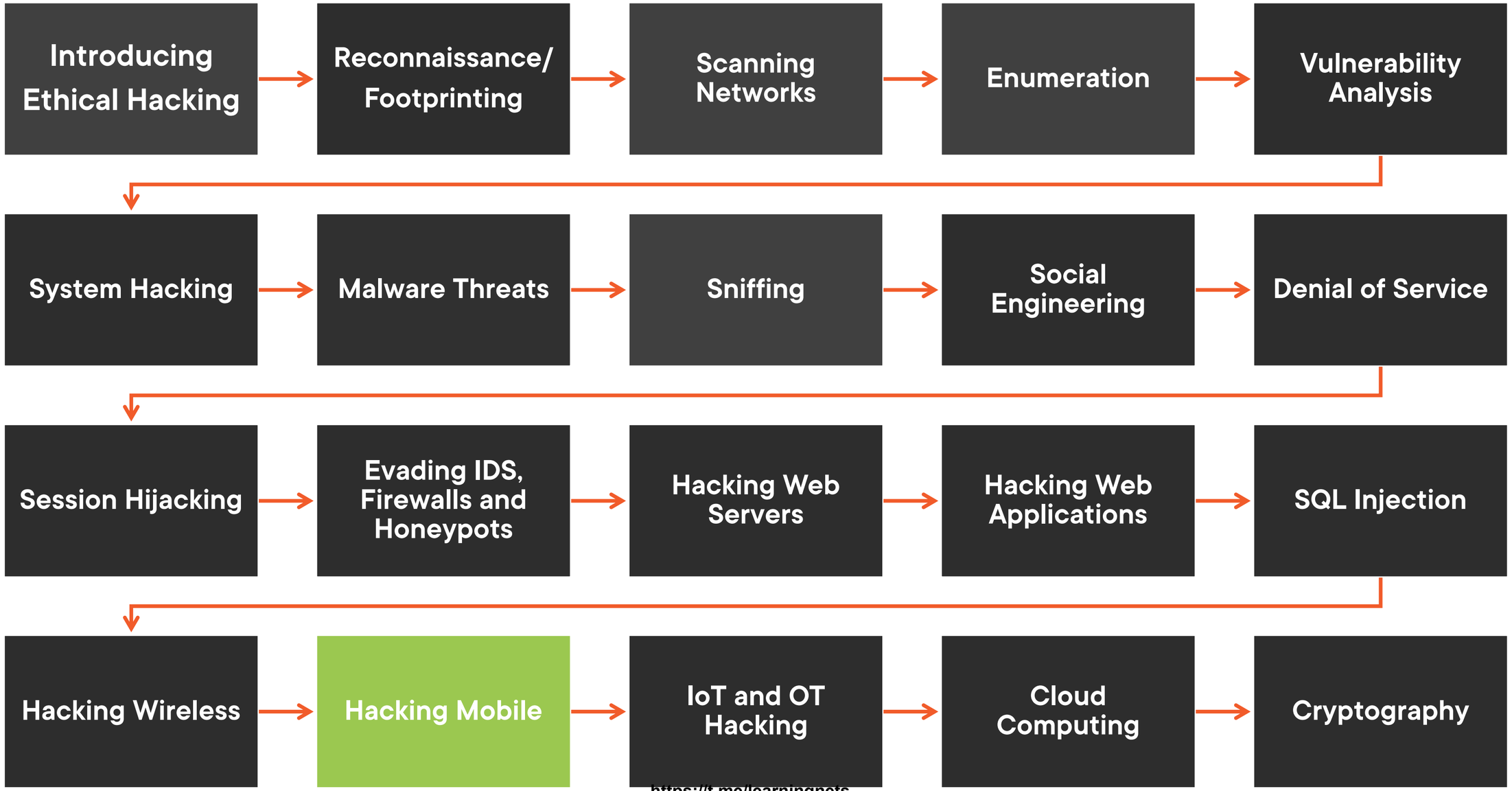
Discovering Mobile Platform Attack Vectors

Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith

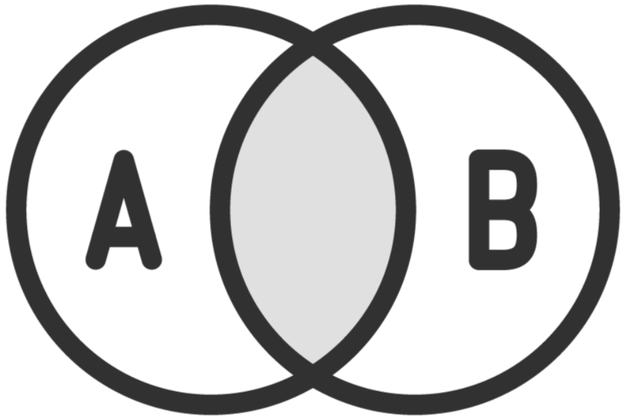
https://t.me/learningnets

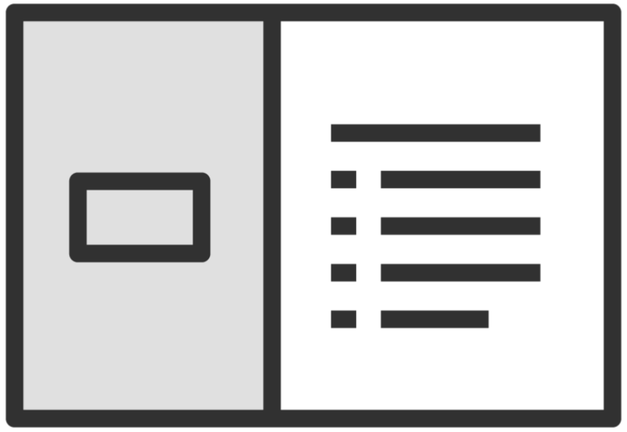
Ethical Hacking Series



https://t.me/learninghets

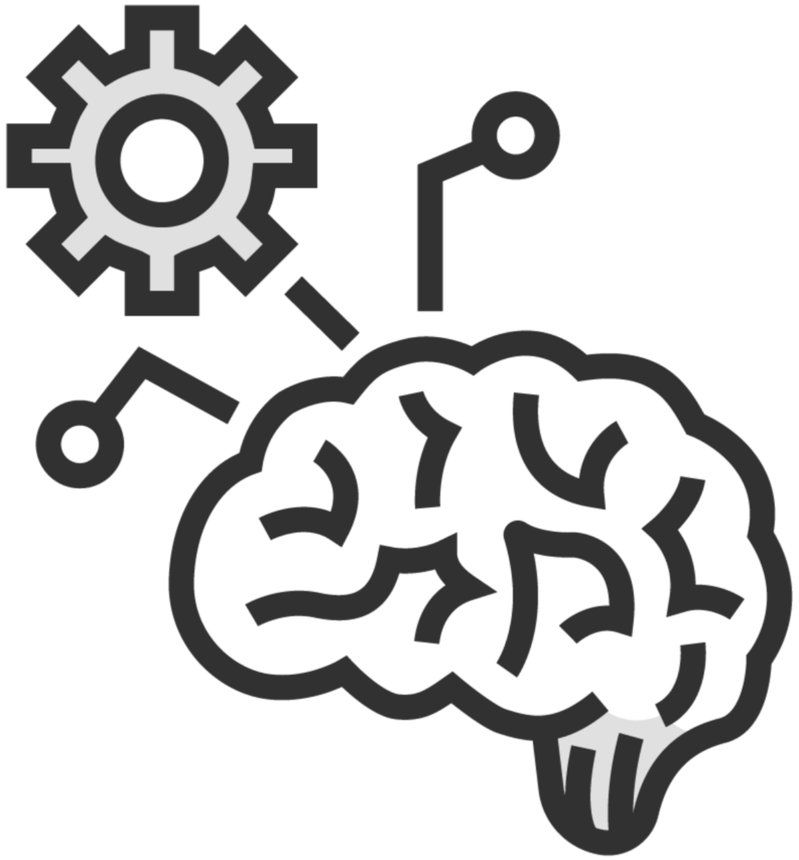
The Method behind My Madness





https://t.me/learningnets

The Method behind My Madness



https://t.me/learningnets

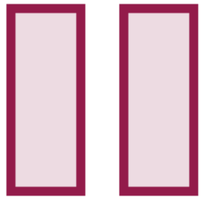
CEH Exam Study Tips

https://t.me/learningnets

Dale's Study Tips

Study space

Take notes

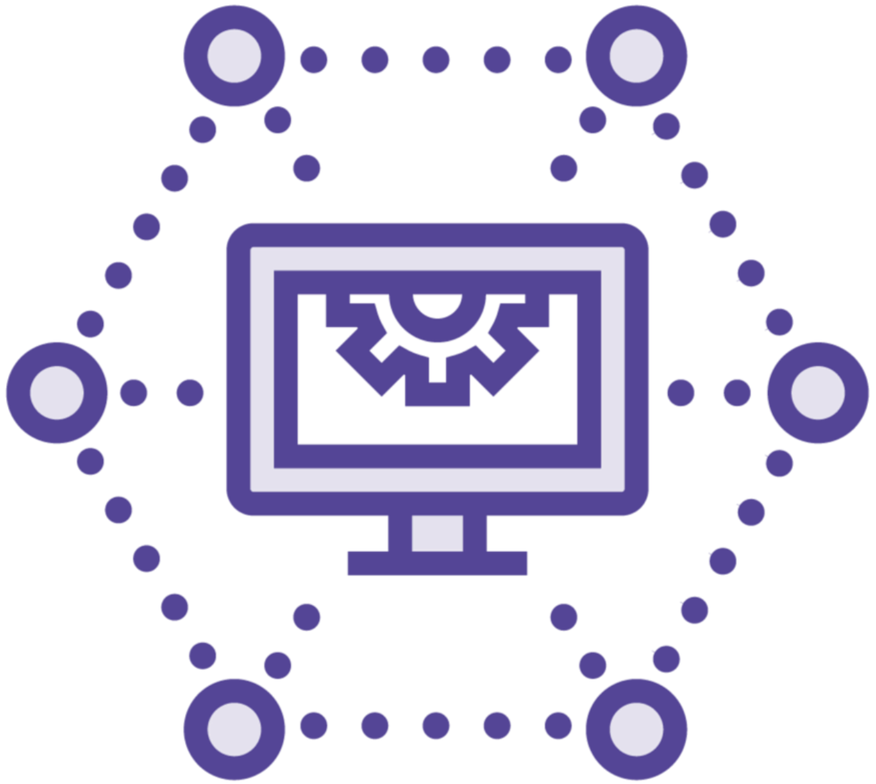


Pause, think, repeat

Be kind and rewind

https://t.me/learningnets

Dale's Study Tips



https://t.me/learningnets

https://t.me/learningnets

“Size matters not. Look at me. Judge me by my size, do you?”

Master Yoda

https://t.me/learningnets

Top 10 Risks for Mobile Devices

https://t.me/learningnets

OWASP

Open Web Application Security Project

https://t.me/learningnets

Top 10 Risks

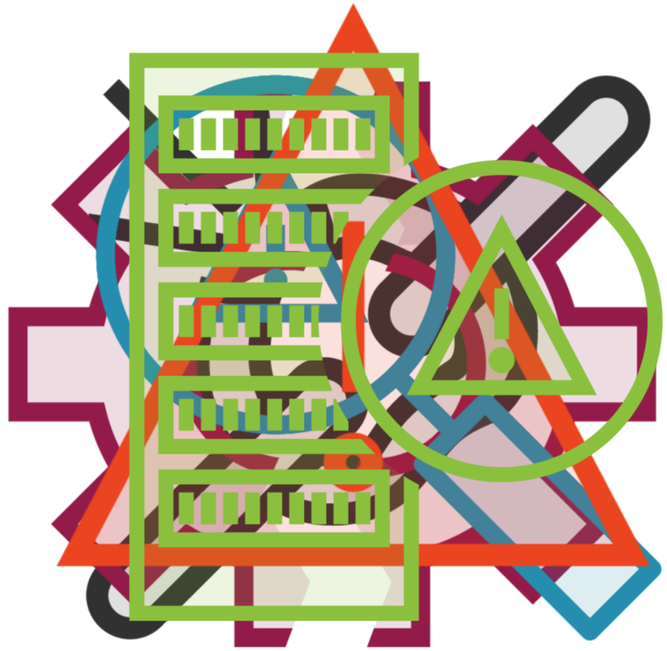
Improper platform usage

Insecure data storage

Insecure communications

Insecure authentication

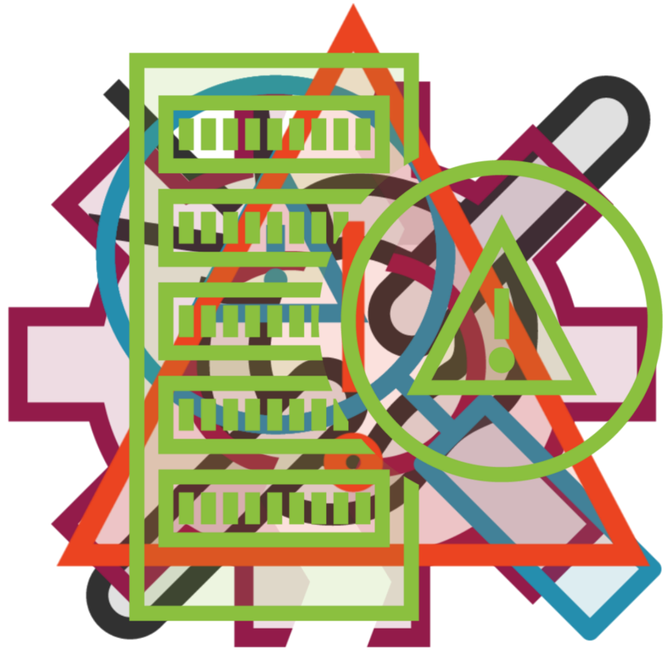
Insufficient cryptography



https://t.me/learningnets

Top 10 Risks

- Insecure authorization
- Client code quality
- Code tampering
- Reverse engineering
- Extraneous functionality



https://t.me/learningnets

Anatomy of Attacking Mobile

https://t.me/learningnets

Bring Your Own Device (BYOD)

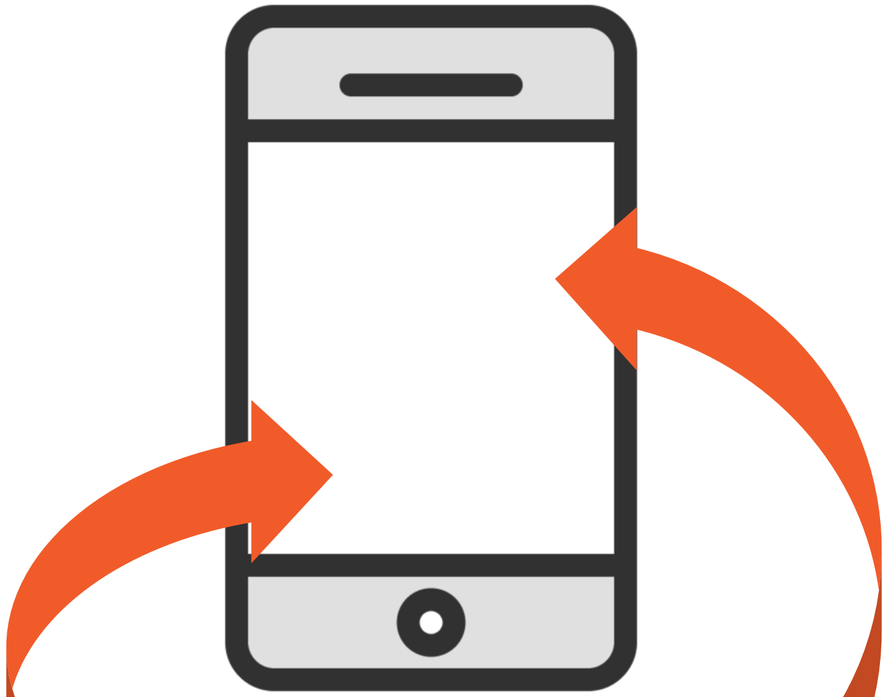
Mobile devices are a major target for attacks

https://t.me/learningnets

Mobile Attacks

- Phishing
- Clickjacking
- Buffer overflow
- Man-in-The-Mobile (MiTM)

https://t.me/learningnets



SMiShing

Baseband attack

https://t.me/learningnets

https://t.me/learningnets

Weak passcodes

Jailbreaking

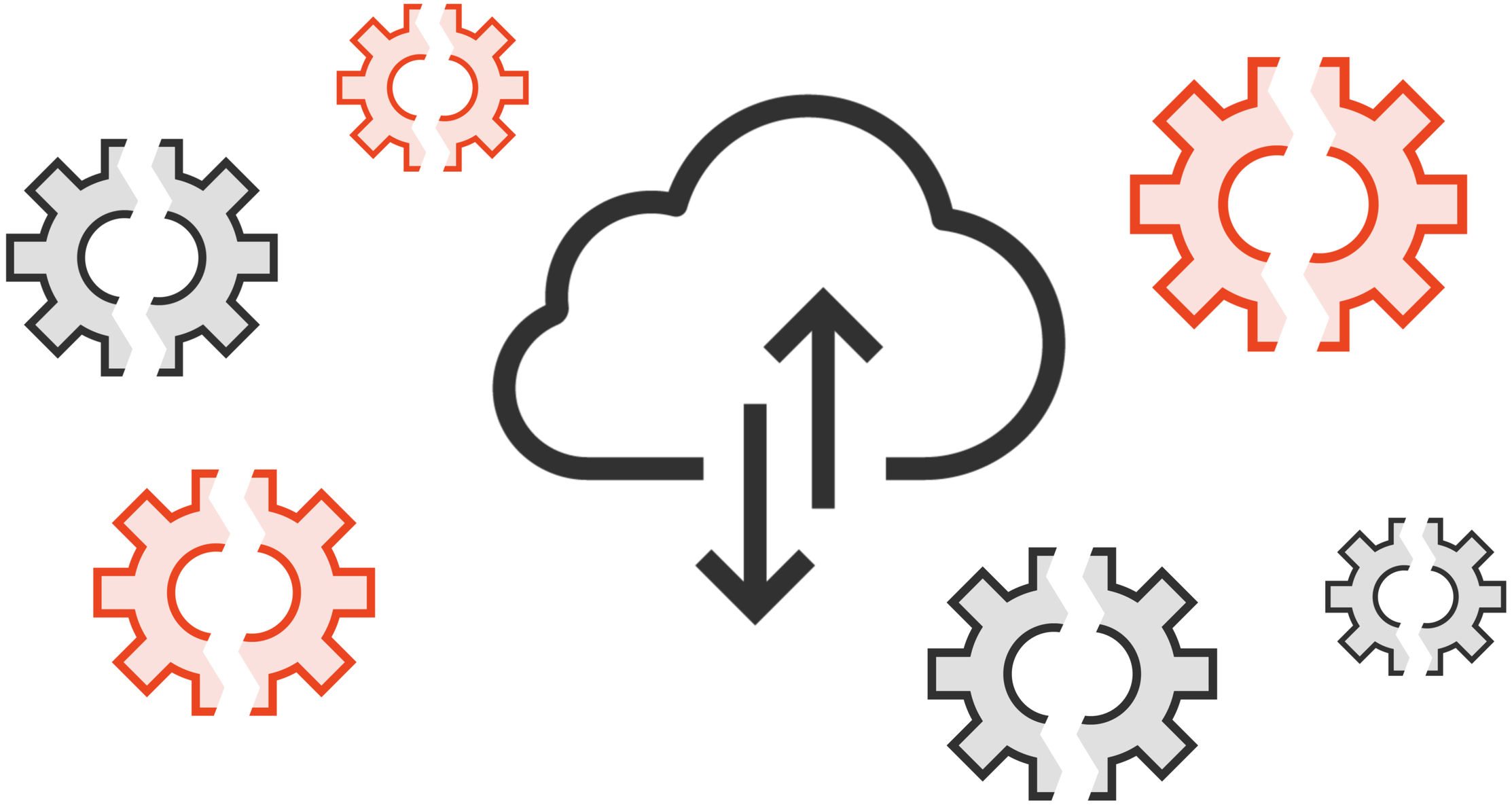
Cached data

Rooting

Preinstalled software

https://t.me/learningnets

https://t.me/learningnets



https://t.me/learningnets

Attack Vectors and Vulnerabilities

https://t.me/learningnets

Mobile Vulnerabilities

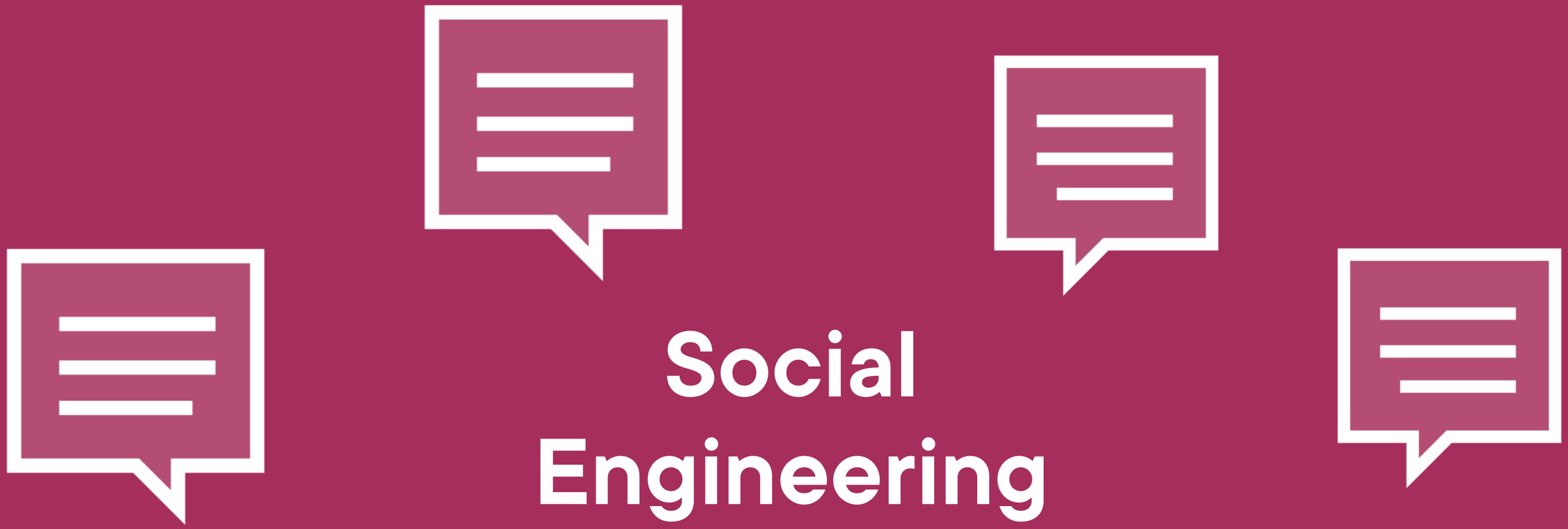
- Malware
- Data Exfiltration
- Data tampering

https://t.me/learningnets

Mobile Vulnerabilities

- **Apps and app stores**
- **Viruses, worms, and rootkits**
- **Data storage**
- **Copying information**
- **Social engineering**

https://t.me/learningnets



Social Engineering

https://t.me/learningnets

Mobile Vulnerabilities

- **SMS environment**
- **Drive-by**
- **Out dated operation systems**
- **Phishing**
- **Connections**

https://t.me/learningnets

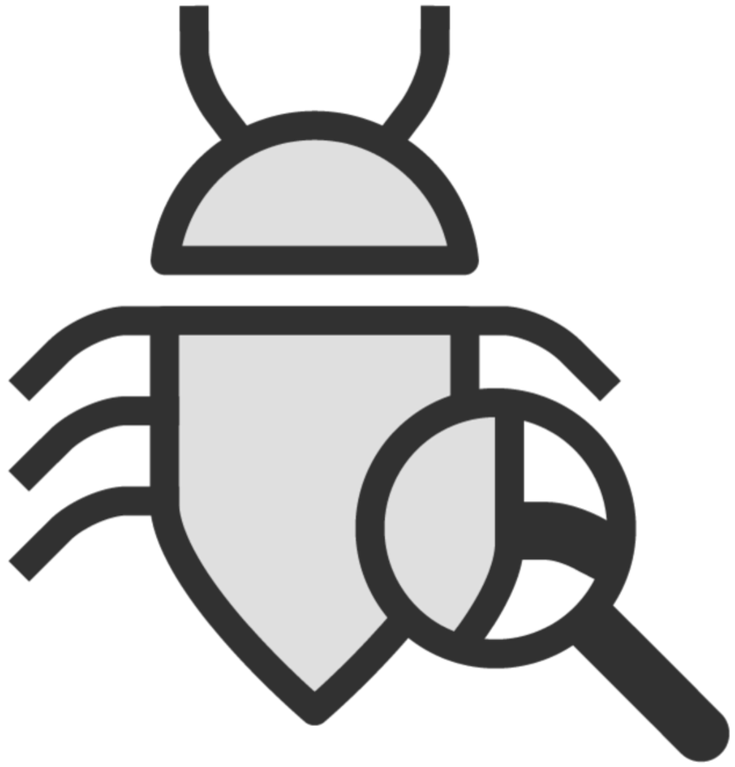
Sandboxing

A method of restricting an app's access to certain resources in order to secure computers and users.

https://t.me/learningnets

Agent Smith, SS7 and Simjacking

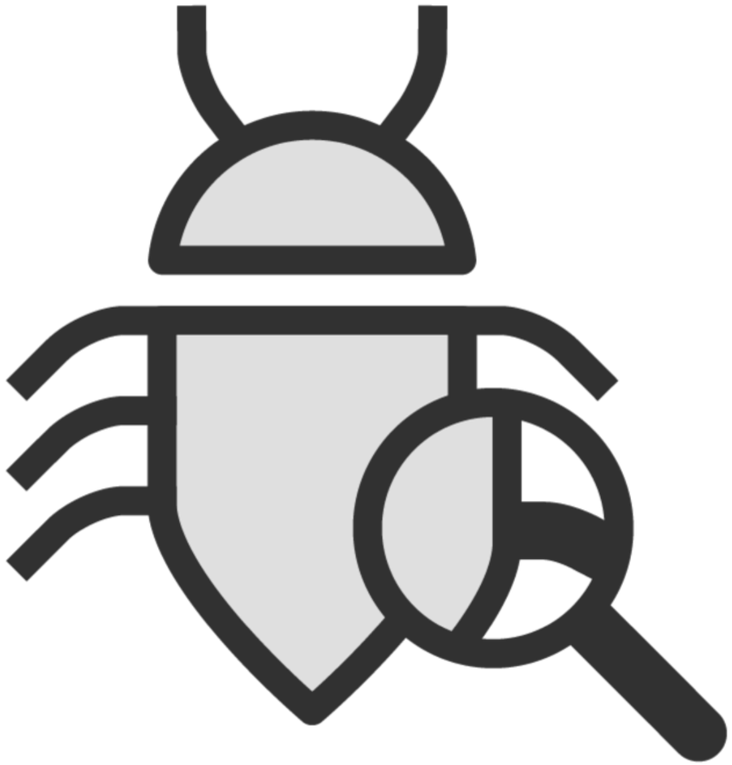
https://t.me/learningnets



Agent Smith

https://t.me/learningnets

Agent Smith



Takes over a android device without the user's knowledge

Replaces a legitimate app with a malicious copy

Disguised as games, photo editors and other tools

Designed to look like system notifications

https://t.me/learningnets

Signal System 7

A cellular network protocol

Allows attackers to read messages, listen to calls, and track the device's location

Used to initiate MiTM attacks

By-passes 2FA and end-to-end encryption

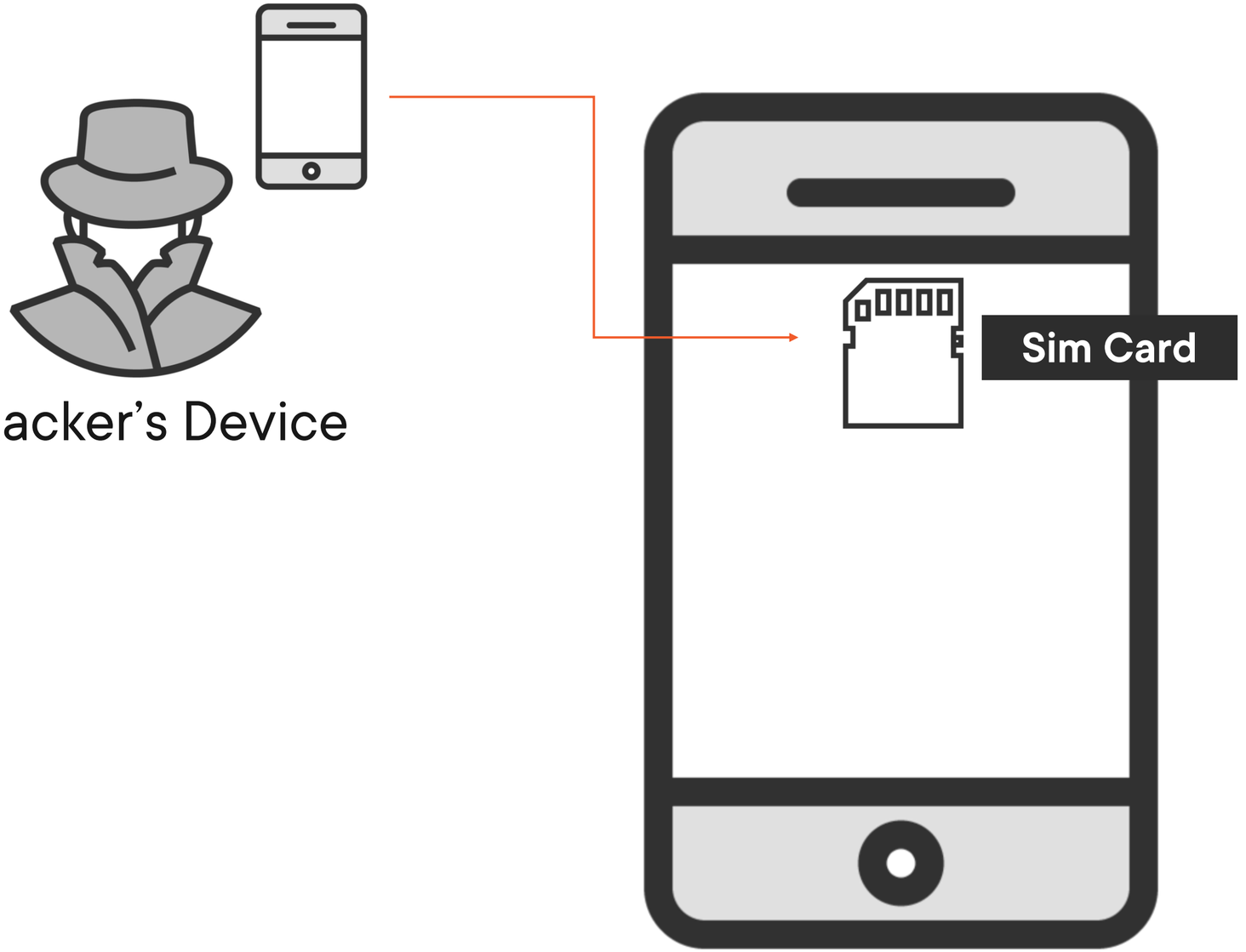
https://t.me/learningnets

Simjacker

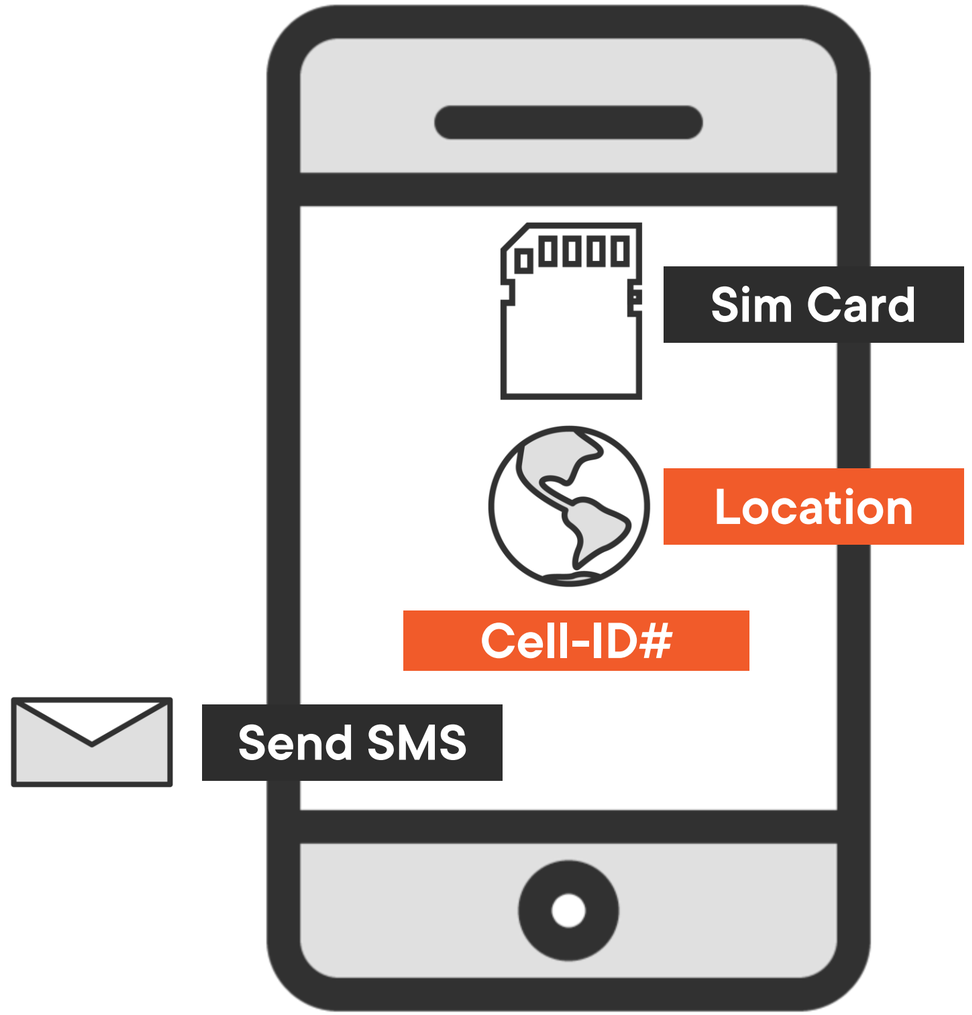
Associated to a SIM card's S@T browser

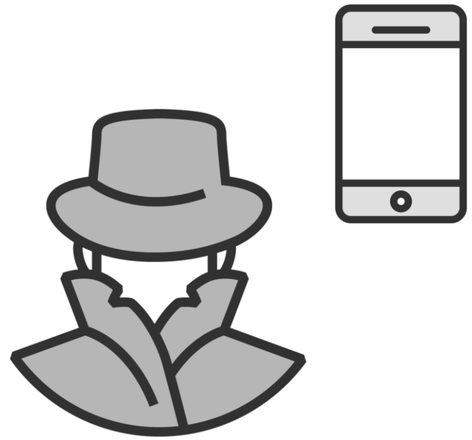
Sends an encrypted message to the network provider that contains your SIM card number and other details

https://t.me/learningnets



https://t.me/learningnets





Attacker's Device

Cell-ID
and location

https://t.me/learningnets

Learning Check

https://t.me/learningnets

Learning Check

- **Man-in-The-Mobile (MiTM)**
- **Simjacking**
- **Drive-by**
- **Agent Smith**
- **SS7**

https://t.me/learningnets

Up Next:
Investigating Android Devices

https://t.me/learningnets