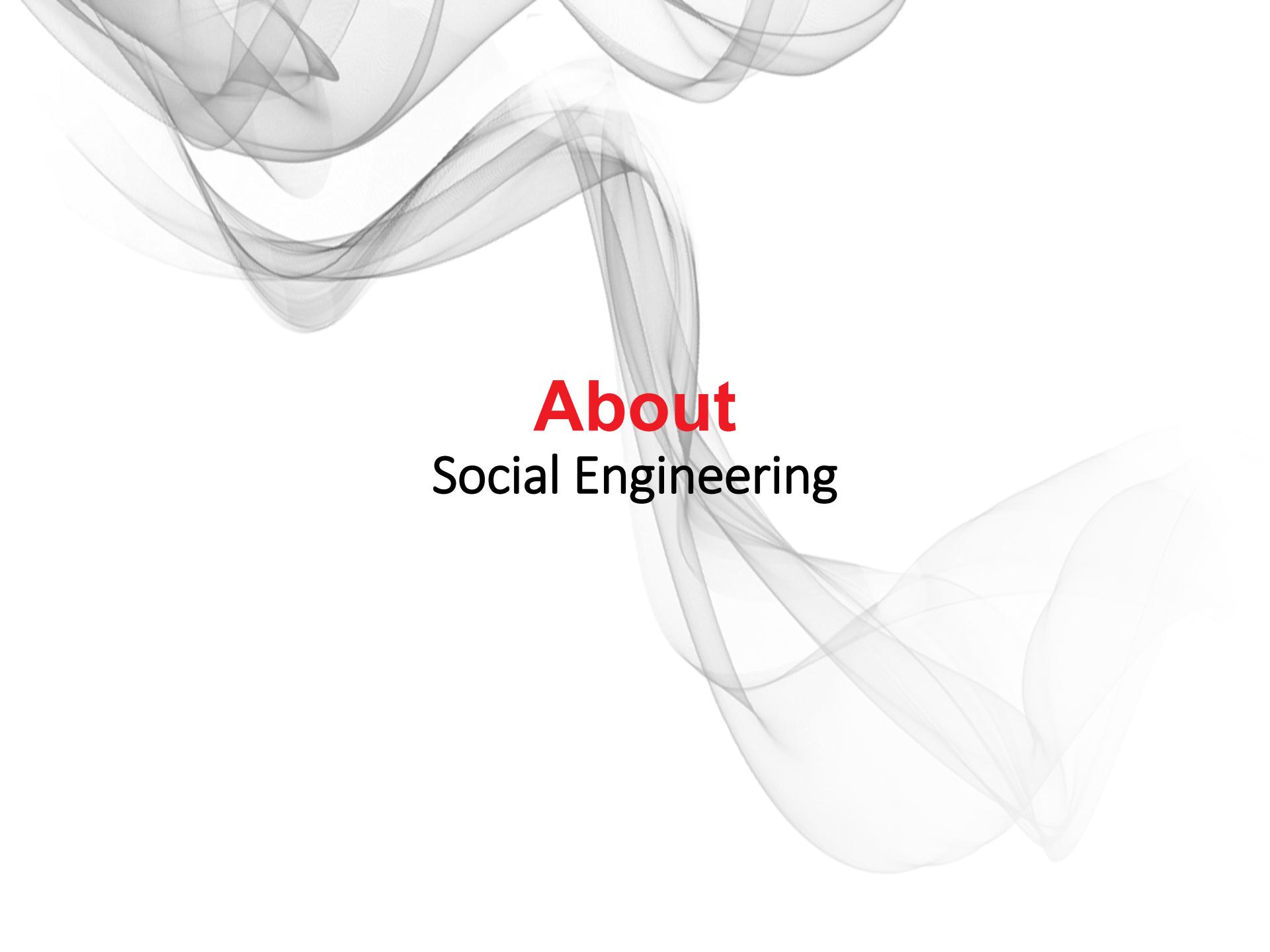




# Social Engineering

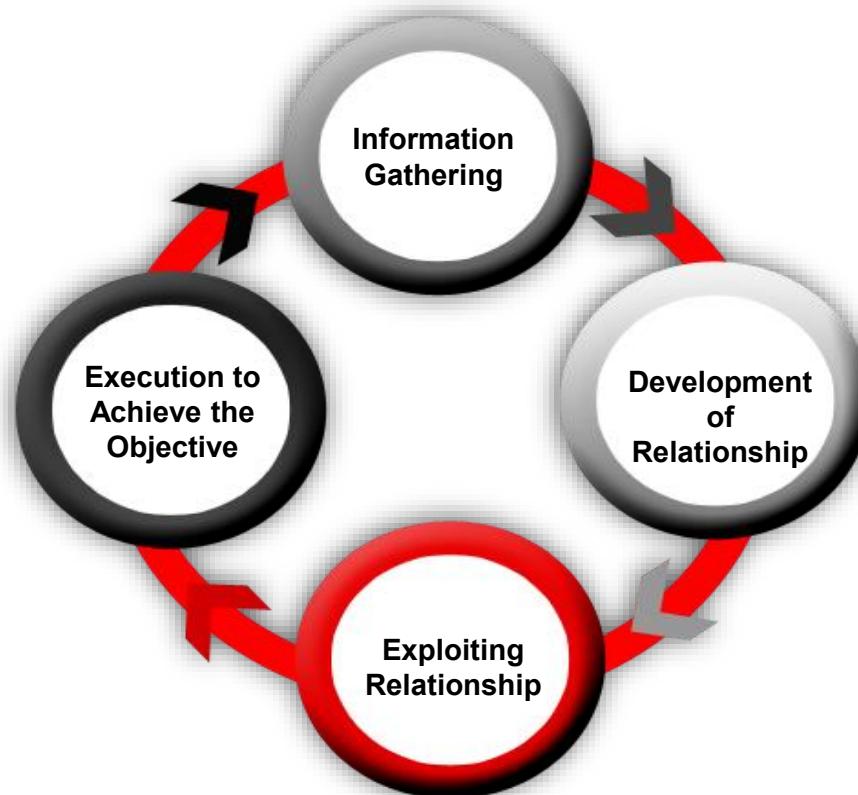
Cybersecurity Awareness

The background features a subtle, abstract design composed of several thin, grey, wavy lines that curve and overlap across the frame, creating a sense of depth and motion.

# About Social Engineering

# What is Social Engineering ?

Social Engineering is the art of manipulating people into performing actions that lead to breach of confidential data & give access to personal sensitive information.



# What are they searching for?

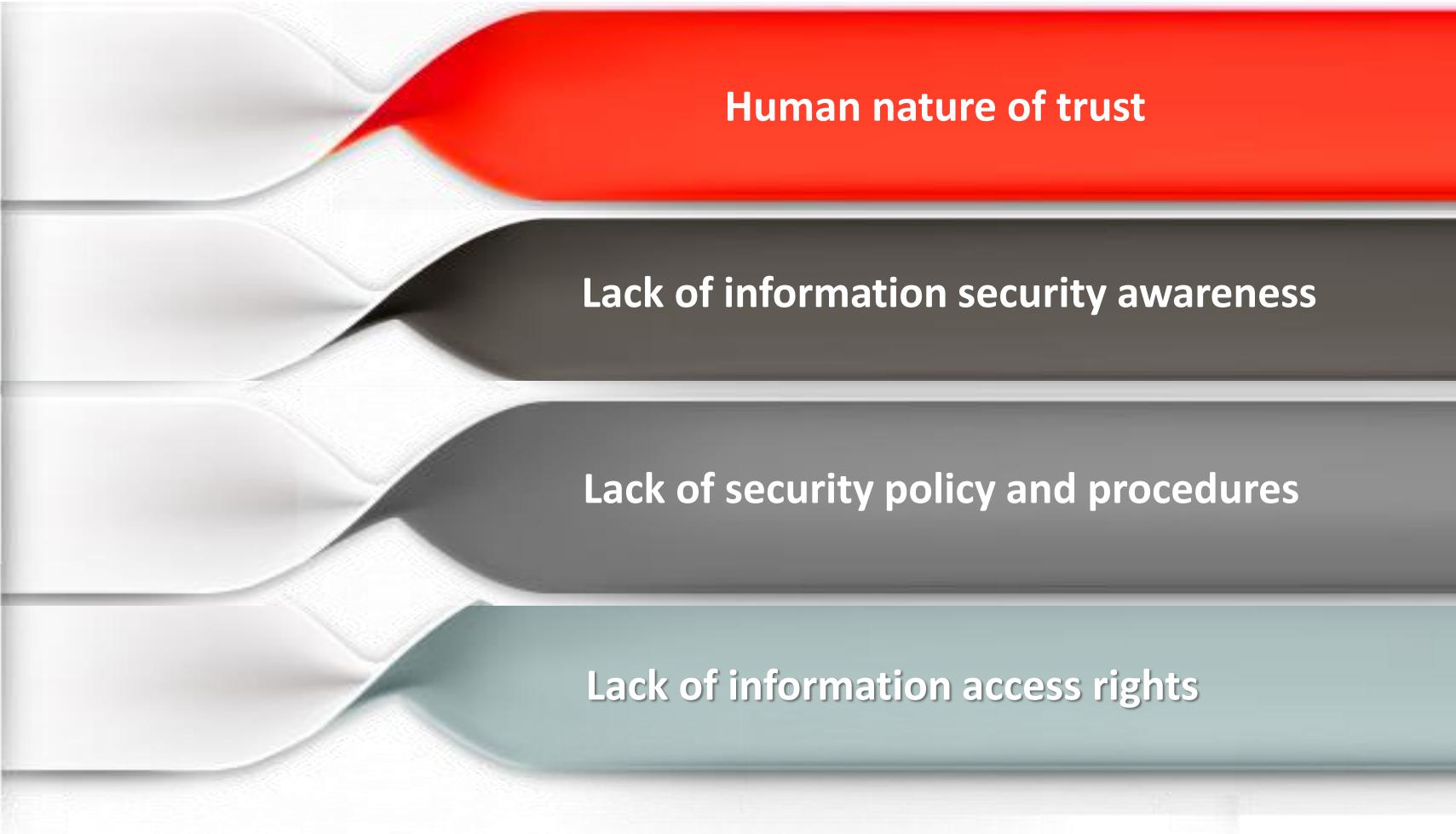
Collect sensitive information

Identity theft

Targeted attacks



# Why they Succeed?



**Human nature of trust**

**Lack of information security awareness**

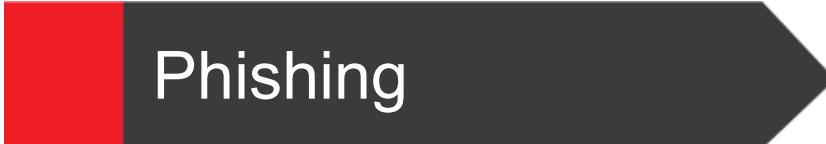
**Lack of security policy and procedures**

**Lack of information access rights**



# Social Engineering **Techniques**

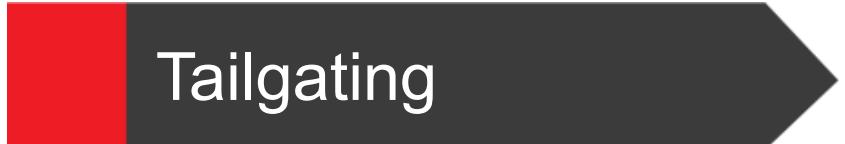
# Techniques



Phishing



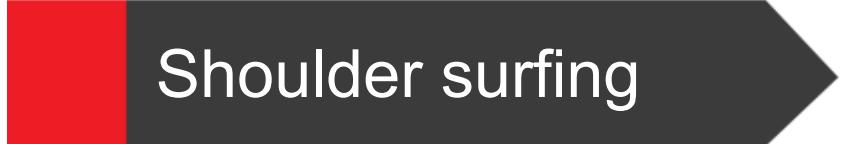
Vishing



Tailgating



SMiShing



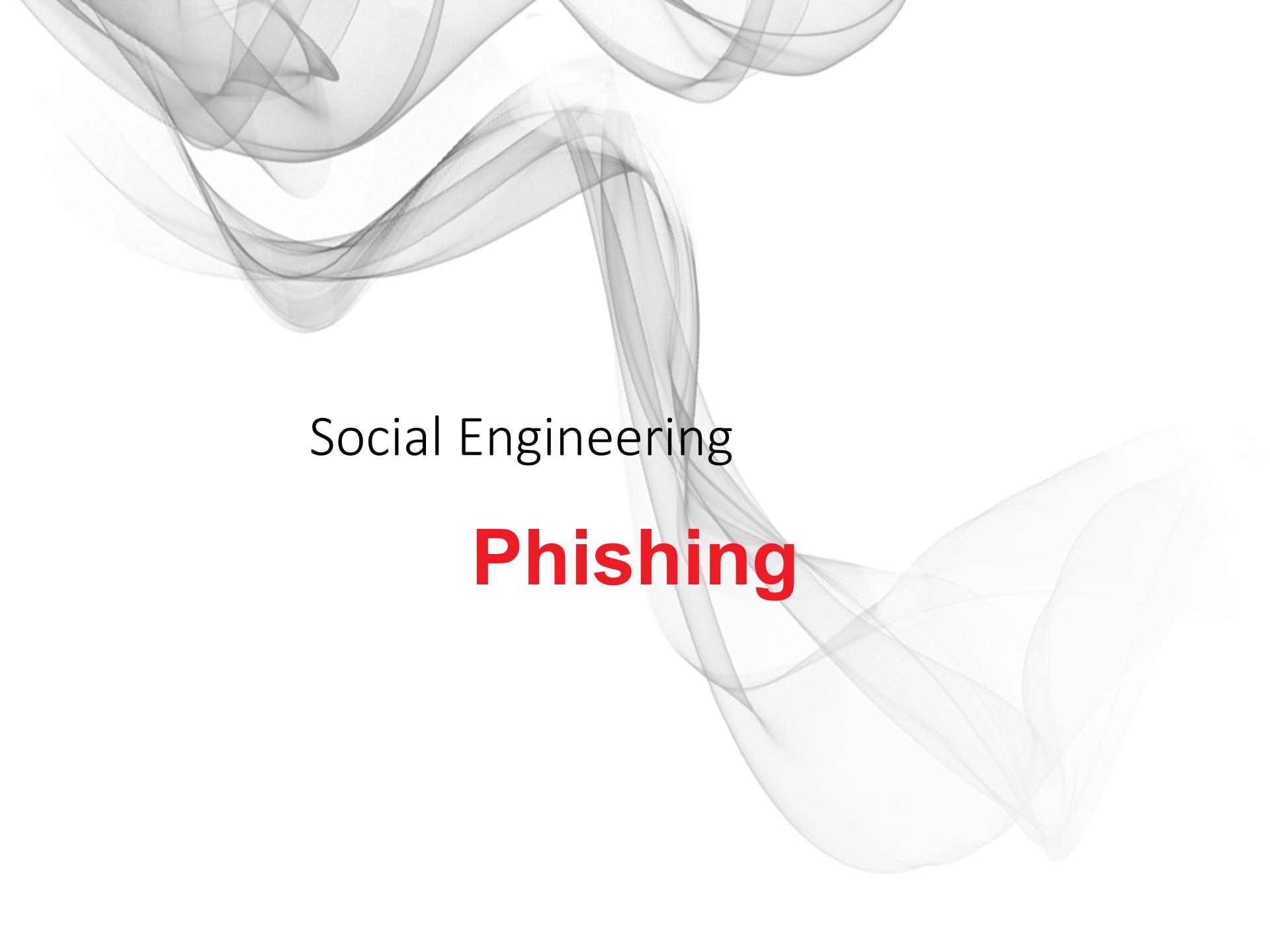
Shoulder surfing



Baiting



Dumpster Diving

The background features a subtle, abstract design of grey wavy lines that curve and overlap across the entire slide, creating a sense of depth and motion.

Social Engineering

# Phishing

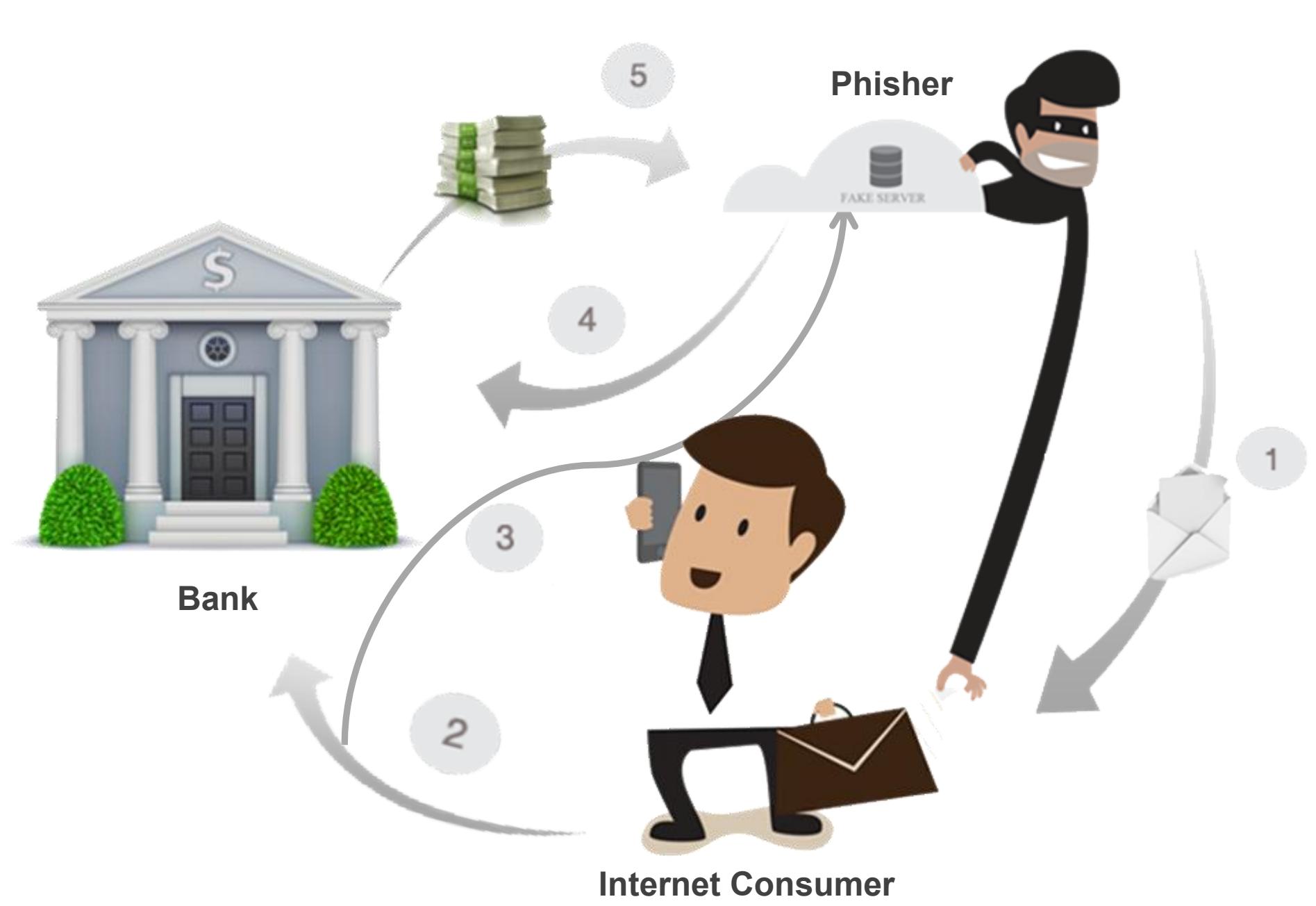
# Phishing

It is a kind of email fraud where the fraudster sends out a legitimate looking email posing as a trusted entity which is designed to extract sensitive information.

## Did You Know?

94% of malware is delivered  
via email





# Phishing: General Phishing

## What is it?

Email messages claiming to come from trusted sources like your bank asking you to verify your account, re-enter your personal information or make a payment.

## Why?

To trick you into providing your bank account details in order to access your bank account then steal your money

## How to Avoid?

Compare these messages with ones you already have and call the source to re-verify



# Phishing: Spear Phishing

## What is it?

Email messages usually targeting higher profile people who have valuable information

## Why?

Directly targeting you to access your bank account then steal your money or collect sensitive information

## How to Avoid?

Look out for spelling mistakes and fake URLs



# Phishing: Authority Fraud

## What is it?

Email messages with addresses similar to that of an authority to request confidential information or request payments within the country.

## Why?

To trick the victim to provide confidential information or transfer money to the cybercriminals

## How to Avoid?

Double-check suspicious requests with the authority before providing information or sending money



# Phishing: Pharming

## What is it?

Redirecting website traffic through hacking which may cause users to find themselves on an illegitimate website without realizing they have been redirected to an impostor site, which may look exactly like the real site.

## Why?

To intercept and steal sensitive information or online payments

## How to Avoid?

Check the URL and look for secure certificate



# Phishing: Examples

## Fake Email Messages

The screenshot shows an email interface with a blue header bar. The title bar reads "Coronavirus (2019 -nCoV) Safety Measures - Temporary Items". Below it, the word "Message" is visible. A red oval highlights the subject line "Coronavirus (2019 -nCoV) Safety Measures". Another red oval highlights the recipient's email address "@who-pc.com>". A green circular icon with the letters "DL" is on the left. The date "Tuesday, February 4, 2020 at 7:08 PM" is shown below the recipient. A red oval highlights the attachment "CoronaVirus\_Safety... 1.6 MB". At the bottom, there are "Download All" and "Preview All" buttons.

Dear Sir/Madam,

Go through the attached document on safety measures regarding the spreading of corona virus.

This little measure can save you.

WHO is working closely with global experts, governments and partners to rapidly expand scientific knowledge on this new virus and to provide advice on measures to protect health and prevent the spread of this outbreak.

Symptoms to look out for; Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards

[REDACTED]

General Internist

Intensive Care Physician

WHO Plague Prevention & Control



FAKE

# Phishing: Examples

## Fake Email Messages

Severity: storage stopped working at 2:03:58 PM

SA System Admin Notification <t.browne@tbig.co.nz>  
To [REDACTED]

(i) This message was sent with High importance.  
If there are problems with how this message is displayed, click here to view it in a web browser.

Reply | Reply All



Hello [REDACTED]

We detected you have 4 undelivered incoming emails on Friday, March 27, 2020, this is because your account storage is full, your action is required for them to be released.

### What you should do?

People trying to contact you will receive a message to this effect except you take action below to your portal to retrieve messages and choose what happens to them.

Release Message

(c) 2020 Microsoft Corporation. All Rights reserved | Acceptable usage policy | Privacy Notice

FAKE

# Phishing: Examples Fake Websites

The image shows two side-by-side web browser windows comparing a real Instagram sign-up page on the left with a fake one on the right.

**Real Instagram Sign-up Page (Left):**

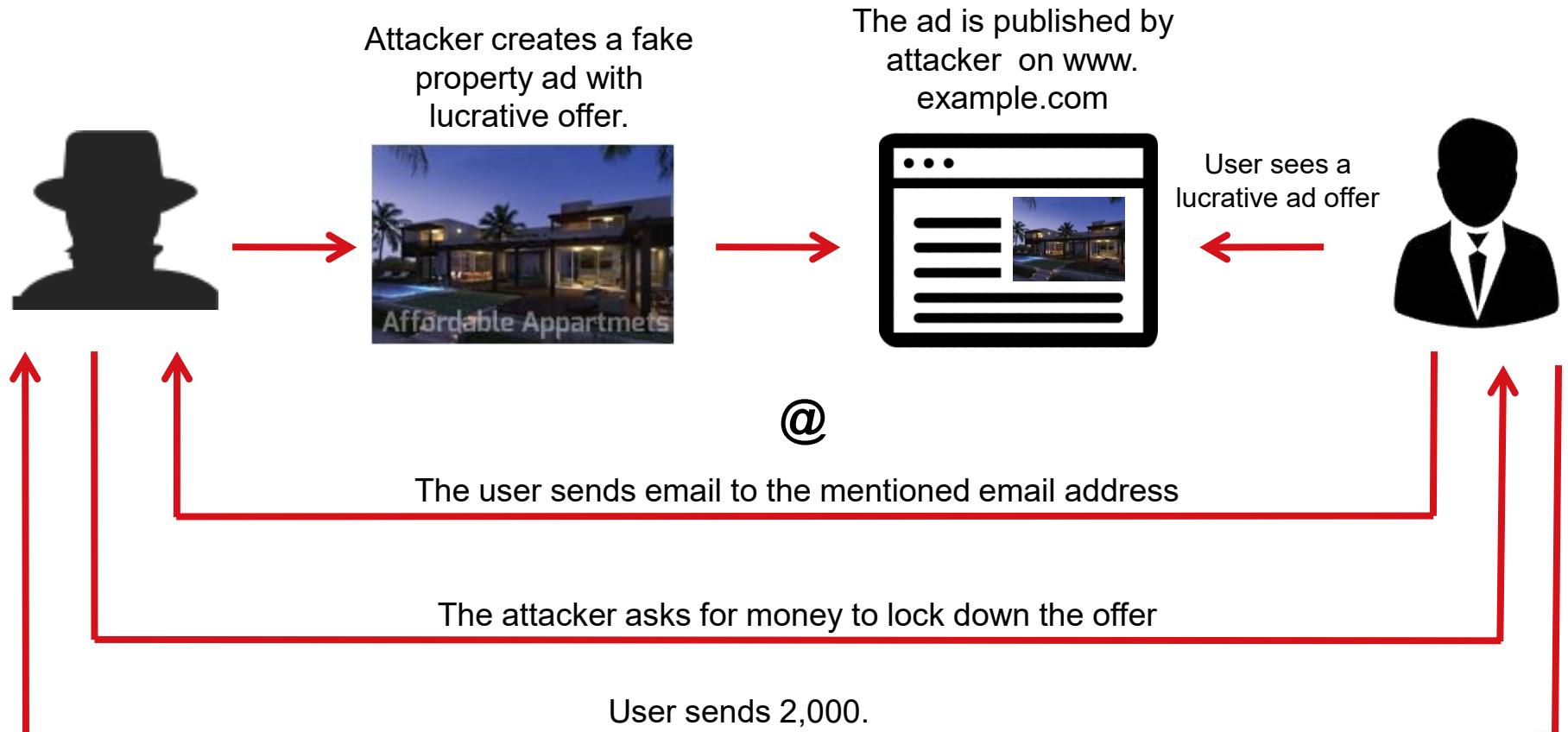
- Header:** "Instagram" logo and "Sign up to see photos and videos from your friends."
- Login Options:** "Log in with Facebook" button.
- Form Fields:** "Mobile Number or Email" and "Full Name" input fields.
- Text Area:** A large green rectangular area containing the word "REAL" in white.
- Buttons:** "Sign up" button and "By signing up, you agree to our Terms, Data Policy and Cookies Policy." link.
- Log-in Option:** "Have an account? Log in" link.
- App Download:** "Get the app." section with "Download on the App Store" and "GET IT ON Google Play" links.
- Footer:** Links to "ABOUT US", "SUPPORT", "PRESS", "API", "JOBS", "PRIVACY", "TERMS", "DIRECTORY", "PROFILES", "HASHTAGS", and "LANGUAGE".
- Copyright:** "© 2019 INSTAGRAM FROM FACEBOOK"

**Fake Instagram Sign-up Page (Right):**

- Header:** "Instagram" logo and "Sign up to see photos and videos from your friends."
- Form Fields:** "Mobile Number or Email", "Full Name", "Username", and "Password" input fields.
- Text Area:** A large red rectangular area containing the word "FAKE" in white.
- Buttons:** "Sign up" button and "By signing up, you agree to our Terms, Data Policy and Cookies Policy." link.
- Log-in Option:** "Have an account? Log in" link.
- App Download:** "Get the app." section with "Download on the App Store" and "GET IT ON Google Play" links.
- Footer:** Links to "ABOUT US", "SUPPORT", "PRESS", "API", "JOBS", "PRIVACY", "TERMS", "DIRECTORY", "PROFILES", "HASHTAGS", and "LANGUAGE".
- Copyright:** "© 2019 INSTAGRAM FROM FACEBOOK"

A red oval highlights the URL bar of the fake page, which shows a suspicious URL: `https://www.instagram.com/fakeinsta.cf`.

# Example Scam



The background features a subtle, abstract design of grey wavy lines that curve and flow across the frame, creating a sense of motion and depth.

Social Engineering

**Vishing**

# Vishing

Collecting sensitive information or attempting to influence action via the telephone. To obtain valuable information that could contribute to the direct compromise of the victim or the organization by exploiting peoples' trust and willingness to help



## Vishing news

20 NOV 2019 NEWS

### Vishing Attacks to Become Commonplace in 2020

During 2019 to February this year, Abu Dhabi Police arrested 13 criminal gangs made up of 142 fraudsters involved in vishing attacks. The fraudsters were posing as bank employees “You cannot find a phishing or vishing news story that does not involve COVID-19,” Christopher Hadnagy, chief human hacker at Social-Engineer LLC, told the *Business Journal*.

Source:

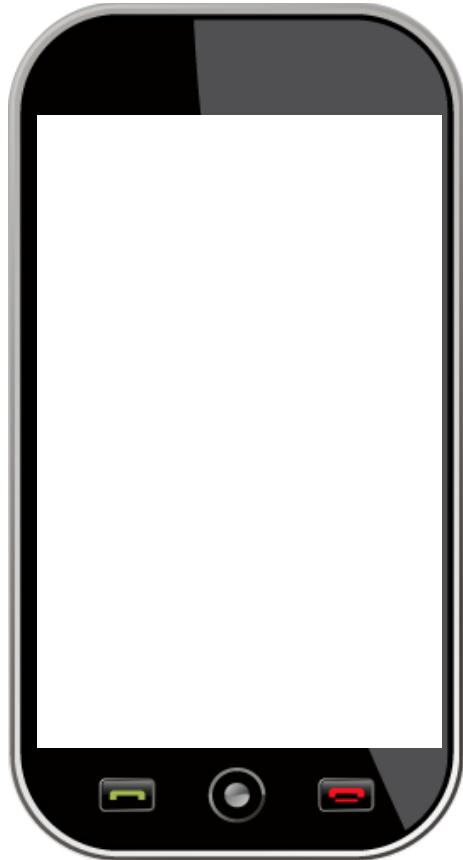
<https://www.infosecurity-magazine.com/news/vishing-attacks-to-become/>

<https://gulfnews.com/business/banking/uae-banking-sector-joins-law-enforcement-agencies-to-fight-fraud-1.70971327>

<https://www.csbj.com/2020/04/10/hackers-exploit-pandemic-to-attack-businesses/>

# Vishing: Examples

## Fake Phone call



“Hello. This is Alex calling from your telecom provider. You have a refund due which I would like to remind you of, but first can you please provide your credit card number for verification before we proceed ? “



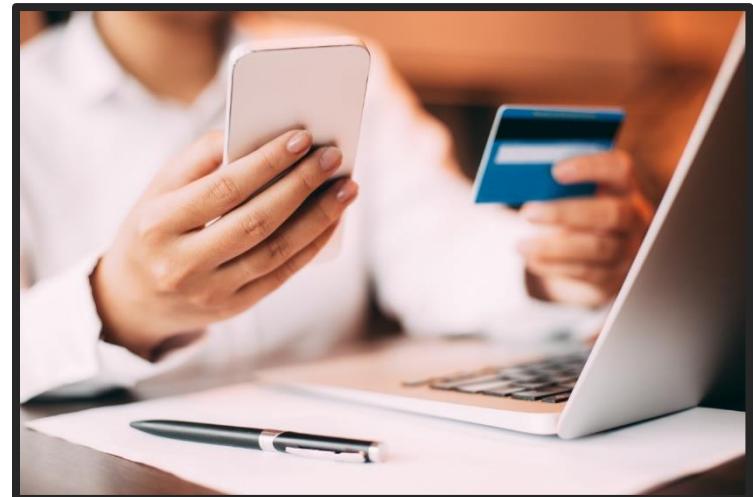
The background features a subtle, abstract design of grey wavy lines that curve and overlap across the entire slide, creating a sense of depth and motion.

Social Engineering

**SMiShing**

# SMiShing

Using mobile phone text messages (SMS) to push victims into immediate action such as downloading mobile malware, visiting a malicious website or calling a fraudulent phone number extract sensitive information or steal money



# SMiShing: Examples

## Fake SMS

(ALERT!) Your Bmo Bank account has been suspended. To unlock your account, click here: <https://bit.ly/1EeZ6m2>

John, transfer €300k to the following a/c. No time to explain just do it and I'll explain after the board meet.

Is this really a pic of you?  
<http://tinyurl.com/ntn9ohk>

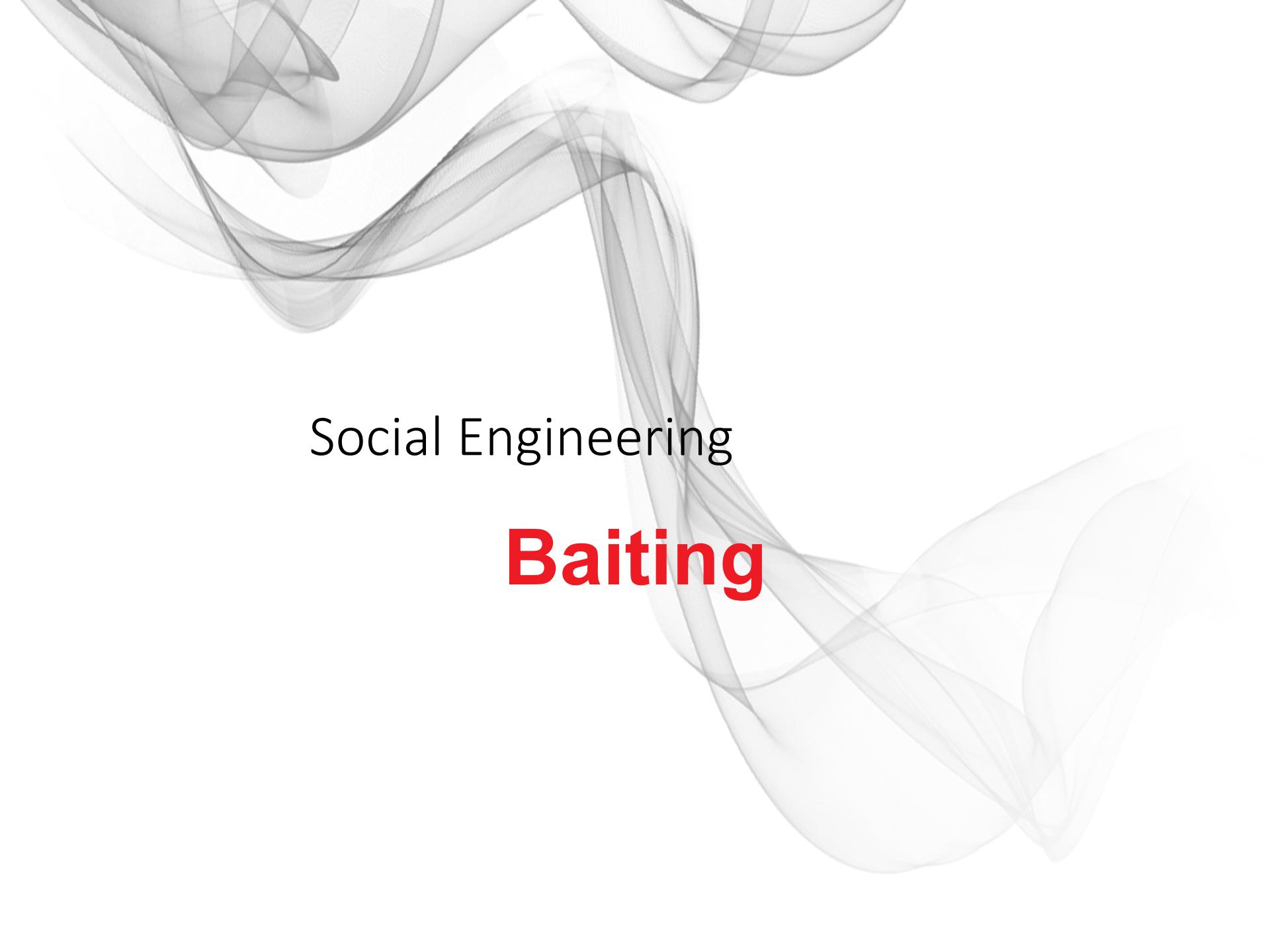
Dear Customer,

Your AppleID is due to expire Today, Please tap <http://bit.do/cRqb6> to update and prevent loss of services and data.

Apple smsSTOPto43420

Dear Walmart shopper,  
your purchase last month  
won a \$1000 Walmart  
Gift Card. Click here to  
claim:  
[www.WmartProgram.com](http://www.WmartProgram.com)  
(Quit2end)

Dear NAB Bank User,  
We have detected some  
unusual activity.  
We urgently ask you to  
follow the account review  
link:  
<http://bit.do/nab-bank>

The background features a subtle, abstract design composed of several thin, grey, wavy lines that curve and overlap across the frame, creating a sense of depth and motion.

# Social Engineering

## Baiting

# Baiting

With the use of physical media like a USB or a CD, the attacker tries to capture the attention of the victim by giving it a mysterious label and deliberately placing it where it can be easily found (washroom, elevator etc).



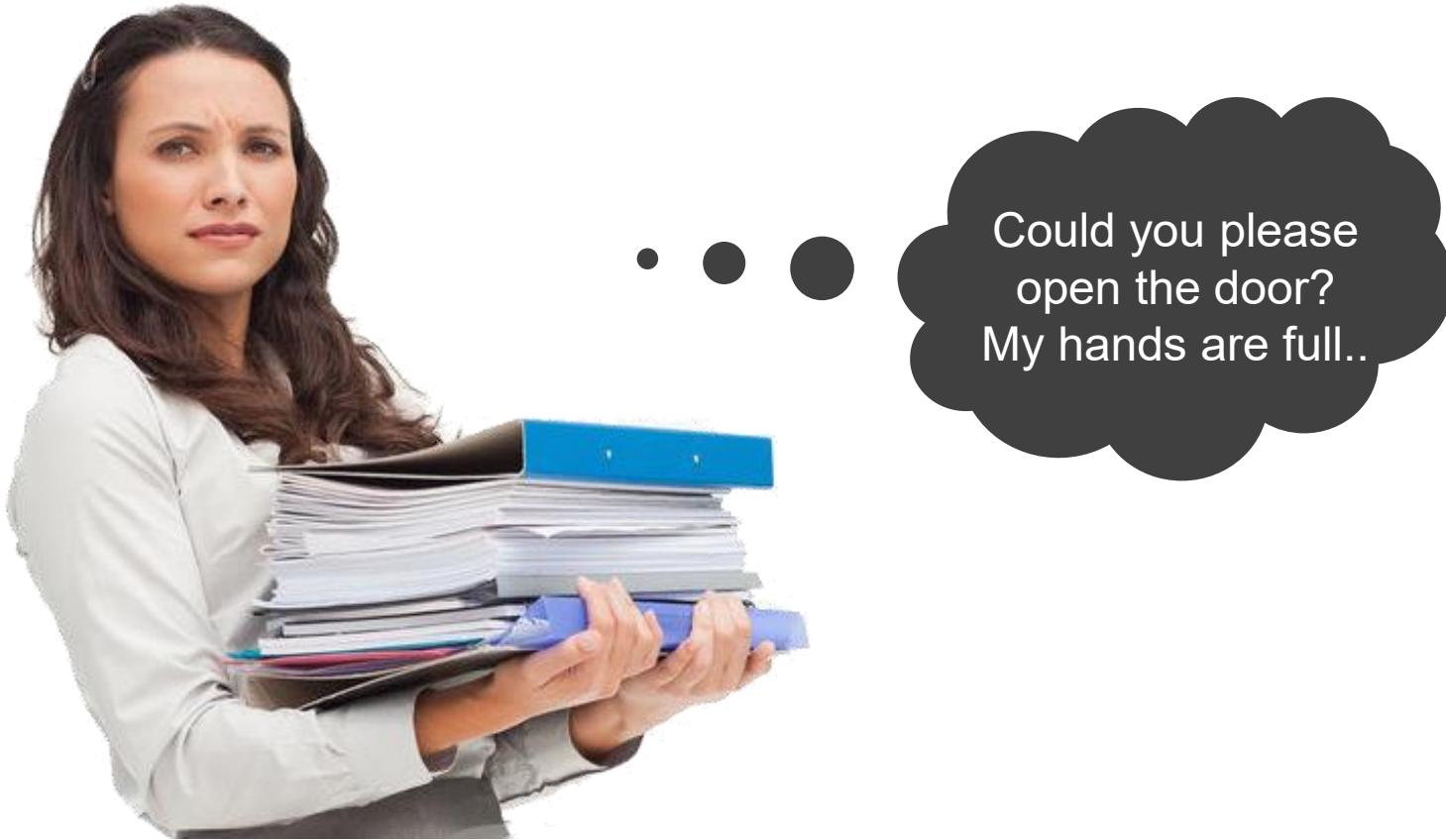
The background features a subtle, abstract design of grey wavy lines that curve and overlap across the entire slide, creating a sense of depth and motion.

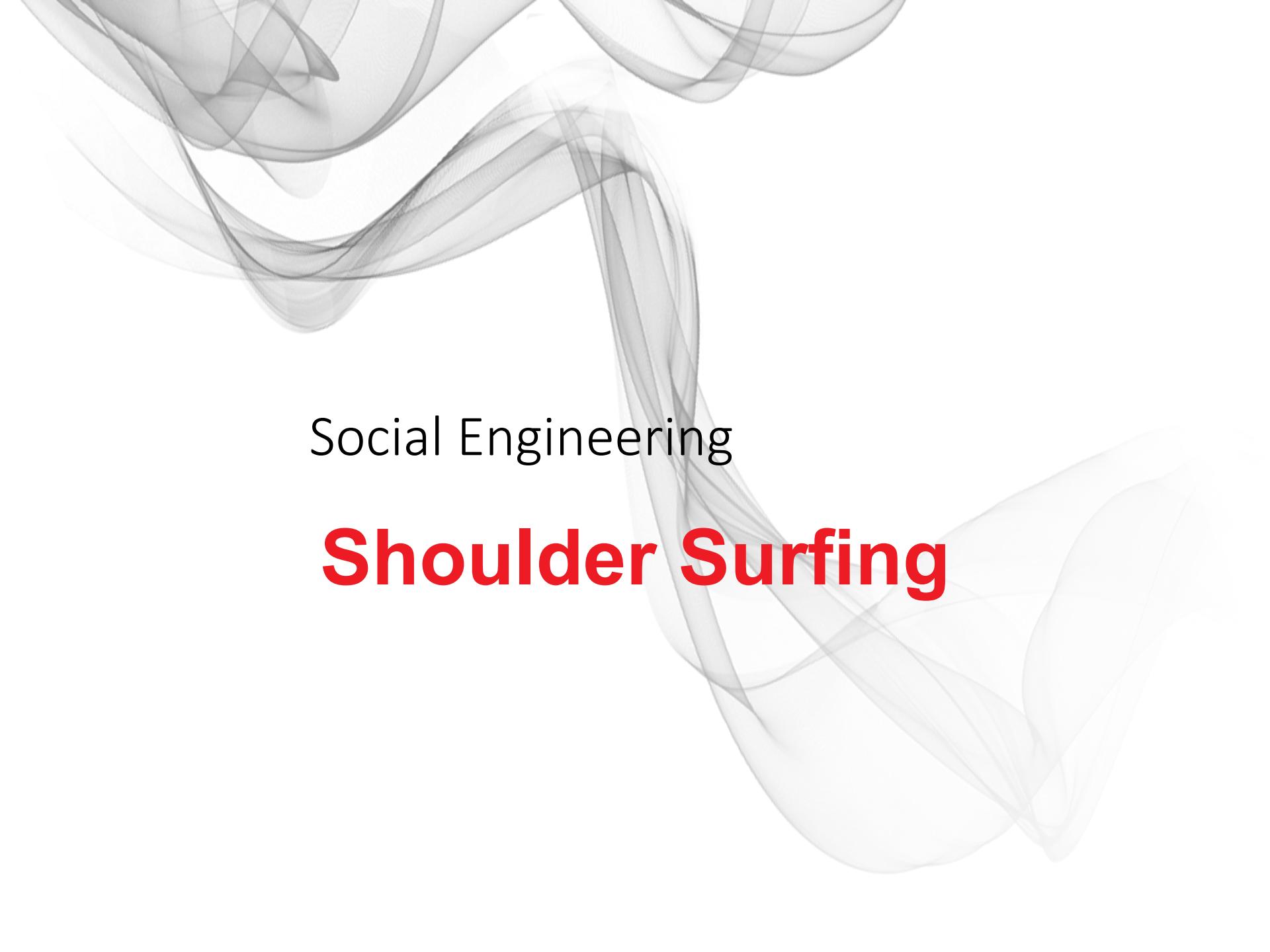
Social Engineering

# Tailgating

# Tailgating

Physically following someone into a limited access area



The background features a subtle, abstract design of grey, translucent wavy lines that curve and overlap across the slide, creating a sense of depth and motion.

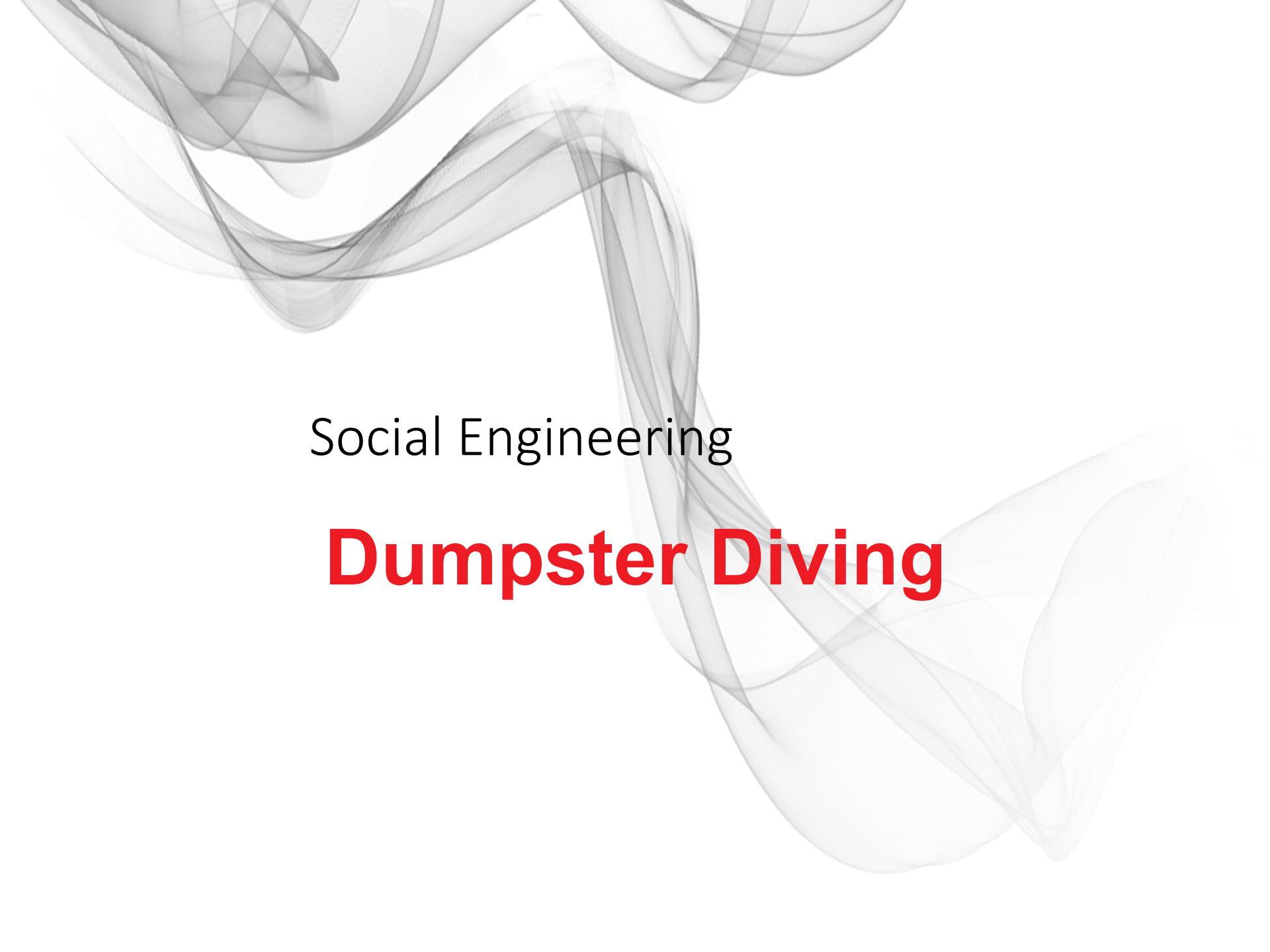
Social Engineering

# **Shoulder Surfing**

# Shoulder Surfing

Shoulder surfing is watching someone's login credentials, ID number, POS terminal PIN, ATM PIN or any other personal secret credentials by looking over their shoulder while they are using it.



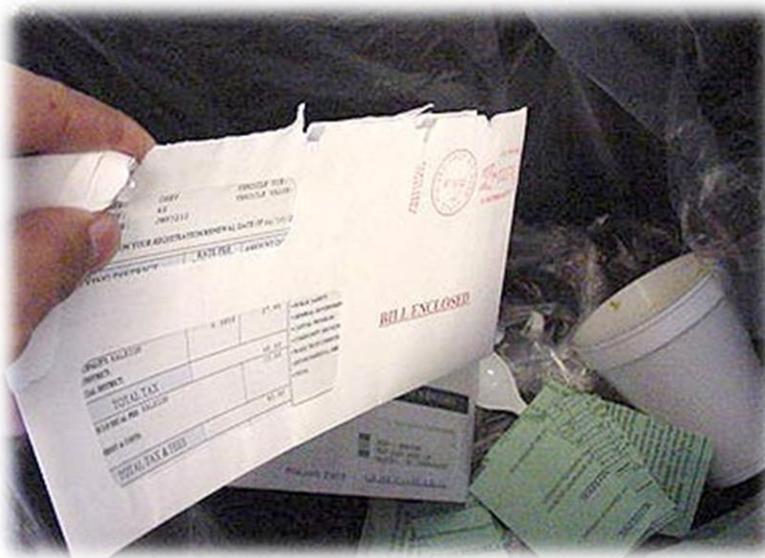
The background features a subtle, abstract design of grey wavy lines that curve and overlap across the slide, creating a sense of depth and motion.

Social Engineering

# Dumpster Diving

# Dumpster Diving

It is a method of stealing personal information by digging through a company's dumpster or trash



**Login:** john  
**Password:** wombat55



Social Engineering

**Protect yourself and  
your organization**

# Best Practices

01

Information Security Awareness Trainings

02

Establish Policies & Procedures to recognize and respond to social engineering threats

03

Build a security-aware culture

04

Be aware of providing personal information to avoid being a victim of phishing, Vishing or SMiShing attacks

**05**

If you are an organization, perform unannounced periodic tests of the network

**06**

Have a proper waste management system to avoid dumpster diving

**07**

Respectfully refuse to lend your identity token / security pass to avoid tailgaters access the building

**08**

Do not use a device on your computer unless it belongs to you or is given to you for a purpose from a trustworthy person

**09**

Review the above steps periodically

# Questions

WHAT? HOW? WHEN?  
WHO? WHERE? WHO?  
WHY? WHERE? WHEN? WHY?  
WHEN? WHY? HOW?  
HOW? WHAT? WHO?  
WHO? WHERE? WHERE?  
WHAT? WHO? WHY?  
WHO? WHERE? WHO?  
WHERE? WHO? HOW?  
HOW? WHAT? WHO?  
WHO? WHERE? WHERE?  
WHAT? WHO? WHERE?  
WHEN? WHO? WHERE?  
WHAT? WHERE? WHO?  
WHO? WHERE? HOW?  
WHERE? WHO? WHAT?  
WHY? WHAT? WHEN?  
WHEN? HOW? WHO?  
WHAT? WHERE? WHO?  
WHY? HOW? WHO?  
WHO? WHERE? WHAT?  
WHERE? WHO? WHAT?  
WHEN? WHO? WHERE?  
WHAT? WHERE? WHO?  
WHEN? WHO? WHERE?

WHERE?  
WHO? WHAT?  
WHERE? WHY?  
HOW? WHEN?  
WHAT? WHO?  
WHEN? WHERE?  
WHAT? HOW?  
WHEN? WHO? WHAT?  
HOW? WHERE? WHO? WHAT?  
WHY? WHAT? WHEN?  
WHEN? HOW?  
WHERE? HOW?  
WHAT? WHAT?  
WHEN? WHO?  
WHERE?