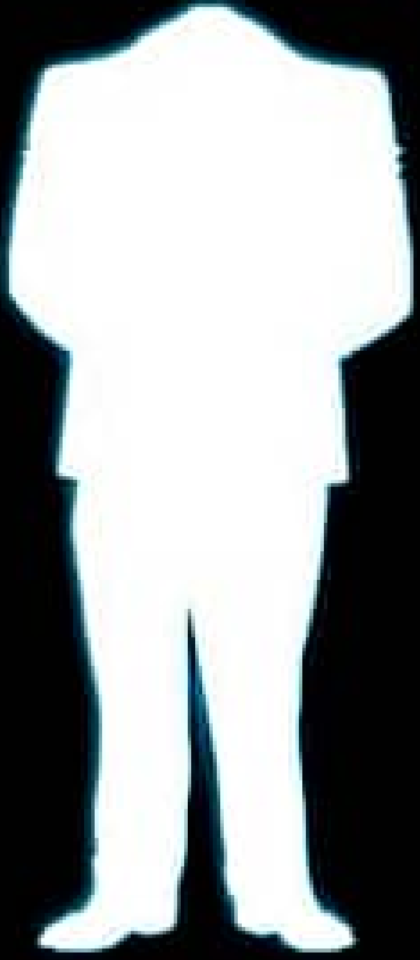
# SOCIAL?ENGINEERING



Ramiro Cid | @ramirocid

# Definitions

- **Cyber Security:** It is also known as "IT security" or "Computer security" is information security applied to computing devices such as servers, computer networks and mobile devices (as smartphones, tablets, etc.), as well as computer networks such as private and public networks, including the whole Internet.

- **Social engineering:** In the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

- **Cybercrime:** It is also known as Computer crime, is any crime that involves a computer and/or a network. The computer may have been used in the commission of a crime, or it may be the target. Netcrime is criminal exploitation of the Internet, inherently a cybercrime. Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones.

## 2. How does social engineering works?

Most social engineering attacks begin with the attacker performing recon and research on the victim. For instance, if the target is a firm, the hacker might learn about its internal processes, organizational structure, industry jargon, potential business partners, and other details. Focusing on the actions and behaviors of workers with low-level but initial access, like a security guard or receptionist, is one strategy used by social engineers. Attackers can search social media accounts for personal information and observe their behavior both online and in person. The social engineer can next use the information gathered to plan an attack and take advantage of the flaws discovered during the reconnaissance process.

If the attack is successful, the attacker may obtain protected systems or networks, money from the targets, or access to private data like Social Security numbers, credit card numbers, and bank account information. In India, credit card fraud is usually committed similarly when someone calls the users, conveys to be a bank official, and asks the users to share the one-time password received on their mobile to safeguard their financial interests or bank accounts, etc.

# Why you should be concerned ?

***"...Why would anybody attack me if I have nothing to hide? I don't have any secret information. Why would an attacker be interested in me so?..."***

These are typical mindsets of users/people who think they are not going to be targeted by criminals.

The mindset of an attacker is different:

- They don't want to attack **<u>YOU</u>**, they want **<u>something</u>** and they will use you along the way if it helps them to achieve their goal.
- With many companies investing heavily into security technologies it is often easier for an attacker to exploit people, rather than to hack into computer networks and systems

  **-> This makes you a target.**

# Social Engineering: Potential Impact

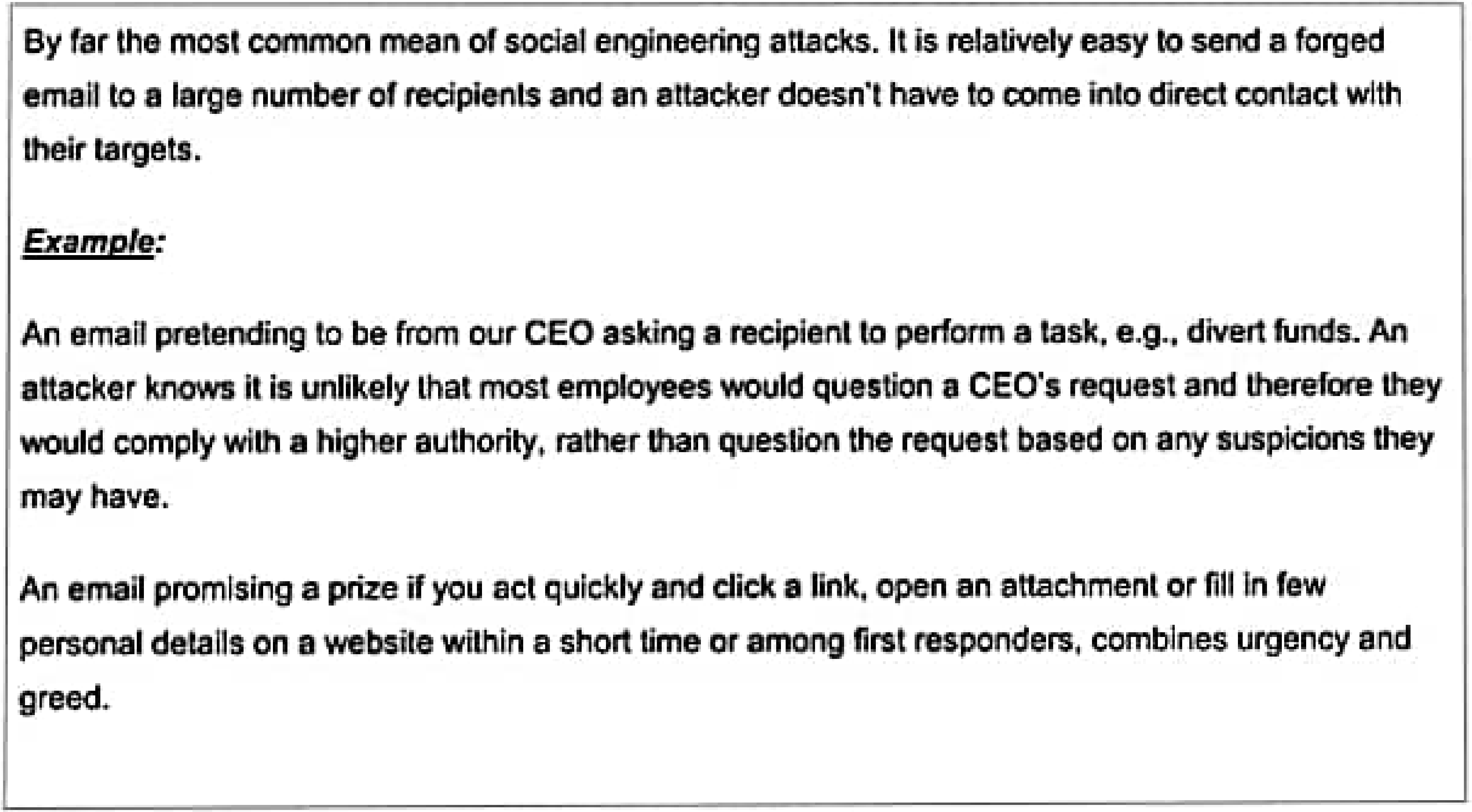
- Financial loss
- Data leak
- Reputation image (company and/or person)
- Management time
- Loss of public trust
- Legal fines
- Loss of new or existing customers
- Loss of company morale
- Increased audit costs

## 3. Social Engineering: Cyber threat to cyber security

**Cyber Security** *“means protecting information, equipment, devices, computer, computer resource, communication devices, and information stored therein from unauthorized access, use, disclosure, disruption, modification, or destruction”*[2]. Cyber security is a part of information security that relates to the protection of computers, networks, programs, and data against unauthorized access. As cybersecurity includes the protection of both company and personal data, the fields of cybersecurity and data protection overlap. The security objectives of confidentiality, integrity, and availability are of paramount importance to both elements of information security. The recent data breach at the payment from Mobikwik in India is alarming. According to reports, the data breach affected 3.5 million customers, revealing know-your-customer records including addresses, phone numbers, Aadhaar cards, and PAN cards, among other things. Until recently, the corporation has claimed that no such data breach occurred. Only until the regulator, the Reserve Bank of India (RBI), instructed Mobikwik to immediately perform a forensic audit by a CERT-IN impaneled auditor and submit the findings did the business begin engaging with the appropriate authorities[3].

In a cyber security context, social engineering is the set of tactics used to manipulate, influence, or deceive a victim into divulging sensitive information or performing ill-advised actions to release personal and financial information or hand over control over a computer system. Cyber attacks are an increasingly sophisticated and evolving danger to your sensitive data, as attackers employ new methods powered by social engineering. Cybercriminals pretend to be an official representatives sending you an email or message with a warning related to your account information. The message will often ask for a response by following a link to a fake website or email address where you will provide confidential information. The format of the message will typically appear legitimate using proper logos and names. Any information entered into the fake link goes to the cyber-criminal.

# Email attacks *(Phishing)*



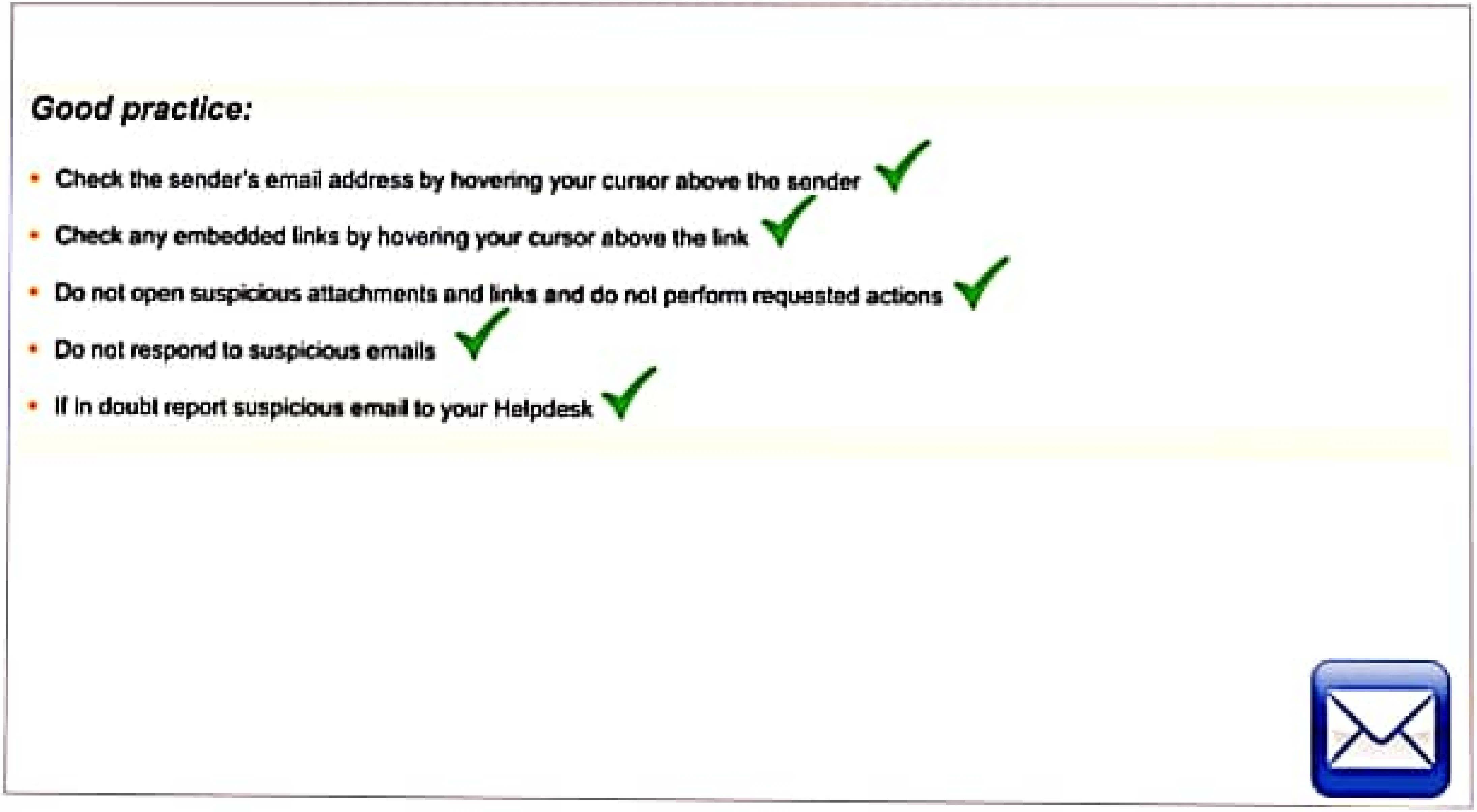
By far the most common mean of social engineering attacks. It is relatively easy to send a forged email to a large number of recipients and an attacker doesn't have to come into direct contact with their targets.

***Example*:**

An email pretending to be from our CEO asking a recipient to perform a task, e.g., divert funds. An attacker knows it is unlikely that most employees would question a CEO's request and therefore they would comply with a higher authority, rather than question the request based on any suspicions they may have.

An email promising a prize if you act quickly and click a link, open an attachment or fill in few personal details on a website within a short time or among first responders, combines urgency and greed.

# Email attacks *(Phishing)*



***Good practice:***

- Check the sender's email address by hovering your cursor above the sender ✓
- Check any embedded links by hovering your cursor above the link ✓
- Do not open suspicious attachments and links and do not perform requested actions ✓
- Do not respond to suspicious emails ✓
- If in doubt report suspicious email to your Helpdesk ✓

## 4. Cybercrime through Social Engineering

The term **Cybercrime** may be judicially interpreted in some judgments passed by courts in India, however, it is not defined in any act or statute passed by the Indian Legislature. Cybercrime is an uncontrollable evil having its base in the misuse of growing dependence on computers in modern life. The usage of computers and other allied technology in daily life is growing rapidly and has become an urge which facilitates user convenience.

Professor S.T. Viswanathan has given three definitions in his book *The Indian Cyber Laws with Cyber Glossary* as follows -

1. Any illegal activity in which a computer is the tool or object of the crime i.e. any crime, the means or purpose of which is to influence the function of a computer,

The growth of social engineering crime in recent years has mainly been attributed to improvements in business firms' physical and online security.

2. Any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention, made or could have made a gain,

3. Computer abuse is considered any illegal, unethical, or unauthorized behavior relating to the automatic processing and transmission of data [4].

Cybercriminals that engage in social engineering are digital con artists, gaining vulnerable people's trust to steal money or data easily. Social engineering fraudsters attempt to manipulate users with a variety of tactics to perform attacks. Generally, they use people's trustworthiness to their advantage and target users that have limited knowledge with regards to keeping their personal/company data safe. Most cybercrime techniques revolve around finding and exploiting weak points in a company's digital infrastructure. Social engineering is different in that it targets employees, not the network itself. Since worker mistakes and misbehavior are the leading cause of data breaches, this method can be painfully effective social engineering attacks are typically more psychological than they are technological. Instead of using sophisticated hacking techniques or in-depth knowledge of computers, they rely on tricking people into giving away information [5].

The most commonly used SE techniques are,