# Social Engineering "People Hacking"

For the computer science majors who can talk to people



## What is Social Engineering?

Social engineering refers to all techniques aimed at talking a target into revealing specific information or performing a specific action for illegitimate reasons.



# Examples





https://youtu.be/GyvRamX1 VyA



https://youtu.be/GyvRamX1 VyA



#### **PHISHING**

01

#### **Spear Phishing**

Targeting a specific individual in an organization

02

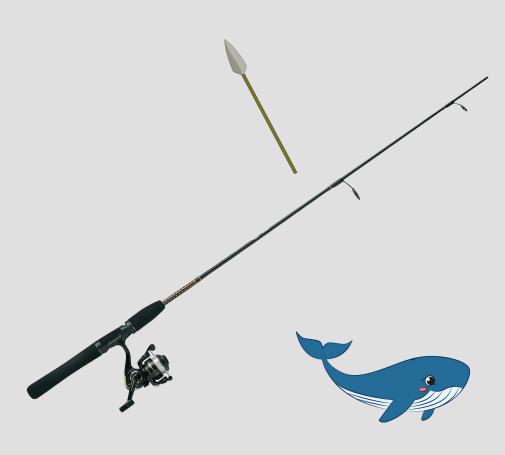
#### Whaling

Targets a senior executive

03

#### **Email/Smishing**

Phishing via Email or SMS





# Who would ever fall for that?

More people than you think

Phishing statistics show that in 2022, there were **300,497** phishing victims with a total loss of **\$52,089,159** in the U.S. alone.

-Forbes Advisor (data from FBI)

**3.4 billion** phishing emails are sent every day.



# Who Else?

## **Smishing**

Smishing is a term used to describe phishing attempts and scams that use text messages or (Short Message Service) SMS as the primary attack platform.

Scam types vary, but they will all attempt to rope you in with lucrative offers (like free prize money from a reputed retailer); attempt to get you to divulge information or take action (by pretending to be a friend or family member in need); or dangle fake information about a transaction or account (like a package delivery).

-Verizon

### The Experiment

- Create a fake, believable service number (989) 899-8986
- Text acting as a 2FA code
- Record results

Your Snapchat 2-Factor Authentication Code:

500371

\_\_\_\_\_

If you did not request this, respond "NOTMF"

### **Statistics**

24
Sent Texts



