# Social Engineering

# Topics

- What is Social Engineering ?
- Types of Social Engineering .
- How to protect from Social Engineering Frauds?

# What is Social Engineering?

- **Social Engineering** is the art of **manipulating people** so they give up **confidential information**.
- When individuals are targeted, the criminals are usually trying
  - to trick them into giving them their passwords or bank information,
  - access their computer to secretly install malicious software–that will give them access to their passwords and bank information as well as giving the hackers control over their computer.

# Why Social Engineering is easy?

- Criminals use social engineering tactics because
  - They **do not need any technical skills** for hacking computers or acquiring any sort of information.
  - it is usually easier to **exploit people's natural inclination** to trust than it is to discover ways to hack their software

# How Is Social Engineering Dangerous?

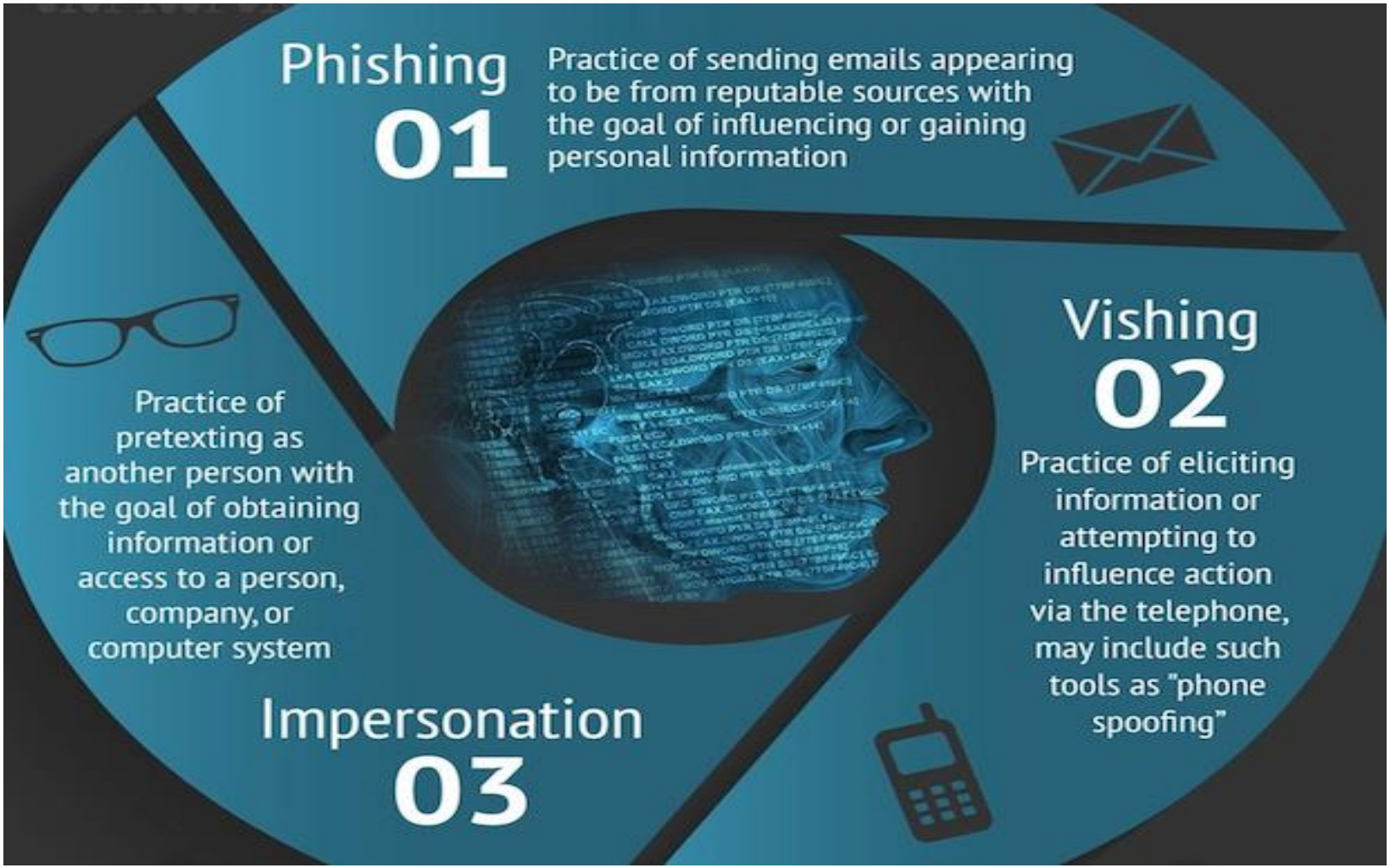
- Possible **identity theft** (bank account numbers, social security numbers, user ids/passwords, etc.)
- Possible all kinds of **data theft**
- Possible **corruption of data**
- Possible unplanned **system downtime**
- Possible (physical) **security threat**

# What are the benefit of Learning about SE?

Advantages of knowing social engineering techniques:

- Prevents unauthorized access
- Prevents possible information theft
- Prevents possible identify theft
- Prevents the possibility of downloading malicious software on unsuspecting user systems
- Preserves the integrity of information systems

# Common Social Engineering attacks



# What is Phishing?

- Phishing is the process of **obtaining personal information** from someone—such as credit card numbers, social security details, or login credentials to a protected system—**via fraudulent emails meant to look authentic.**
- They can appear to be sent from a person's school, bank, personal doctors, etc. Within companies, they often look like they're from the CEO or another higher-up, or the organization's technical support department.
- These emails contain fake links that take users to submission forms, where they're asked to enter their information. This is then sent to the scammers, who use it to hack employees' accounts, steal credit card info, carry out identity theft, and more.

# Types of Phishing

- There are two main types of email phishing:
- **Spear phishing** is a targeted attack at a **specific individual** (like spearing one fish), in the hopes of obtaining their information for identity theft, credit card use, etc.
- **Whaling** refers to scams **targeting people within a business or government** office, with the hopes of using that person's credentials to hack the system and obtain several users' or consumers' data at once (like fishing with a net).

# Email Phishing

**Email from a friend.**

*These messages may use your trust and curiosity.*

- **Contain a link** that *you just have to check out*–and because the link comes from a friend and you're curious, you'll trust the link and click–and be infected with malware so the criminal can take over your machine and collect your contacts info and deceive them just like you were deceived.
- **Contain a download**–pictures, music, movie, document, etc., that has malicious software embedded. If you download–which you are likely to do since you think it is from your friend–you become infected. Now, the criminal has access to your machine, email account, social network accounts and contacts, and the attack spreads to everyone you know. And on, and on.

# Email Phishing

- **Urgently ask for your help**–your 'friend' is stuck in country X, has been robbed, beaten, and is in the hospital. They need you to send money so they can get home and they tell you how to send the money to the criminal.
- **Asks you to donate to their charitable fundraiser, or some other cause** – with instructions on how to send the money to the criminal.

# Example 1: Email Phishing

---

From: "INDIANA.EDU SUPPORT TEAM" <supportteam01@indiana.edu>
Reply-To: "INDIANA.EDU SUPPORT TEAM" <spupportteam@info.lt>
Date: Sat, 12 Jul 2008 17:42:05 -0400
To: <"Undisclosed-Recipient:;"@iocaine.uits.indiana.edu>
Subject: CONFIRM YOUR ACCOUNT

Dear INDIANA.EDU email Subscriber

This mail is to inform all our {INDIANA.EDU} users that we
will be maintaining and upgrading our website in a couple of days from
now.As a Subscriber you are required to send us your Email account
details to enable us know if you are still making use of your
mailbox. Be informed that we will be deleting all mail account that is
not functioning to enable us create more space for new students and
staffs of the school, You are to send your mail account details which
are as follows:

*User Name:
*Password:
*Date of birth:

Failure to do this will immediately render your email address deactivated from our database.

Thank you for using INDIANA.EDU
FROM THE INDIANA.EDU SUPPORT TEAM

---

# Example 2: Document Delivery Platforms

- Document-sharing has simultaneously expanded and simplified the business world, but it was only a matter of time before con artists wedged their way into it too.
- Networks like Dropbox, Google Docs and others have seen breaches of security in recent months that compromised users' privacy, spread malware, and more.

# How to protect yourself or organization from Phishing Frauds?

- setting your privacy settings on social media to include only people you know in real life, and
- observing emails carefully to gauge their authenticity.
  - The once-obvious warning signs of typos,
  - unofficial-looking documents, and
  - false URLs.

# What is a Phishing Test?

- A phishing test allows you to find out if your team is vulnerable to attacks before they happen, and take the proper measures to decrease that susceptibility.

Some findings:

- One study found that 31% of the 11,542 employees tested (across 400 organizations) clicked the links in the test email, and 17% entered the requested information.
- 26% and 45% of employees at three companies in their case study were prone to phishing.
- What's even more shocking than these numbers? The fact that 94% of users believe they can recognize phishing attempts…yet nearly half of them still click on false links at some point.

# Vishing

- The most prevalent type of social engineering attack is conducted by phone. A hacker will ***call up and imitate someone*** in a position of authority or relevance and gradually pull information out of the user.
- Hackers are able to pretend they are calling from inside the corporation by playing tricks on the PBX or the company operator, so caller-ID is not always the best defense.

https://youtu.be/lwc9iU2MidQ

# Vishing

- Help desks are particularly vulnerable because they are in place specifically to *help*, a fact that may be exploited by people who are trying to gain illicit information.
- Help desk employees are trained to be friendly and give out information, so this is a gold mine for social engineering.
- Most help desk employees are minimally educated in the area of security and get paid peanuts, so they tend to just answer questions and go on to the next phone call. This can create a huge security hole.

# How to protect yourself or organization from Vishing Frauds?

There are steps you can take to avoid vishing scams. Some employ technical means, while others involve being proactive.

1. Never answer a call from an unknown number
2. If you do answer, never give personal information over the phone
3. Use a caller ID app
4. But don't completely trust caller ID
5. Treat vishing scams as you would smishing scams

# Smishing

**SMiShing** as "the act of using **mobile phone text messages (SMS)** to **lure victims** into immediate action such as downloading mobile malware, visiting a malicious website or calling a fraudulent phone number."

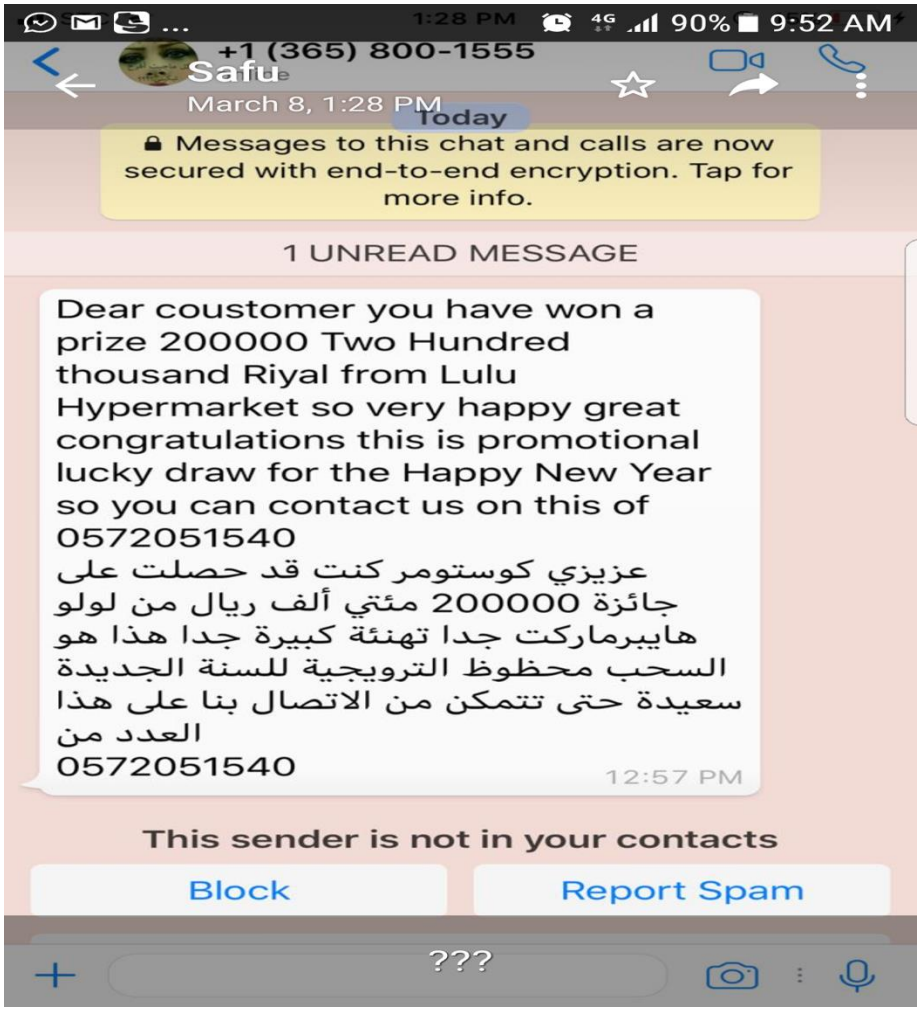
**SMiShing** messages are usually crafted to elicit an immediate action from the target, requiring them to hand over personally identifying information and account details. They will often do so by using fear or greed based terminology such as "**impending account suspension**," "**fraudulent account activity detected**," or by offering some type of **award or discount**.

# Smishing

- Cyber criminals will either **obtain a phone number from the dark web** following a data breach, through web crawlers checking social media posts or even through a random number generator. They'll then **send out text messages** asking users to call a number or click on a link. The messages scammers send often involve bank accounts, and in some cases, may even contain most or all of a potential victim's credit card or bank account number.

# Example 1: SMiShing Tactics by offering some type of prize

Many users won't think twice before acting when they receive a message from any organization.



# Example 2: SMiShing w.r.t. Financial Institutions

Due to the fact that more and more users are conducting banking transactions through smart phones, many SMiShing messages claim to be from a financial institution. Many users won't think twice before acting when they receive a message from their bank. Attackers will use legitimate sounding verbiage and even some branding to assist their pretext.


Image via Numbercop
http://numbercop.tumblr.com/post/120439546107/weekly-summary-518-531

# How to protect yourself or organization from SMiShing Frauds?

- The best way to educate users against SMiShing attacks is by **conducting simulated attacks** as part of your **security awareness** and training program. This provides the opportunity to train an individual how to respond to and prevent future threats.
- Simulated attacks can lead to educational pages that allow the moment an employee behaves badly to be a teachable moment.

# Impersonation

- **Impersonation** is defined as the "practice of pretexting as another person with the goal of obtaining information or access to a person, company, or computer system."
- Two common attack vectors are impersonating a
  - ***Delivery person*** or
  - ***Tech support***.

# Impersonation-Delivery Person

- Impersonating a delivery person is an effective and easy attack because not much acting is required. Usually, the hardest thing about impersonating a delivery person is looking the part and having all your credentials, papers, and “deliveries” in order.
- For example, someone dressed as a Ministry of Interior employee is automatically trusted, since they are an employee for the Saudi government. They can typically walk in and out of a building with few restrictions and sometimes are even allowed into secure areas to deliver packages with little to no questions asked. This is a perfect attack vector for a criminal to take since trust is already built into the uniform.

# Impersonation - Tech Support

- A person who uses social engineering to impersonate a tech support worker can have devastating effects on a network.
- One of the reasons for its effectiveness is because it can give an attacker *physical* access to network computers. It only takes a matter of seconds for someone to compromise a computer with physical access.

# Impersonation - Tech Support

- Gaining physical access to a computer through technical support is the best-case scenario for an attacker since it puts them right at the computer. This is a perfect opportunity to download an “anti-virus” program or some sort of scanner to “clean” the computer. Once the “helping” file is installed, it creates an opportunity for the attacker to infect the computer so they can gain further access to other computers or to the network.

# Common Social Engineering attacks

## Dumpster Diving

**Dumpster diving,** also known as **trashing,** is another popular method of social engineering. A huge amount of information can be collected through company **dumpsters.**

These sources can provide a rich vein of information for the hacker. **Phone books** can give the hackers **names and numbers** of people to target and impersonate.

**Organizational charts** contain information about people who are in **positions of authority** within the organization.

# Common Social Engineering attacks

**Dumpster Diving**

**Memos** provide small tidbits of **useful information** for creating authenticity.

**Policy manuals** show hackers **how secure** (or insecure) the **company** really is.

**Calendars** are great – they may tell attackers which employees are out of town at a particular time.

**System manuals,** sensitive data, and other sources of **technical information** may give hackers the exact keys they need to unlock the network.

Finally, **outdated hardware**, particularly **hard drives**, can be **restored** to provide all sorts of useful information.

# How to Avoid SE frauds?

- Secure your computing devices
- Set your spam filters to high
- Beware of any download
- Delete any request for financial information or passwords


# How to Avoid SE frauds?

- **Slow down.** Spammers want you to act first and think later. If the message conveys a sense of urgency, or uses high-pressure sales tactics be skeptical; never let their urgency influence your careful review.
- **Research the facts.** Be suspicious of any unsolicited messages. If the email looks like it is from a company you use, do your own research. Use a search engine to go to the real company's site, or a phone directory to find their phone number.
- **Delete any request for financial information or passwords.** If you get asked to reply to a message with personal information, it's a scam.

# How to Avoid SE frauds?

- **Reject requests for help or offers of help.** Legitimate companies and organizations do not contact you to provide help. If you did not specifically request assistance from the sender, consider any offer to 'help' restore credit scores, refinance a home, answer your question, etc., a scam.

  Similarly, if you receive a request for help from a charity or organization that you do not have a relationship with, delete it. To give, seek out reputable charitable organizations *on your own* to avoid falling for a scam.

# How to Avoid SE frauds?

- **Don't let a link in control of where you land.** Stay in control by finding the website yourself using a search engine to be sure you land where you intend to land. Hovering over links in email will show the actual URL at the bottom, but a good fake can still steer you wrong.
- Curiosity leads to careless clicking–if you don't know what the email is about, clicking links is a poor choice. Similarly, never use phone numbers from the email; it is easy for a scammer to pretend you're talking to a bank teller.

# How to Avoid SE frauds?

- **Email hijacking is widespread**. Hackers, spammers, and social engineers taking over control of people's email accounts (and other communication accounts) has become rampant. Once they control someone's email account they prey on the trust of all the person's contacts. Even when the sender appears to be someone you know, if you aren't expecting an email with a link or attachment check with your friend before opening links or downloading.
- **Beware of any download.** If you don't know the sender personally AND expect a file from them, downloading anything is a mistake.

# How to Avoid SE frauds?

- **Foreign offers are fake**. If you receive email from a foreign lottery or sweepstakes, money from an unknown relative, or requests to transfer funds from a foreign country for a share of the money it is guaranteed to be a scam.
- **Set your spam filters to high.** Every email program has spam filters. To find yours, look under your settings options, and set these high–just remember to check your spam folder periodically to see if legitimate email has been accidentally trapped there. You can also search for a step-by-step guide to setting your spam filters by searching on the name of your email provider plus the phrase 'spam filters'.

# How to Avoid SE frauds?

- **Secure your computing devices.** Install anti-virus software, firewalls, email filters and keep these up-to-date. Set your operating system to automatically update, and if your smartphone doesn't automatically update, manually update it whenever you receive a notice to do so. Use an anti-phishing tool offered by your web browser or third party to alert you to risks.