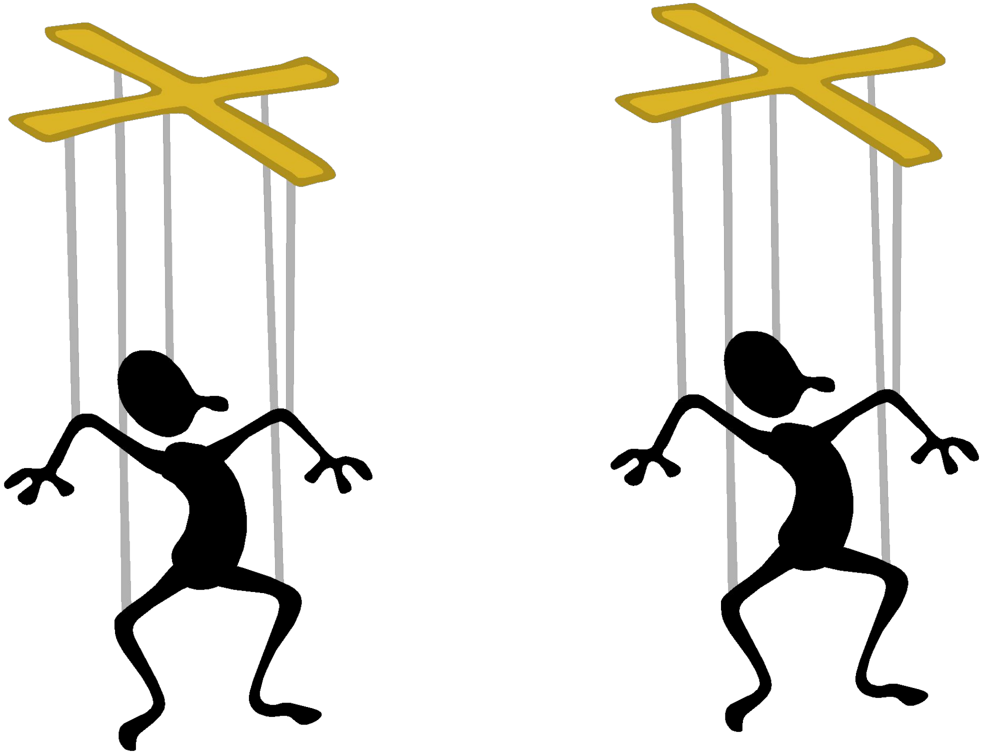
CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

Computer Security Principles

Lecture 6: Social Engineering

What is Social Engineering?

"The art and science of getting people to comply with your wishes"



So What is the Problem?

- An outsider's use of psychological tricks on legitimate associates, in order to obtain information needed to gain access to a facility or system
- Buildings, computers, networks and software applications have been hardened – The human being has become the **weak link** in security
- Getting needed information (for example, a password) from a person rather than breaking into a system

Social Engineering involves gaining sensitive information or unauthorised access privileges by building ***inappropriate trust relationships*** *with insiders.*

How does it work?

- Social engineers leverage trust, helpfulness, easily attainable information, knowledge of internal processes, impersonation of authority, technology
- Often **use several small attacks** to reach their final goal.
- Social engineering is all about taking advantage of others to gather information and to infiltrate an organisation.

Here are some examples

- Posing as a legitimate end-user
- The irate Vice President
- A published security vulnerability
- Posing as a **system administrator**
- Calling in looking for someone or specific information
- Use of Search engines to glean information about a company and its associates

Let’s Review Their Techniques

- Pretexting
- Phishing
- Spear Phishing
- IVR/Phone Phishing
- Trojan Horse
- Shoulder Surfing
- Dumpster Diving
- Road Apples
- Quid pro quo – Something for something

Pretexting

- Pretexting is the act of creating and using an **invented scenario** (the pretext) to persuade someone to release information or perform an action and is typically done over the telephone.
- It often involves some prior research or set up and the use of pieces of known information (e.g. for impersonation: date of birth, PPS number, last bill amount) to **establish legitimacy** in the mind of the target. Often used by private investigators to gain copies of personal records

Pretexting

- This technique is most often used to trick a business into **disclosing customer information**.
- Pretexting can also be used to impersonate co-workers, police, bank, tax authorities or insurance investigators — or any other individual who could have perceived authority or **right-to-know** in the mind of the company who is being contacted.
- **Voice over IP** programs are starting to become a standard in pretexting, as it is harder to track an IP address than a phone number, making the pretexter less vulnerable to capture.

Phishing

- Usually involves email but phone calls can be used
- They appear to come from a **legitimate business** – one you use
- They include a **sense of urgency**
- There is usually a threat to your personal safety or security
- You are asked to **verify personal data**
- Banks and other Credit Card Shopping sites are frequent targets

Spear Phishing

- Spear phishing is any **highly targeted** email or telephone scam; but they usually are employed in a business environment.
- Spear phishers send email messages or make calls that **appear genuine** to all the associates or members within a certain company, government agency, organization, or group.
- The message might look like it comes from your company or agency, or from a colleague who might send an email message to everyone in the company, such as the head of HR.
- It might include requests for user names or passwords or might contain **malicious software**, like a Trojan or a virus.

IVR/Phone Phising

- This technique uses a **rogue Interactive voice response (IVR)** system to recreate a legitimate sounding copy of a bank or other institution's IVR system.
- The victim is prompted (typically via a phishing email) to call in to the "bank" via a provided (ideally toll free) number and **verify information**.
- A typical system will continually reject logins ensuring the victim enters PINs or passwords **multiple times**, often revealing several different passwords.
- More advanced systems will even transfer the victim to the attacker posing as a customer service agent for further questioning.

Trojan Horse

- Uses your curiosity or greed to deliver “malware”.
- Arrives **posing as something free**
  - Attached to email
  - Screen Saver
  - An important Anti-Virus or system upgrade
  - Latest gossip about someone
- Opening attachment loads Trojan onto your computer
  - Tracks keystrokes, uploads address book, looks for financial software files

Shoulder Surfing

- Prevalent in aircraft, airports, coffee shops, public Wi-Fi areas in hotels, other public places.
- Use of phone/laptop cameras very prevalent
- Observation discloses your logins and passwords.
- Disclosure of credit cards and other High Risk Data.
- Confidential materials can be disclosed.
- Bank ATMs, security locks, alarm keypads.
- Includes "**piggy backing**" – someone walking into a secure area based on your authentication.

Dumpster Driving

- Dumpster diving is the practice of sifting through commercial or residential **trash** to find items that have been discarded by their owners, but which may be useful to the Dumpster diver.
- What do they want?
  - Confidential Information, PII and credit card data
  - Banking information – blank credit applications
  - A phone list
- It is not unusual for security to catch people going through trash bins.

Cross-cut shred all confidential information.

Road Apples

- A road apple is a **real-world variation of a Trojan** Horse that uses physical media and relies on the curiosity of the victim.
  - CD, floppy, USB Flash Drive
- The attacker leaves a malware infected floppy disc, CD ROM or USB flash drive in a location sure to be found, gives it a legitimate looking and interesting label, and simply waits.
- Once placed into PC to view, the "**autorun**" feature loads Trojan or virus to track keystrokes
  - Looks for IDs and passwords

Quid pro quo

- The Something for Something Scam
- Two Examples:
  - Impersonation of a Help Desk
  - **Gift in exchange for Information**
- Surveys continually show that people are willing to trade private information for relatively low value
  - Chocolate lure
  - Cheap pen
  - Surveys themselves

Other Types of Social Engineering

- Because free email services are so popular, it is easy for criminals to create programs that automatically generate millions of combinations of email addresses, knowing that statistically, they will get many that are valid.
- One point to remember is to **never opt-out of a bogus email** as this just validates the email .
- Need to find a free wireless? Any college student can open a laptop in the area and name it "**Free Wi-Fi**" If it is peer-to-peer, you just connected directly to someone else's computer. They can load a Trojan, virus or even pull files.

Other Types of Social Engineering

- Web sites are open to the world.
- **Web crawling** is the term used to describe how Google, Yahoo and other search engines gather all of their information.
- Criminals can crawl websites too. They are looking for email addresses and other information so they can send you an email that looks legitimate.
- Know how to tell a good Universal Resources Locator URL from a bad one. A simple technique is to direct you to your bank or other key site via a **proxy**, a site that will monitor what you are typing and steal your data.
- ATM Fraud

So What is the Risk?

- It takes only **one unsuspecting person** to defeat a company’s system security. One person who is tricked into releasing their login and password.
- Social Engineering is based on **gaining trust** – for service oriented companies, this is a risk – Associates are trusting and want to help
- Social Engineers are after an associate’s **access rights** - either physically to a building or to a software system.
- What can a criminal do if they have access to everything you have at work?

What can you do?

- Never share passwords – **NEVER, NEVER, NEVER**
- Use different passwords for personal and business matters.
- **Don’t discuss company confidential matters in public**.
- Shred company confidential information.
- Found CD’s, USB thumb drives? Don’t use them.
- Know how to spot a phish – beware of email attachments.
- **Never use a link within an email** or call a phone number from within an email – look up the organisation independently.
- Don’t forward or respond to unsolicited email, chain letters and other hoaxes.
- **Screen lock your computer** when you walk away.
- Don’t let strangers into secure areas – let them use their badge – **door coasting is the easiest way in**!
- Don’t share confidential information with strangers over the phone.

Footprint on Web

- While it's exciting to live in an ever connected and always on world, the flip side that we have to accept is that we also live in a world where **information is becoming increasingly interlinked**.
- Today it is relatively simple to follow footprints on the Web if we want to track both people and brands.
- **No delete button** on web.
- While the information about me on the Web is not terribly exciting, I do leave a little bit of information on every site I visit.
- Say something in passing on a social site and it may come back to haunt you.

Footprint on Web

What is digital footprint ?

- A digital footprint is the **collection of all the traces** you leave in electronic environments as you use or move through them.
- Some is content you **actively volunteer**—like your Facebook profile.
- Other material is **passive**—the cookies a site stores in your browser, the content your distro collects about your use of their equipment, etc.
- All this data can be **aggregated** to build a profile of you and your behaviour.

Footprint on Web

Pair up and answer the following questions:

- If we were to look you up online what would we learn about you?
- What are your digital footprints?
- Is there anything online that you wouldn't want your employer or parent to know about you?

Table Quiz Questions

1) What is your understanding of **Social Engineering**? Discuss **4** techniques used in Social Engineering.
2) What is a Botnet? Discuss 2 possible uses of Botnets.
3) Discuss the difference between **Polymorphic** and **Metamorphic** viruses.
4) Describe 3 techniques used in Anti-virus software.