Cabrillo College

Personal Information Security Basics

Session 2: Social Engineering and Physical Safety for Your Data

https://github.com/infosecirvin/pisb

About Your Instructor...

Irvin Lemus

Cybersecurity Professor; Computer Information Systems Department
Bay Area Cyber Competitions Regional Coordinator

irlemus@cabrillo.edu (831) 479-6296
@infosecirvin

Topics For Today

Social Engineering Introduction

Phone Call Attacks and Scams

Personalized Scams

Disposing of Your Mobile Device

Excerpt from CIS 76

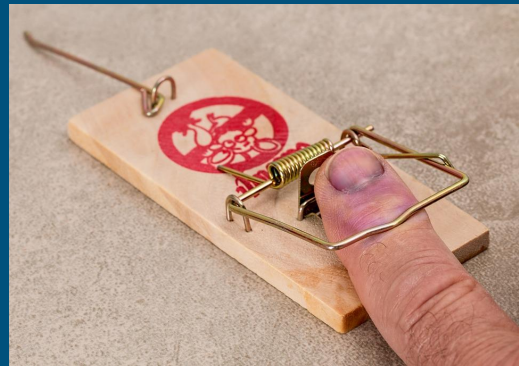
Activity: Social Engineering Attack

All topics come from SANS OUCH! Newsletter

Social Engineering Introduction

Social Engineering Intro

- Common misconception is cyber attackers only use highly advanced tools and techniques to hack into computers or accounts
  - NOT THE CASE
- The easiest way to steal information, accounts or infect systems is simply manipulating you into making a mistake



What is Social Engineering?

- Psychological attack tricking you into doing something you should not do
  - Old concept (con artists)
- Today's technology makes these attacks more effective for the attacker because you can't see them
  - Allows them to pretend to be anyone/thing and target millions around the world
  - Social Engineering bypasses many security technologies

Example 1

- You receive a phone call from someone claiming to be from a computer support company, ISP, or Microsoft Tech Support
- Caller explains your computer is actively scanning the Internet and believe it is infected
  - Use variety of technical terms to take you through confusing steps to convince you
  - Find files on your computer as proof your computer is infected
    - Even though the files they point out are common files

Example 1

- Caller pressures you to buy their security software or give them remote access to your computer to fix
  - They have fooled you to infect your system and paid them
  - You gave them full access to your system to steal your data to use it for their bidding

Detecting/Stopping Social Engineering Attacks

- Someone creating a tremendous sense of urgency. They are attempting to fool you into making a mistake.
- Someone asking for information they should not have access to or should already know, such as your account numbers.
- Someone asking for your password. No legitimate organization will ever ask you for that.

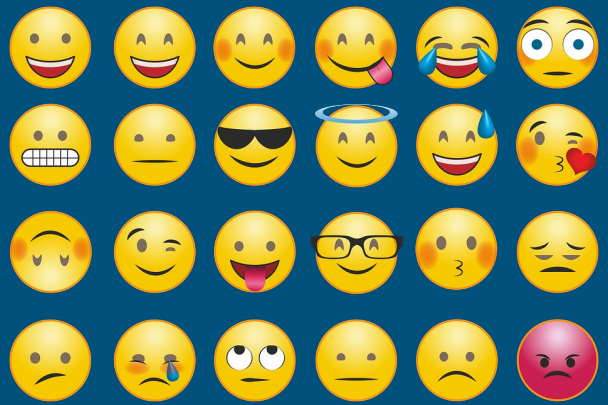
Detecting/Stopping Social Engineering Attacks

- Someone pressuring you to bypass or ignore security processes or procedures you are expected to follow at work.
- Something too good to be true. For example, you are notified you won the lottery or an iPad, even though you never even entered the lottery.
- You receive an odd email from a friend or coworker containing wording that does not sound like it is really them.
    - A cyber attacker may have hacked into their account and is attempting to trick you. To protect yourself, verify such requests by reaching out to your friend using a different communications method, such as in person or over the phone.

Phone Call Attacks and Scams

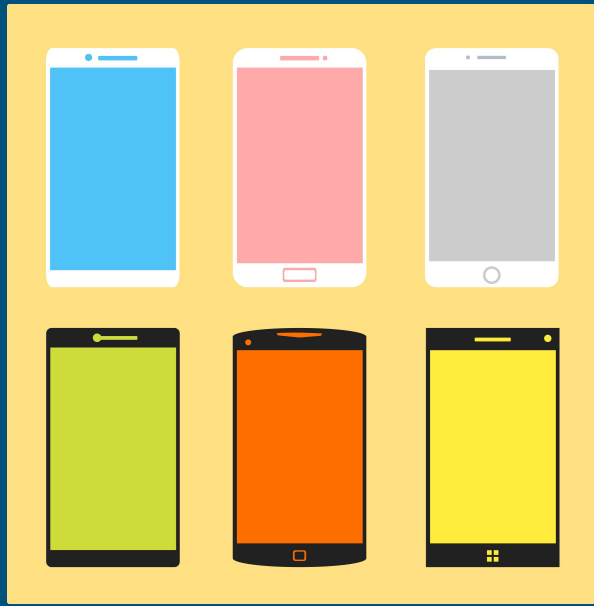
Phone Attacks and Scams

- Many of today's cyber criminals use phones to trick their victims
  - Fewer security technologies that monitor phone calls and detect/stop attacks
  - Easier for bad guys to convey emotion over phone and successfully trick victims



How do Phone Call Attacks Work?

- What are they after?
  - Money, information, access to computer, all of the above
  - Trick you into doing what they want
- Methods of attacks
  - Urgency
  - Get you off balance so you don’t think clearly
  - Rush you into a mistake



Example 2

The caller pretends that they are from a government tax department or a tax collection service and that you have unpaid taxes. They explain that if you don’t pay your taxes right away you will go to jail. They then pressure you to pay your taxes with your credit card over the phone. This is a scam.

Many tax departments, including the IRS, never call or email people. All official tax notifications are sent by regular mail.

Example 3

The caller pretends they are Microsoft Tech Support and explain that your computer is infected. Once they convince you that you are infected, they pressure you into buying their software or giving them remote access to your computer.

Microsoft will not call you at home.

Example 4

You get an automated voicemail message that your bank account has been canceled, and that you have to call a number to reactivate it. When you call, you get an automated system that asks you to confirm your identity and asks you all sorts of private questions.

This is really not your bank, they are simply recording all your information for identity fraud.

Protecting Yourself

- Anytime anyone calls you and creates a tremendous sense of urgency, pressuring you to do something, be extremely suspicious. Even if the phone call seems OK at first, but then starts to feel strange, you can stop and say no at any time.
- If you believe a phone call is an attack, simply hang up. If you want to confirm if the phone call was legitimate, go to the organization's website (such as your bank) and get the customer support phone number and call them directly yourself. That way, you really know you are talking to the real organization.

Protecting Yourself

- Never trust Caller ID. Bad guys will often spoof the caller number so it looks like it is coming from a legitimate organization or has the same area code as your phone number.
- Never allow a caller to take temporary control of your computer or trick you into downloading software. This is how bad guys can infect your computer.
- If a phone call is coming from someone you do not personally know, let the call go directly to voicemail. This way, you can review unknown calls on your own time. Even better, you can enable this by default on many phones with the “Do Not Disturb” feature.

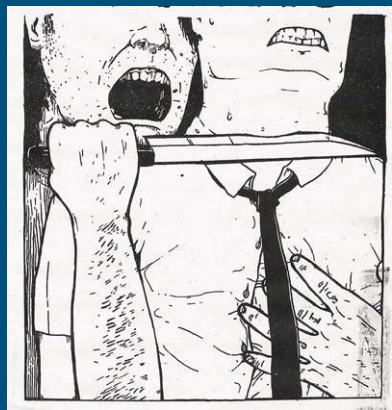
Personalized Scams

Overview

- Cyber criminals continue to come up with new, creative ways to fool people
- Criminals find or purchase information about millions of people, then use that information to personalize their attacks

How Does It Work?

- Criminals do research and create customized messages
  - They purchase databases with names, passwords, phone numbers, etc
- This (usually) valid information is then used against victims in order to create fear and add extra claims (i.e have records of your web history)
- They threaten to release the information to your friends and family if you do not pay their extortion fee

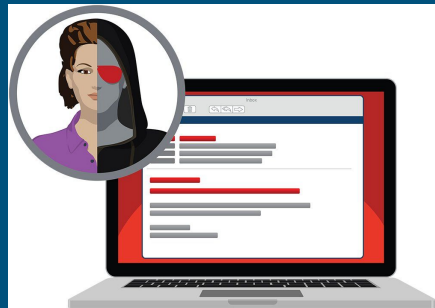


What Should I Do?

- Remember, the sender is lying while using information they acquired
- Attacks like these are normally part of an automated mass-scale campaign, not directed to you
- Attacker only has a few pieces of information, some of which can be changed
- Staying suspicious to new and unknown messages will keep you centered against their attempts to get you off balance

What is CEO Fraud/BEC?

- Business Email Compromise
- Research the victim in order to target the company
  - If you're the target
    - They would research your boss or other superiors/co-workers
    - Craft emails pretending to be someone you know with the same tactics listed before
      - Urgent, take action, reply with sensitive documents, pressure you to take action
- Consistent training for all employees against the threats of attackers against your company is vital



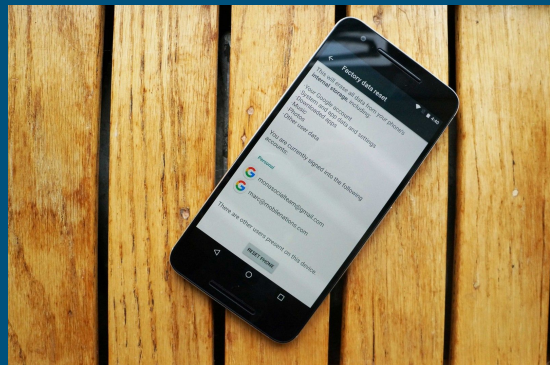
Disposing of Your Mobile Device

Overview

- As Mobile Devices advance and innovate, people replace their phones as frequently as every year
  - Not realizing how much personal data is stored in these devices
- Your Information
  - Where you live, work, and places you visit
  - The contact details for everyone in your address book, including family, friends, and co-workers
  - Phone call history, including inbound, outbound, voicemail, and missed calls
  - Texting or chat sessions within applications like secure chat, games, and social media
  - Web browsing history, search history, cookies, and cached pages
  - Personal photos, videos, and audio recordings
  - Stored passwords and access to your accounts, such as your bank, social media, or email
  - Health related information, including your age, heart rate, exercise history, or blood pressure

Wiping Your Device

- Regardless how you dispose of your device, deleting data is not enough
- Easiest way is reset your device
  - Steps vary by manufacturer
    - Apple iOS Devices: Settings | General | Reset | Erase All Content and Settings
    - Android Devices: Settings | Privacy | Factory Data Reset
- Enable Encryption on your device before resetting it
  - Ensures data is unreadable after reset

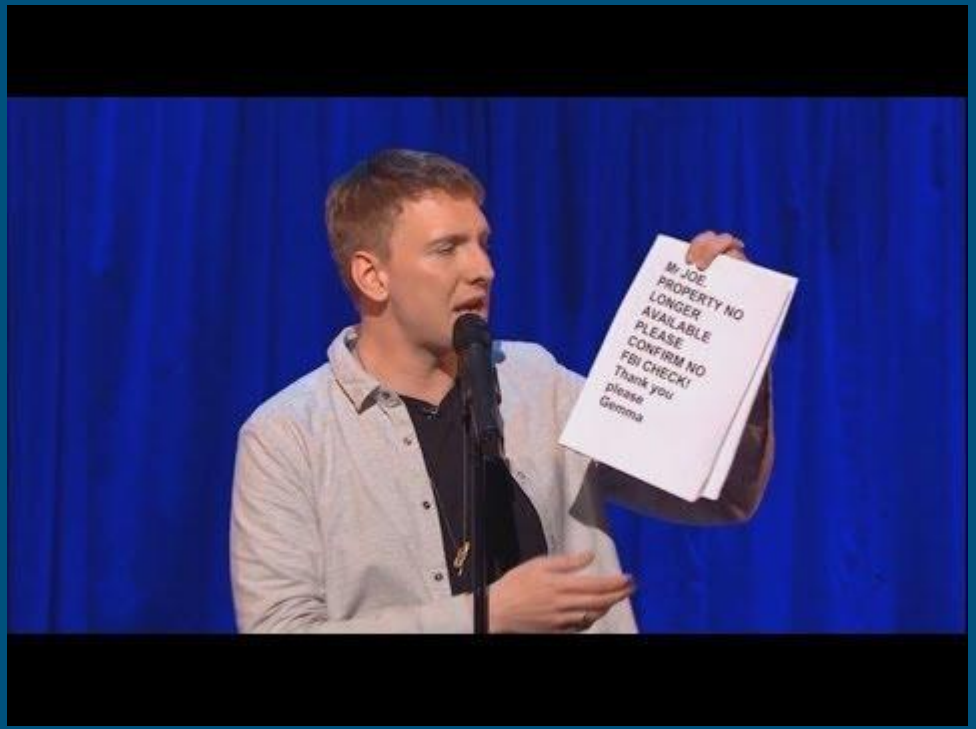


SIM & External Cards

- Subscriber Identity Module (SIM) card
  - Mobile devices uses this to make cellular and data connections
  - SIMs retain your account information even when phone is reset
  - Talk to service provider about transferring your SIM card
    - If not possible, keep or physically destroy old SIM cards
- External Cards
  - Some devices have an SD (Secure Digital) card for additional storage
  - As with SIM cards, they are not automatically wiped on a phone reset
  - Also as with SIM cards, if reusing the card is not possible, the recommendation is to physically destroy the card.

Excerpt from CIS 76: Ethical Hacking

Scamming a Gumtree Scammer: Joe Lycett



Preying on Human Weakness

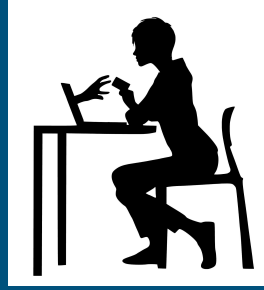
- Worker's lax attitude towards maintaining secrecy of sensitive information makes this a serious threat

Type	Behavior	Example
Reciprocation	Someone is given a token and feels compelled to take action.	You buy the wheel of cheese when given a free sample.
Consistency	Certain behavior patterns are consistent from person to person.	If you ask a question and wait, people will be compelled to fill the pause.
Social Validation	Someone is compelled to do what everyone else is doing.	Stop in the middle of a busy street and look up; people will eventually stop and do the same.
Liking	People tend to say yes to those they like, and also to attractive people.	Attractive models are used in advertising.
Authority	People tend to listen and heed the advice of those in a position of authority.	"Four out of five doctors recommend . . ."
Scarcity	If something is in low supply, it becomes more precious and, therefore, more appealing.	Furbees or Sony Playstation 2.

Human Based Social Engineering

- **Posing as Legitimate End User** - via reciprocation, favor begets a favor
- **Posing as an Important User** - via intimidation, perceive to be authority
- **Posing as Technical Support** - via consistency, give end user instructions OR as end user to Technical Support, reciprocate urgency and helplessness to gain access

Human Based Social Engineering



- **Eavesdropping** - in person, audio, video, written, network sniffing
- **Shoulder Surfing** - in person covert watching from a distance
- **Dumpster Diving** - going through trash to find information
- **In-Person Attack** - disguised as techs, custodians, etc., physically survey victim

Human Based Social Engineering

- **Third-Party Authorization** - represent themselves as agents authorized by an authority figure to obtain information on their behalf
- **Tailgating** - unauthorized person follows closely someone who is authorized into a building
- **Piggybacking** - unauthorized person convinces an authorized person to allow him/her into secured area

Computer Based Social Engineering

- Computer based social engineering uses software to retrieve information

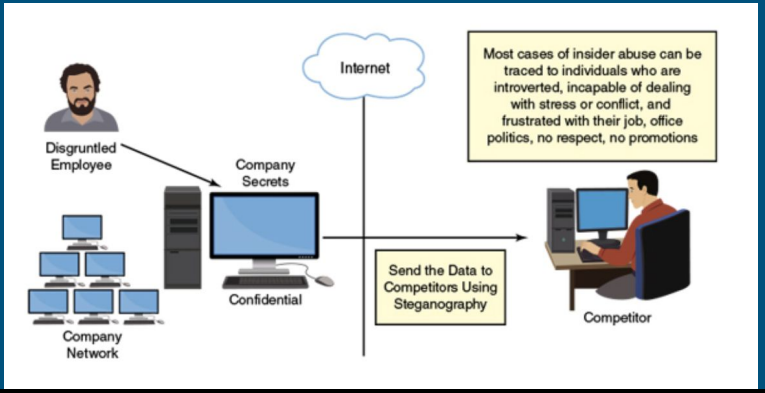
Attack Goals	Description	Cost
Theft of personnel information	Hacker requests staff member's personal information.	Confidential information, money
Download malware	Hacker tricks a user into clicking a link or opening an attachment.	Business availability, business credibility
Download hacker's software	Hacker tricks a user into clicking a link or opening an attachment.	Resources, business credibility, money

Computer Based Social Engineering

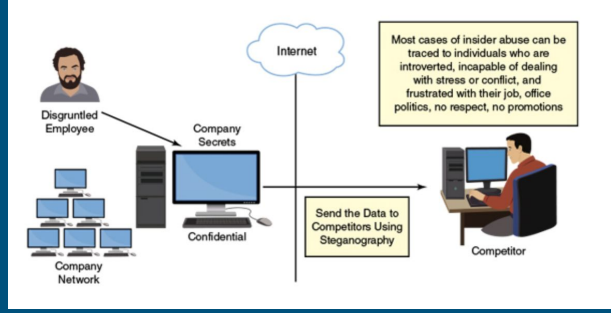
- Pop-Up Windows
- Email Attachments
- Web Sites
- Instant Messenger
- Phishing

Insider Attack

The scariest of all social engineering attacks is the one from the inside

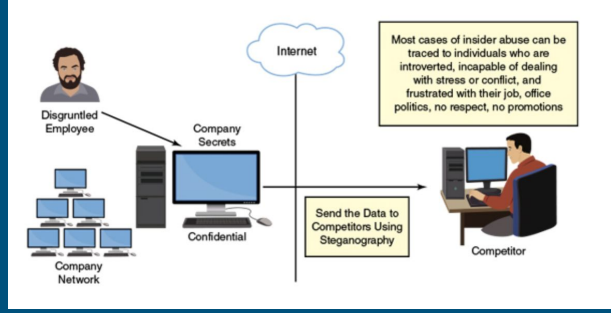


Preventing Insider Attack



- Separation of Duties - divide responsibilities among various employees, so if attack occurs, it will be limited in scope
- Rotation of Duties - single duty allotted to different employees at different times so malicious user does not damage entire system
- Restricting Privileges - Least Privilege Principle

Preventing Insider Attack



- Controlling Access - Implement ACLs
- Logging and Auditing - check if resources are misused
- Legal Policies - enforce policies to prevent theft of sensitive data
- Archiving Critical Data - backup what’s important

Social Engineering Defense

- Constant User Training and Education
  - Persuasion is powerful
- Users must feel comfortable escalating confrontational situations
- Could have Service Desk be the single point of contact
  - But must emphasize training on Service Desk to keep company information private and not be so open and willing to work with whomever calls

Social Engineering Defense

- Social Engineering is an art and science of getting people to comply with attacker’s wishes
- No one method can guarantee complete security against social engineering
- No hardware/software is available to defend against social engineering attacks

Activity

Social Engineering Attack

Please go to link and open the “trashdump.pdf” file.

Read through the contents; how will you socially engineer this person to get their information?

Cabrillo College

Personal Information Security Basics

Session 2: Social Engineering and Physical Safety for Your Data

https://github.com/infosecirvin/pisb