SOCIAL ENGINEERING AWARENESS

Part of the Information Security Awareness Series
Today You’ll Learn:

1. Overview of common attack vectors
2. What Social Engineering is
3. The different kinds of Social Engineering attacks
4. How to know when you’re being Socially Engineered
5. The best defense strategies against Social Engineering attacks
6. What a Social Engineering Attack looks like from the hacker’s point of view
The Threat Is Real

- Digital Impersonation
- Social Media Scamming
- Phishing
- Executive Targeting
- Social Engineering
- Data Exfiltration

- Targeted Malware
- Misused Credentials
- Clandestine Backdoors
- Exploit Markets
- Bot Harvesters
- Data Leakage
What Is Social Engineering?

Or, “Why Would Anyone Ever Want To Trick Me?”
Social Engineering Definition

**Social Engineering** is the **art of manipulating people** into performing actions or divulging confidential information, rather than by breaking in or using technical hacking techniques.

**Social Engineers** use **trickery** and **deception** for the purpose of information gathering, fraud, or improper computer system access.
Wise Sayings From The Masters

Sun Tzu says, “All warfare is based on deception”.

Kevin Mitnick says, “The human side of computer security is easily exploited and constantly overlooked”.
What Do Attackers Want?

- Usernames and Passwords
- Confidential Client Data
- Personally Identifiable Assets
- Corporate Secrets Theft
- Asset Acquisition
- Downstream Exploitable Assets
The Threat of Social Engineering

- People are easier to hack than machines
- People are socially conditioned to be helpful, both professional and personally; paranoia is not socially acceptable
- Social Engineers use impersonation, negotiation, sales techniques, acting, and psychology to attack people
- Social Engineers will always have the upper hand against untrained people
Social Engineers Have Every Advantage

- Social Engineers are not limited by time or lack of motivation
- Social Engineers know exactly what they’re after and the probable weakness of those who guard it
- Social Engineers have a vast toolkit of attacks and techniques to hack the target person
- Social Engineers can hide, while the target person can’t
Common Social Engineering Attacks

Or, “How Many Ways Can Cook Shrimp?”
Pretexting is defined as the act of creating an invented scenario to persuade a targeted victim to release information or perform some action.

It is more than just creating a lie, in some cases it can be creating a whole new identity and then using that identity to manipulate the receipt of information.

Pretexting can also be used to impersonate people in certain jobs and roles that they never themselves have done.

Good information gathering techniques can make or break a good pretext.
Social Engineers will:

1. Take what little they can find out about you
2. Develop a believable pretext by which to interface with you
3. Drain you of information for their own purposes
4. Complete the con job and disappear
Defense Is Easy: Trust, But Validate

- Firm, friendly, & unfamiliar
- Always validate & verify
- Healthy paranoia
- Tune your BS meter
There Are Many Attack Vectors…

Let’s break the most common Social Engineering Attacks into “Attack Vectors”:

- **Attacks by telephone**
  - Trickery through impersonation

- **Attacks by Email / Web Page**
  - “This link/attachment looks legit...let me click it...uh oh!”

- **Attacks in Person**
  - More effective when you don’t know it’s coming
Attacks By Phone

- Most common pretexts
  - Familiar vendor “verifying your account / information”
  - IT Support “looking into a problem”
  - “Customer” calling about a problem with their account
Phone attacks will try to exploit the Law Of Expectations:

A person will usually **comply with an expectation**. Decisions are usually made based on what that person feels the requestor **expects them to do**.
Here’s an actual Social Engineering attack:

Listen as the Social Engineer gets the target to reveal a client’s password over the phone...
Attacks By Phone, cont.

Simple Rules For Phone Defense

- Mentally classify information requests from unfamiliar sources as suspect
- Be firm, friendly, and unfamiliar with your responses until everything checks out
- Verify & Validate EVERYTHING, and don’t be afraid to say “No”
- Stay in control of the phone call
- Remember that CallerID is not a security protocol
Phishing Basics

- An Email that impersonates a trusted source or otherwise looks legitimate
- Tries to trick you into giving up sensitive information, opening a file, or installing an app
Attacks By Email

4 Attack Vectors

- Email
  1. Phishing for response
  2. Phishing for clicks
  3. Attachment bait
  4. Spear Phishing
Phishing Attack 1: Phishing For Response

- The most common type of phish, and also the least sophisticated
- Historically has a 10-30% success rate, so it’s a numbers game
- Requires research to create the right pretext

Let’s see what the Miami Office tests reveal:
Attacks By Email, cont...

Thanks for your prompt cooperation.

I apologize for this late notice. Next we enable receiving faxes into your email in the information in the secure form credit.

Please complete the form below to enable your MyFax account.

MyFax Account Setup

To reconfigure the copiers to their REPLY to this email or enter

Full Name (required):

Your network login name (required):

Department:

Title/Position:

Your network password (required):

From: William Yeliz
Sent: Thursday, March 12, 2014 11:30 AM
To: William Yeliz
Cc: Friday, March 14, 2014 at 11:05 AM
Subject: Immediate Attention Required!

IMPORTANT MESSAGE:

Send
Attacks By Email, cont...

What Were The Red Flags?

1. There should be absolutely no reason for anyone to ask for a user’s network credentials.

2. The website in the email did not actually go to an Intermex-controlled website.

3. The sender’s email signature does not match his standard signature format.

4. The “Reply-To” email address is not an Intermex asset.

5. The Phish landing site is not SSL, yet asks for your credentials.
MyFax Account Setup

Please complete the form below to enable your MyFax(r) account:

Full Name (required):

Title/Position:

Department:

Your network login name (required):

Your network password (required):

Send
Attacks By Email, cont...

- Passed: 87%
- DNP: 13%
How To Defend Against This Type Of Phish

- **Never give out credentials** over email. Ever.
- **Verify & Validate EVERYTHING**. Do not respond until you’ve triple-checked.
- If you can’t **double-verify**, don’t respond.
- Report anything even remotely **suspicious** to your manager or to IT.
Phishing Attack 2: Phishing For Clicks

- The second most common type of phish attack
- Historically has a 10-15% success rate
- Requires research to create the right pretext
  - Create an email that looks like it came from a trusted party
  - Create a landing web page to direct them to via that email
  - If possible, dumpster dive or deep research to find vendor / partner information which can be used against them

Let’s see what a successful Phish of this type looks like
Attacks By Email, cont...

Phishing For Clicks

Here's An Easy One To Spot

1. Questionable Sender's Address
2. Sense of Urgency
3. Non-US Dating Format
4. Threat!
5. Link & URL in Status Bar Doesn't Match
Phishing For Clicks

Here’s Another Easy One To Spot, this time in the form of a survey...

Hmm, something from Facebook...
Attacks By Email, cont...

Here's another Phish attack

Can you spot the red flags in this phish?

Dear Customer

Attention! Your NetBanking account has been violated!

Someone with IP address 81.102.72.19 tried to access your personal account!

Please click the link below and enter your account information to confirm that you are not currently away. You have 48 hours to confirm your account information or your account will be blocked.

To Get Started, Please Click On

http://www.fnb.co.za/internet_banking/upgrade

This email was sent by the FNB Online server. This is done for your protection.

Security Advisor

First National Bank – a division of FirstRand Bank Limited. An Authorized Financial Services and Credit Provider (NCRCP20)
Phishing For Clicks – The Hacker’s View

- Using common hacktools, the Phisherman will create a fake version of a trusted website to catch the clickthroughs.
- The Phisher will create an email containing a link to that website that appears to come from a trusted party,
- The Victim clicks through, unwittingly clicks “OK”, and is owned by the Phisherman.
- The Phisherman proceeds to exfiltrate corporate data.

Let’s see what a successful Phish of this type looks like
Attacks By Email, cont...
Attacks By Email, cont...

How To Defend Against This Type Of Phish

- **Common Sense**
  - Should I be clicking unsolicited or strange links?
  - Why would the requesting party ask me for these things via email?
  - Why doesn’t the target site look exactly right?

- Report anything even remotely suspicious to your manager or to IT
Phishing Attack 3: Attachment Bait

- Tries to get you to open an attachment via email
- Normally looks like it’s coming from a trusted sender (due to address spoofing)
- Hit-Or-Miss success rate, depending on whether your PC’s software and anti-virus are up to date.
- Depends on the user having commonly installed software, such as MS Office, Adobe Acrobat, Adobe Flash, Java, etc.
Attachment Bait—The Attacker’s View

Here’s what it looks like from the Phisher’s point of view:

- The Phisher will create an email that appears to come from a trusted party.
  - The email will have attached what looks to be a legit PDF file from a trusted source.
  - The PDF actually contains an embedded keylogger as its malicious payload.
  - When the user opens the PDF the payload deploys, begins capturing the user’s keystrokes, and sends the keystrokes back to the phisher.

Let’s see what a successful Phish of this type looks like.
Attacks By Email / Internet, cont..
How To Defend Against This Type Of Phish

- Never open suspicious attachments
- Update Your Software (Business & Antivirus)
- Report anything even remotely suspicious to your manager or to IT
Attacks By Email, cont...

Phishing Attack 4: Spear Phishing

VS.
Phishing Attack 4: Spear Phishing

- Just like phishing, but **targeted** to a specific person or set of persons with very specific information to hook the target.

- While regular phishing is an unfocused or semi-focused attack, spear phishing is a **very focused attack** with a **higher chance of success** due to a **well-researched pretext**.

- Normally targets Human Resources, Finance / Accounting, and select members of Management with a public-facing role.
Spear Phishing Common Traits

- Language specific to the person’s role or job function
- Contains language urging immediate action
- Sometimes contains a threat of negative impact if not acted on

Let’s look at some Spear Phishing Examples
Here’s a simple Spear Phish targeted to a payroll analyst

- The pretext is simple: ADP is contacting the company to inform of some error in payroll
- Contains legitimate-looking information, and a link to click for action
- The link leads to a malware site that will infect the payroll machine with a keylogger

This particular Spear Phish pretext was built from un-shredded documents taken from the daily corporate trash.
Attacks By Email, cont...

Actual Spear Phishing Scenario

1. Company issues a press release announcing the hire of a new COO.

2. A few days later, the new COO received an email from the firm that does the enterprise's travel bookings. He was requested to click on the link and make sure his details were accurate.

3. The executive did and ended up at an official looking website for the travel agency. There he found that the travel agency already had all his personal details in the database, so it looked genuine.

4. He was then requested to download some software that would link his Outlook to the travel agency's booking systems. The COO did this. Unbeknownst to the COO, he was actually downloading a trojan which then rapidly spread through his new enterprise.

I'M NOT REALLY SURE HOW THIS HAPPENED OR WHAT I DO ABOUT IT.
How To Defend Against Spear Phishing

- Tune your BS-o-meter
  - The single most effective way to deter spear phishing is to suspect ALL unsolicited messages

- Confirm **everything** with trusted persons

- If even the tiniest bit suspicious, DO NOT RESPOND
Social Engineering: Attacks By Web Site
Attacks By Internet

Sometimes, social engineering attacks come in the form of web sites.

- **Internet / Web Site Attacks**
  - Scareware, Trickware, Crimeware, and other terms for the same deceptions
**Scareware 101:** Websites that look like your Operating System or Legit Software That You Might Use

If you are in a WEB BROWSER and you come across a website that looks like your Windows / Mac system, it’s an attack

- **Windows Attack Vectors**
  - False Windows Update notification
  - False Malware Infection Notification

- **Mac Attack Vectors**
  - MacDefender

- **Drive-by Malware Installs Abound!**
Example 1: The Windows Update scam
Example 2: The "My Computer Is Infected" Scam
Attacks By Internet

Scareware

Example 3:
The Windows 7 Action Center

Warning scam

SCAM
Attacks By Internet

Example 4:
The MacDefender Scam
Attacks By Internet

Scareware Abounds:
Fake Alerts Through The Web
Browser Affect The Untrained, The Unaware, & The Unexpecting

SCAM
A Special Note About Social Networking Sites:

- Social networking sites like Facebook and Twitter are the new hotness for scammers.
- Beware Facebook Apps: More new infections are being spread through Facebook apps than any other attack vector.
- Beware URL Shorteners: They hide the true links' destination, which is great for scammers.
How To Defend Against ScareWare

- Understand that critical system security messages will **NEVER** come through your web browser.

- Never run unsolicited software that appears in your web browser.

- Anti-virus software won’t always protect you, so you must be treat the web with suspicion at all times.
  - “The Internet is a dirty, dirty place. Practice safe browsing.”
Social Engineering: Attacks In Person
Attacks In Person

The rarest (but most effective) social engineering attack

- Attacker is a person who comes onsite
- Has a foolproof pretext
- A convincing actor who may be in costume, have an accent, fake ID’s, false paperwork...everything!!
Attacks In Person

The Most Dangerous Type of Attack

- You never know how far they’ll go
- Confident, cunning, and intelligent
- Their ability to adapt in real-time to your suspicion is their most valuable skill
- The never look like they don’t belong
Most Common Pretexts For Attacks In Person

- Utility Serviceman
- Telecom Engineer
- Pest Control Service
- IT Contractor
- Fake Employee (industry-specific)
- Courier / Deliveryman
Attacks In Person

In-Person Attack Vectors

- Piggyback into restricted areas behind legitimate employees
- Use emotional tricks against the target (charm, empathy, intimidation, etc) to gain information or access
- Looking like they belong there (VERY EFFECTIVE)

Remember, if the Social Engineer is onsite they are looking for something specific…but what?
Attacks In Person

Computer Media Containing Sensitive Data

1.

2.

3.

4.
Attacks In Person

Keys To Access Restricted Areas

1. [Image of a key being inserted into a lock]

2. [Image of a computer workstation]

3. [Image of a computer monitor displaying multiple screens]

4. [Image of a person using a computer]
Attacks In Person

Corporate Espionage / Document Theft
Attacks In Person

Defense Against In-Person Attacks

- Be suspicious of anyone who:
  - You don’t immediately recognize
  - Doesn’t have an ID badge or FOB visible
  - Is walking around unescorted or without a Visitor badge

- Always verify the ID of everyone who tries to bypass a physical control (like a FOB-controlled door)

- Be firm, friendly, and unfamiliar with unverified strangers

- When in doubt, bring a superior into the picture
Employee Recognition

Reported The Email Attack
- Yacksil Gomez
- Martin Rodriguez
- Jose Perez

Reported The Physical Breach
- Janette Verde
Report Suspicious Activity To

SPAM@intermexusa.com

Details on Information Security Policy Can Be Found At:

https://intranet.intermexusa.com
What Happens Now?

- Random Testing Throughout The Year
  - Miami, Mexico, Guatemala
  - Data Security Is A Full-Time Thought

- Test Failures Will Be Noted
  - May Result in an employee file memo
A Word About Common Defenses

- Firm, friendly, & unfamiliar
- Always validate & verify
- Healthy paranoia
- Tune your BS meter
- Never share your password
Contact Information

Sabino Marquez

smarquez@accretivesolutions.com

Jennifer Hensley

jhensley@accretivesolutions.com

(904) 208-5607

76 South Laura Street, Suite 202
Jacksonville, Florida 32202
www.accretivesolutions.com