AGENDA

Thank you for the interest

INTRODUCTION

What social Engineering is about

SE ATTACK

Brief introduction to social engineering attacks

SE Attacks Techniques

Discussion on the various forms of SE attacks techniques

SE PROCESSES

From social media to shell and the processes involved

Business Impact

Result of SE attacks on a business and the psychological impact on the victim

DEFENCES AGAINST SE ATTACKS

How Social Engineering attacks can be prevented

Shall We DEMO?

3

INTRODUCTION

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information...Wikipedia

"BUGS" IN HUMAN HARDWARE

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information

SOCIAL ENGINEERING ATTACKS

Motive determines everything

A social engineering attack is an orchestrated campaign against employees at either a variety of companies or one high valued business using a variety of digital, in-person or over the phone techniques to steal intellectual property, credentials or money.

ATTACK METHODOLOGY

It starts with "Hi"

Preparing the ground for the attack:

· Identifying the victim(s).

· Gathering background information.

· Selecting attack method(s).

**Closing the interaction,
ideally without arousing suspicion:**

· Bringing the charade to a natural end.

· Removing all traces of malware.

· Covering tracks.

INVESTIGATION

Social Engineering Life Cycle

EXIT

HOOK

PLAY
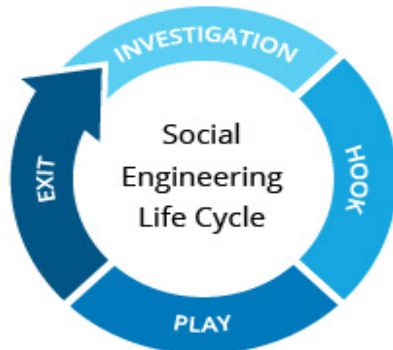
Deceiving the victim(s) to gain a foothold:

· Engaging the target.

· Spinning a story.

· Taking control of the interaction.

Obtaining the information over a period of time:

· Expanding foothold.

· Executing the attack.

· Disrupting business or/and siphoning data.

7

FORMS OF SE ATTACKS

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam nec sem.

PHISHING

Looks legit

TAILGATING

Right behind you

PRETEXTING

Lie to me one more time...

BAITING

Click and get sweets...I promise

SCAREWARE

You have less than 2 minutes

SPEAR PHISHING

Hello... from the boss side

Phishing

Keep the hook

Phishing scams might be the most common types of social engineering attacks used today

Characteristics:

1. Often unsolicited

2. Seek to obtain personal information such as names, addresses and passwords

3. Uses link shorteners or embed links to redirect users to suspicious websites

4. Incorporates threats, fear and sense of urgency

5. Often crafted with grammar and spelling errors

9

PRACTICAL EXAMPLE

Apologies to Victoria, Oga Livi we go jam

Hi Mr. Livinus,

There was a login attempt into your account today at 12:00 EST from 202.168.23.56 in Canada.

Your XERO account has been temporarily disabled to protect you. Click here to login immediately or call +1(485)34564.

We apologize for the inconvenience
At your service,

XERO support team.

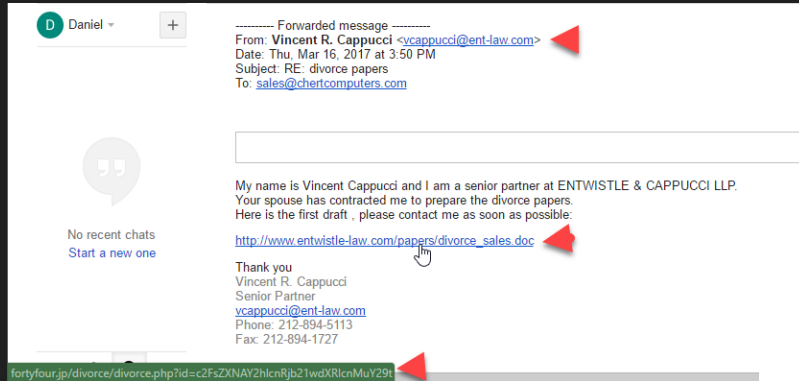Click here to Reply, Reply to all, or Forward

Convincing Email

After gathering information about chert.ng, the attacker crafts a personalized email to all employees in Chert

(Also an example of spear phishing)

CAUGHT?

Unsuspecting victims believing their accounts have been truly hacked tried to prove their identity as requested by the hacker

```
[fragment] =>
[userName] => victoria@chert.ng
[password] => 4in@anceChert
[__RequestVerificationToken] => YEBLiXWsdi4K-fbNHkcA894-1TBsNBHUog7TVbIkICRtQz5btLQ67SdBS6BDisUVUep
b-Y1LILA7uHLcCc63iDDCALBHR1ZwEgLTIBq2VDTXqAiQFrJJLztfoHN__m0uEu9wEA2
)
Array
(
[fragment] =>
[userName] => livinus@chert.ng
[password] => nigeria01
[__RequestVerificationToken] => YEBLiXWsdi4K-fbNHkcA894-1TBsNBHUog7TVbIkICRtQz5btLQ67SdBS6BDisUVUep
b-Y1LILA7uHLcCc63iDDCALBHR1ZwEgLTIBq2VDTXqAiQFrJJLztfoHN__m0uEu9wEA2
)
```

Let's do beautiful bu

10

---------- Forwarded message ----------
From: Vincent R. Cappucci <vcappucci@ent-law.com>
Date: Thu, Mar 16, 2017 at 3:50 PM
Subject: RE: divorce papers
To: sales@chertcomputers.com

My name is Vincent Cappucci and I am a senior partner at ENTWISTLE & CAPPUCCI LLP.
Your spouse has contracted me to prepare the divorce papers.
Here is the first draft , please contact me as soon as possible:

http://www.entwistle-law.com/papers/divorce_sales.doc

Thank you
Vincent R. Cappucci
Senior Partner
vcappucci@ent-law.com
Phone: 212-894-5113
Fax: 212-894-1727

fortyfour.jp/divorce/divorce.php?id=c2FsZXNAY2hlcnRjb21wdXRlcnMuY29t

From: London Green <longre4550@nrms.org>
Date: 2 March 2017 at 23:29:26 GMT
To: undisclosed-recipients:;
Subject: Urgent Request For Quotation Sales Offer112632

Dear Sir,

We would like to take this opportunity to introduce ourselves as one of the leading Importe
Distributor in the country.

Recently we have a Request to quote for the followings see attach for more details

Please Contact us urgently to confirm us what will be the Distributor Price.

Your Prompt Response will be highly Appreciated,

With Best Regards.

Please this is very urgently

Sales Offer 11263...
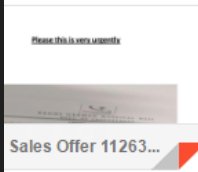
BEHAVIOURAL FLAWS

Show me your flaws and I will tell you who you are...Daniel C.O

Trust

Thinking everybody want your best interest...Sike!!!

Desire To be Helpful

Someplace somewhere someone is trying to help

Greed

Ifa or longer throat, trying to get something for nothing

Curiosity

Some people like behaving like cats...then get killed – opening attachments from unknown senders

FEAR

Fear of the unknown, or losing something

Ignorance

Can lead to stupidity

-Dumpster diving

SCARY

What makes social engineering scary

Social engineering is one of the most overlooked yet most effective ways for a malicious user to extract information to gain access into a network

There is no science or appliance that can fully protect against social engineering

Why Should You Care?
Employees Targeted By Hackers

Note:
Business impact of social engineering attacks to organizations:
- Legal
- Financial
- Operational
- Reputational

Source: Verizon's "2012 Data Breach Investigation Report"

BUSINESS IMPACT

A system or institution is only as strong as its weakest link
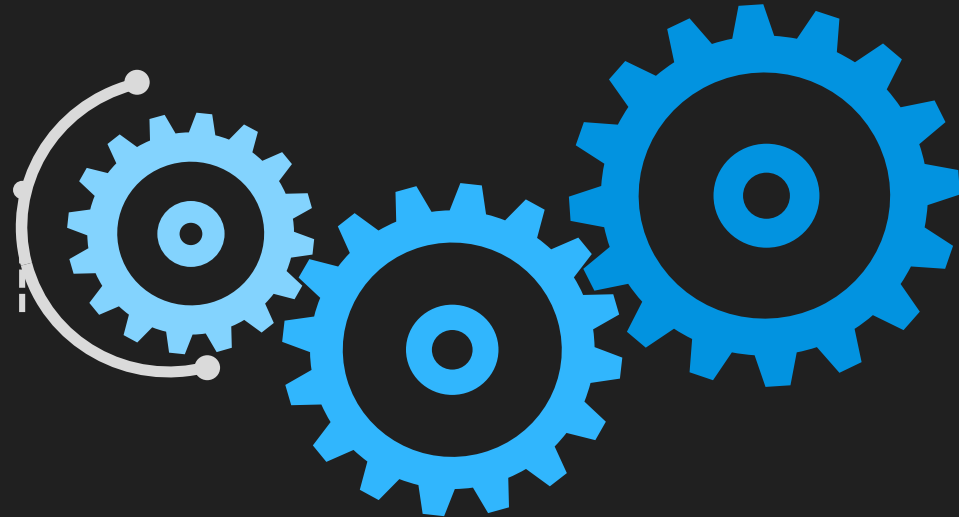
Cloud effect

Most businesses move their infrastructure and critical application to the cloud to prevent hacking, but... they forget one thing...

Reputational Impact

Once hacked, twice shy

Compliance Risk

SE threatens compliance

Legal Repercussions

1000 ways to get sued

DEFENCE AGAINST SE ATTACKS

Raising the shield of common sense

Well-Documented Security policy

Every organization should have a well-documented and accessible security policy of a good security strategy.

Trainings

For the policies to be effective, training must be regular. All new employees must be trained as soon as they start with the organization

Awareness

Employees need to be informed on latest security threat that could impact the organization negatively

Looking Too good to be true

It's probably is

16

DEMONSTRATION

In this demo, I will be giving a Chert system solution employee her biggest sale this year...or will I (Rubs hands suspiciously)