

Deceptive Information Gathering (Social Engineering)

Twitter @Raj_Samani

Structure

Problem? - What Problem?

What?

Who and Why?


Obstacles?

Solutions?

The InfoSec View?

Threats: Network, O/S, Database, Application, Malware, Physical, People

Counters: Segment, Patch Mgt, Firewalls, Monitor, Pen Test [IPS], [IDS]

Network	O/S	Database	Application	Malware	Physical	People
Segment	Harden	Harden	Reviews	Antivirus	Locks	
Patch Mgt	Patch	Patch	Test	Anti Spyware	Alarms	
Firewalls	Policy	Audit Trails	Patch	Web-blocking	Segregation	
Monitor	Audit Trails	Policies	Monitor	Spam Filters	Guards	
Pen Test [IPS]	Monitor	Pen Test	[Pen Test]		Processes	
[IDS]	Pen Test	[IDS]	[IDS]			

Hacking (Network, O/S, Database, Application, Malware, Physical)

Social Engineering (People)

I must defend all that data sitting in my technology

It's the (small) fuzzy bit at the end of the job...

Problem? - What Problem?

3

... "Information Brokers"

One Information Broker earned £50,000 a month from one client for tracing, (Addresses at £35 a time. Address and Employer £55.) The Broker had many clients, and is one of many

Tariff of charges in Motorman Case

Information Required	Price paid to 'Blagger'	Price charged to customer
Occupant search/Electoral roll check (obtaining or checking an address)	Not known	£17.50
Telephone reverse trace	£40	£75
Telephone conversion (mobile)	Not known	£75
Friends and Family	£60-80	Not known
Vehicle check at DVLA	£70	£150-200
Area search (locating a named person across a wide area)	Not known	£60
Company/Director search	Not known	£40
Ex directory search	£40	£65-75
Mobile telephone account enquiries	Not known	£750
Licence check	Not known	£250

... just the tip of the iceberg

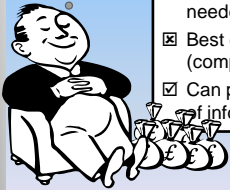
Problem? - What Problem?

4

The Information Brokers View...

Problem? - What Problem?

My client will pay £££ for info on x.
How can I get it?



Hacking	Social Engineering
<input checked="" type="checkbox"/> Frontal assault on technical defences	<input checked="" type="checkbox"/> Few Defences
<input checked="" type="checkbox"/> Takes a while to set up	<input checked="" type="checkbox"/> Fast Results
<input checked="" type="checkbox"/> A bit hit and miss - may not get specific information	<input checked="" type="checkbox"/> Easy to target specific information
<input checked="" type="checkbox"/> High Skill Levels	<input checked="" type="checkbox"/> Easy to teach
<input checked="" type="checkbox"/> Audit Trails of activity	<input checked="" type="checkbox"/> Few (no) audit trails – hard to prosecute
<input checked="" type="checkbox"/> High startup costs (capital needed)	<input checked="" type="checkbox"/> It works, or can keep on trying until it does
<input checked="" type="checkbox"/> Best done from off shore (complex)	<input checked="" type="checkbox"/> Low cost
<input checked="" type="checkbox"/> Can provide industrial quantities of information	<input checked="" type="checkbox"/> Can be industrialised
	<input checked="" type="checkbox"/> Tends to provide only snippets of information

It's a no brainer

5

Problem, What Problem? Summary

Problem? - What Problem?

•The Facts:

- It is the Information Broker's preferred option
- Our defences are poor
- It happens. (There is an industry exploiting it)
- We don't understand it

•Conclusions:

- We cannot ignore this – it is a major threat
- We need to understand it more fully to even start to counter it.

Place to start is by getting a better understanding...

6

Web Definitions

“Breaking an organization’s security by interactions with people, for example tricking someone into giving out a password”

High Tech Dictionary: <http://www.computeruser.com/resources/dictionary/definition.html?lookup=8057>

“Taking advantage of people’s naivety via influence, persuasion and manipulation to obtain vital information”

Mitnick, Kevin D. & Simon, William L. “The Art of Deception” 2002.

“A collection of techniques used to manipulate people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access and in most cases the attacker never comes face-to-face with the victim.”

Wikipedia en.wikipedia.org/wiki/Social_engineering

“A skill by which an unknown person gains the trust of someone inside your organisation and encourages them to make changes to an IT system in order to grant them access rights”

CISSP Study Guide

“A hacker’s clever manipulation of the natural human tendency to trust, with the goal of obtaining information that will allow him/her to gain unauthorized access to a valued system and the information that resides on that system.”

www.securityfocus.com/infocus/1533

... vary from unhelpfully generic to inaccurately over specific. A portent!

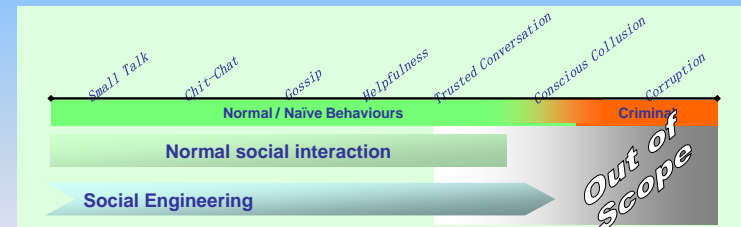
A Working Definition

“The deliberate application of deceitful techniques designed to manipulate people into:

- a) divulging personal, commercial, or otherwise confidential information or
 - b) performing actions that may result in the release of that information.
- ... with the express intent of obtaining that information.

During a Social Engineering interaction, the ‘mark’ is not consciously aware that what they are doing is wrong. Social Engineering is an exploitation of natural instincts, not criminality.

Corruption and deliberate abuse of authority are not Social engineering. “



It’s about manipulating the unconscious for data, not conscious collusion

Tapping into the unconscious...

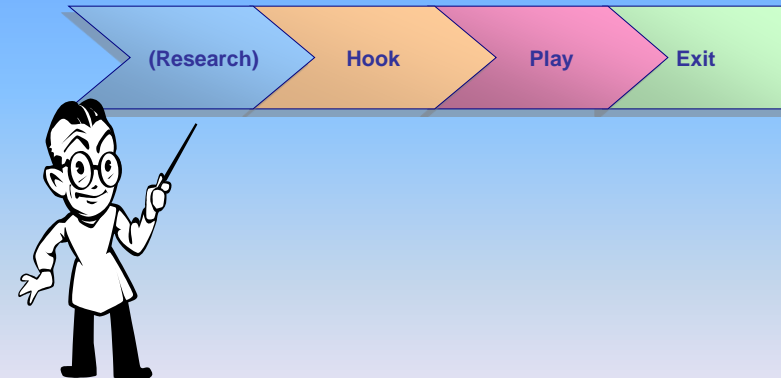
6 'compliance tendencies' *

1. *Authority*
2. *Liking*
3. *Reciprocation*
4. *Consistency*
5. *Social Validation*
6. *Scarcity*

It relies on hacking into the human operating system!

*Sources: Mitnick, Kevin D. & Simon, William L. "The Art of Deception" 2002.

Attack Lifecycle



Understand the lifecycle, and you may be able to disrupt it...

Modus Operandi

Hunting



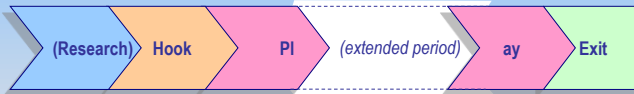
Objective: - Get information and close



Farming



Objective: - To establish a source, then 'milk' information



Hunting is much easier to counter than Farming...

Targeting vs. Opportunism

The 'Hook' provides the best opportunity for defence. It tends to work in one of two ways, although strictly speaking they can be seen as two ends of spectrum:

	Targeted	Opportunistic
Aim Mark	Focused on obtaining specific information, usually from a specific individual	Generic information from anyone in a position to give it – often with intent to assemble it into a 'bigger picture'
	<ul style="list-style-type: none"> • Jon Smith • Mr X • Jon the Receptionist 	<ul style="list-style-type: none"> • <u>A</u> Receptionist (any one will do) • <u>The</u> Help-desk (any engineer will do) • An Employee

Defending against opportunists may be the best place to start

What? - Summary

The Facts:

- Is a form of con – the objective being to obtain information
- Very hard to distinguish from normal behaviour
- Bypasses the conscious, so is hard to counter
- Follows a Research-Hook-Play-Exit lifecycle
- Has two distinct modus operandi – Hunting and Farming
- The Hook tends to a Targeted / Opportunistic separation

Conclusions:

- Its complex - it is unlikely there is a panacea
- Countermeasures need to be specific - If you try to cover everything, you risk spreading resources too thin

Starting place: Understand who and why...

Who?

- *Private Investigators (Information Brokers)*
- *Debt Collection & Tracing Agencies*
- *Journalists*
- *Internal Individuals*
- *Government Agencies .*
- *Organised Crime (Local)*
- *Organised Crime (Remote)*
- *Activists*
- *Academics/Researchers*
- *Individuals, External*
- *Security Services*
- *Commercial Organisations*
- *Aggregators*
- *Solicitors*

Not a bad list to start with...

Who?... Why?

Target: Information Assets

1) Primary Information

- *Personal Data* – names and addresses, contact details etc.
- *(Saleable) Commercial Information* – Trade Secrets, design concepts, information about commercial contracts, sales etc.

2 Enabling Information

- *Public Internal* – phone books, intranet, etc.
- *Public External* – already available to the general public, e.g. brochures, web pages, etc.
- *HR Data* – available in HR and training systems, employee details, etc..
- *Management Information* – financial, information related to deployment and planning, etc.
- *IT Technical Design* – Logical or conceptual design documentation.
- *Technical Operational* – Detailed technical designs, system logs, system configurations, etc.

... depends on the business you are in

Who? ... Why?

15

Who/Why: Summary

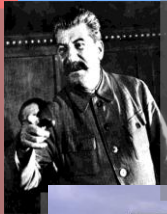
	Modus Operandi		Example Motives
	Hunt	Farm	
Private Investigators			Address/Salary/employment status of Mr X. Bid results. New pricing structures. Anything for a client.
Debt Collection/Tracing			Confirm address of employee, earning capabilities or bank details
Journalists			Confirm elements of story. Find story' on organisation, its plans, 'dirt', financial or commercial strategies
Internal Individuals			Details of prospective in-law. Helping a friend. Curiosity.
Government Agencies			Where does Mr X live. What is his training record? His attendance record? Where was he on [date/time].
Organised Crime (Local)			Where is witness living? ID Theft, Drug dealers
Organised Crime (Remote)			ID Theft
Activists			Who was involved in the tests? Are you trading with my target organisation? Who can I exert pressure on?
Academics/Researchers			Can I get info for my research through the back door? How is my rival doing?
Individuals/External			Where is my ex living? Is there a story I can sell? Information to aid technical hacking. Investment info.
Security Services			Background info, personal info...
Commercial Orgs			Commercial strategy, bid prices, info on key personnel. Insurance claim checks, Sales support info
Aggregators			Anything to add to my database?
Solicitors			Address of client's ex? Salary/employment status. Indications of corporate culpability.

Normal Risk Assessment methods apply...

Who? ... Why?

16

Terminology



Generates:

Anger

- Social Engineer/ Social Engineering

Annoyance

- Blagger, Blagging
- Mark

Confusion (False Friends)

- Victim
- Conman
- Bogus Caller
- Hustler
- Fraudster

OK, it's "Deceptive Information Gathering" (DIGing)...

Obstacles?

17

The Standard Answer



Awareness Campaigns are nothing new ... but do they work?

Obstacles?

18

Sources: www.ussm.org, www.war-experience.org; www.bbc.co.uk

... nope!

- “Having characterised the staff of the old Department of Social Security as being ‘subservient to the rules, rather lacking in personal character’ and ‘utterly paranoid about bogus callers’, the [Blaggers] manual offered the following advice:

‘The way to con this type of person is to convince them that you are just as prim and proper as they are. Don’t even bother calling them under the pretext that you are a cockney or an idiot, because you won’t last five seconds. They deal with idiots and layabouts all day, so ring them in the style of a keen little civil servant who wants to learn to solve their problems instead of relying on senior Staff at another other office. Speak with a clear, confident manner. Be polite and friendly at all times as rudeness will not work here.’”*

- DSS awareness campaigns had worked, engendering paranoia, but had not necessarily increased resistance to Social Engineering.

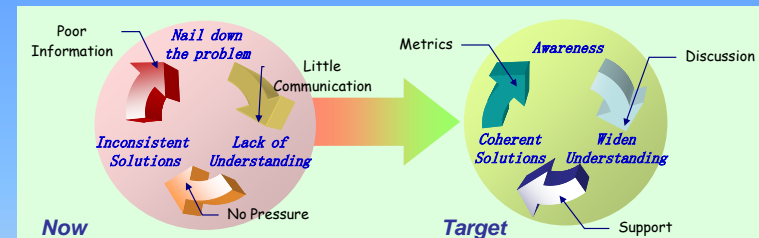
It works on the subconscious!

Obstacles?

19

*Source: What Price Privacy, ICO

The Text-Book Solution



- Admit to the problem
- Clear boundaries
- ‘Permission to verify’
- A sense of the importance of information
- Nurture a ‘no blame’ mentality
- Stop relying on technology for security

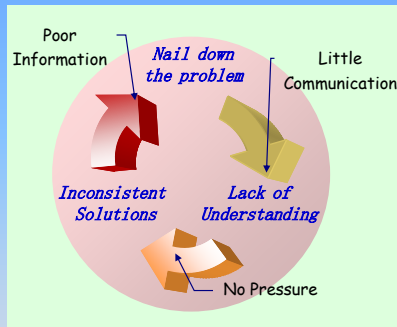
Widen Understanding, and the rest follows...

Obstacles?

20

... but:

We are here!



(Is particularly difficult from of a technology department, which has always advocated technology to provide quick fixes before...)

There has to be another way...

So:

- *Lack of Understanding means support is limited*
- *(We don't even have a common language)*
- *It would be politically difficult to admit to a wide-scale problem*
- *If you did, the solution would have to arrive fast*
- *(There are no fast solutions in cultural change)*

Obstacles: Summary

The Facts:

- We can't even talk about the subject
- We don't believe in the 'solutions' that have gone before

Conclusions:

- Solutions have to be politically pragmatic

Most common techniques

	Hook	Play
Reciprocation		
Liking		
Scarcity		
Authority		
Consistency		
Social Validation		

Looks like several things going on...

DIGing: 4 different Aspects

Technical

- Largely opportunist
- Phishing, (spear phishing) Malware, Web pages, social networking etc.
- Counter with technology and instruction

Bullying

- **NOISY!**
- Use authority/uniforms, quote the regulations, bamboozle
- Both Hunting & Farming
- Counter with processes MAU's, permission to verify

Deceptive Information Gathering

Familiar

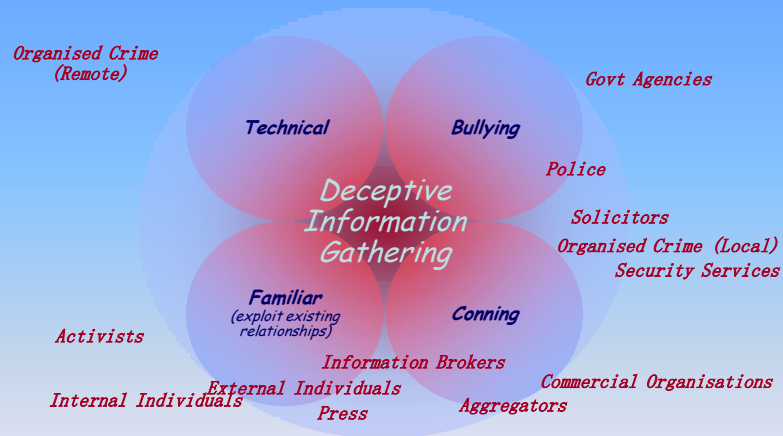
- Exploit s existing relationships (not just Farming)
- People may be suspicious, but won't rat on their friends
- Counter by education – whistle-blowing, discipline

Conning

- 'Blagging', sweet-talking – well done, will not raise suspicions
- Both Hunting and Farming
- Counter by education & simulation 'no blame', reporting

Different Aspects, different solutions

Who does what?

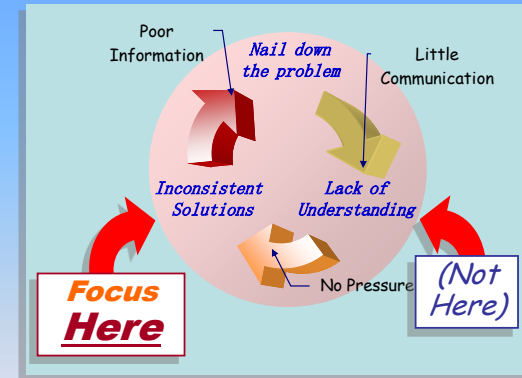


Fits back into the Risk Analysis...

Solutions

25

Political Pragmatism:



Change the behaviours, understanding may follow

Solutions

26

Conclusion:

- Not a single problem...
 - ...Deal with the elements



- ...Questions?