Social Engineering for Penetration Testers

Sharon Conheady

Brucon 2009, 2018

Alternative names for this talk

- ✓ “Buffer overflows are really hard, lying is easy”
- ✓ “If you can’t go through the firewall, go through the secretary”
- ✓ “To attack and surely take it, attack where they do not defend”
- ✓ Social engineering still works (2018)

A Definition (2009)

efforts to influence popular attitudes and social behaviour on a large scale, whether by governments or private groups

- Wikipedia definition

A Definition (updated)

efforts to influence popular attitudes and social behaviour on a large scale, whether by ~~governments~~ <*insert government*> *or* ~~private groups~~ *-Facebook*

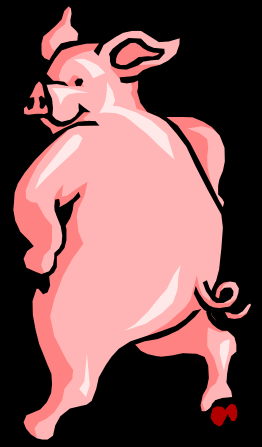
- Based on Wikipedia definition, 2009


SHE MAY LOOK CLEAN - BUT
PICK-UPS
"GOOD TIME" GIRLS
PROSTITUTES
SPREAD SYPHILIS AND GONORRHEA
You can't beat the Axis if you get VD


CHANGE
WE CAN BELIEVE IN
Obama
OBAMA'08

- ✓ *Bush Down to 8 Friends on Myspace*
- ✓ *Jesus Christ to Star in Next Series of Batman*
- ✓ *Bush Claims He Has Supernatural Abilities*
- ✓ *Donald Trump missing, feared kidnapped*
- ✓ *What Annoyed Us About The Olympic Opening Ceremony*
- ✓ *Fox News Admits Grievous Error*
- ✓ *New Economic Stimulus Package Includes Goat*
- ✓ ***Preliminary US Presidential election polls results here***

Swine Flu Social Engineering



- First US swine flu victims!
- US swine flu statistics
- Salma Hayek caught swine flu!
- Swine flu worldwide!
- Swine flu in Hollywood!
- Swine flu in USA
- Madonna caught swine flu!

Most common email subject lines for Q2 2018

- ✓ · Microsoft: Re: Important Email Backup Failed
- ✓ · Microsoft/Office 365: Re: Clutter Highlight
- ✓ · Wells Fargo: Your Wells Fargo contact information has been updated
- ✓ · Chase: Fraudulent Activity On Your Checking Account – Act Now
- ✓ · Office 365: Change Your Password Immediately
- ✓ · Amazon: We tried to deliver your package today
- ✓ · Amazon: Refund - Valid Billing Information Needed
- ✓ · IT: Ransomware Scan
- ✓ · Docusign: Your Docusign account is suspended
- ✓ · You have a secure message

Source: https://www.knowbe4.com/press/knowbe4-releases-q2-2018-top-clicked-phishing-report

What is Social Engineering?

techniques hackers use to deceive a trusted computer user within a company into revealing sensitive information, or trick an unsuspecting mark into performing actions that create a security hole for them to slip through

- Kevin Mitnick

What has changed?

- Nothing
- What does this say about our industry?
- It’s human nature.

Advance Fee Fraud

- The Spanish Prisoner, 16th Century
- The Letter from Jerusalem, 18th Century
- Nigerian postal/fax scams in the 1980s
- 419 scam
- Friend scam
- Scams work because they evoke emotion or greed (and may come in from your friend)

The Spanish Prisoner

- ✓ Dates from 16th Century and the era of the Spanish Armada.
- ✓ The con man, accompanied by a beautiful lady, approached British nobles with the story that the lady's father, a fellow nobleman, had been imprisoned in Spain.
- ✓ A letter smuggled from the prisoner was shown as evidence.
- ✓ The prisoner's identity was concealed, supposedly to prevent the Spanish from realising they had such a valuable prisoner.
- ✓ If the British noble would pay the ransom the jailed father would issue a reward on his release and offer his daughter's hand in marriage.

The Letter from Jerusalem

- *"...These latter [the plotters] obtained the address of certain rich persons living in the, province, which was easy from the number of prisoners who were constantly arriving. They then wrote letters to them, called, in the slang language, "letters of Jerusalem..."*
- The sender would pretend to be a valais-de-chambre to a marquis who on their travels had lost/hidden a casket containing 16,000 Francs and would request an advance.
- Of 100 letters, Vidocq claims that 20 were always answered!

Memoirs of Vidocq: Master of Crime

"...The Parisians themselves sometimes fell into the snare: and some persons may still remember the adventure of the clothseller of the Rue des Prouvaires, who was caught undermining an arch of the Pont Neuf, where he expected to find the diamonds of the duchess de Bouillon..."

Nigerian scams in the 1980s

- In the early 80's, Nigeria's oil-based economy declined.
- Some unemployed university students original devised this scam to manipulate visitors to Nigeria interested in shady oil deals.
- They went on to target businessmen in the west, sending messages via letter, fax or Telex...and eventually email.

Dr. Bakare Tunde
Astronautics Project Manager
National Space Research and Development Agency (NASRDA)
Plot 555, Misau Street, PMB 437
Garki, Abuja, FCT NIGERIA

Dear Mr. Sir,

REQUEST FOR ASSISTANCE-STRICTLY CONFIDENTIAL

I am Dr. Bakare Tunde, the cousin of Nigerian Astronaut, Air Force Major Abacha Tunde. He was the first African in space when he made a secret flight to the Salyut 6 space station in 1979. He was on a later Soviet spaceflight, Soyuz T-16Z to the secret Soviet military space station Salyut 8T in 1989. He was stranded there in 1990 when the Soviet Union was dissolved. His other Soviet crew members returned to earth on the Soyuz T-16Z, but his place was taken up by return cargo. There have been occasional Progrez supply flights to keep him going since that time. He is in good humor, but wants to come home.

…

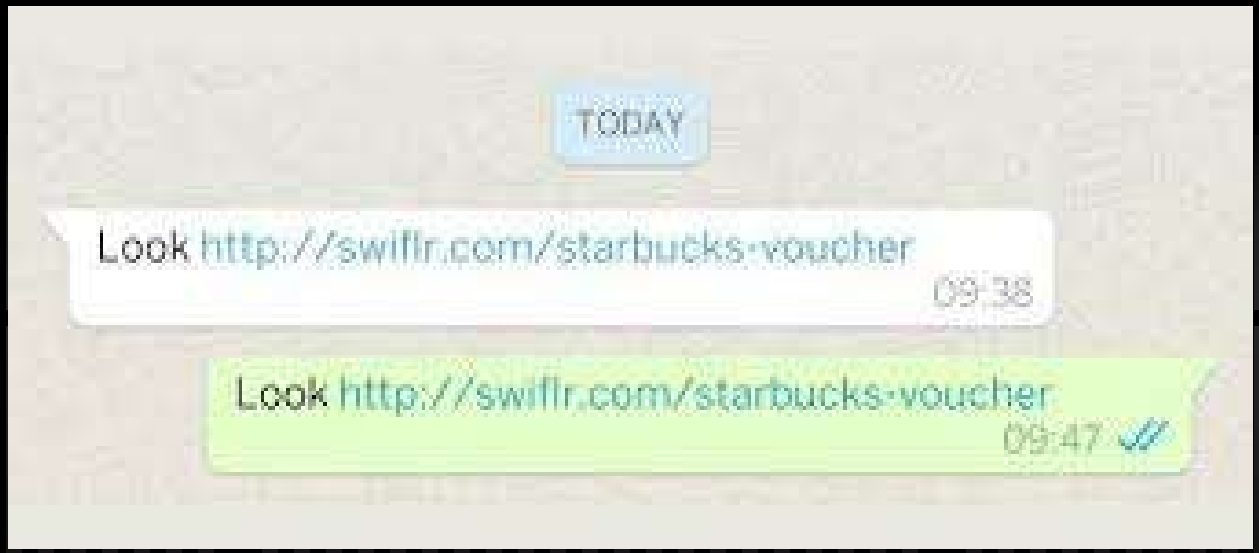
Needless to say, the trust reposed on you at this juncture is enormous. In return, we have agreed to offer you 20 percent of the transferred sum, while 10 percent shall be set aside for incidental expenses (internal and external) between the parties in the course of the transaction. You will be mandated to remit the balance 70 percent to other accounts in due course.

…

Friend Scams

- The stranded traveller
  - I'm stranded in <random location from the news> because of the <news story>. Please could you lend me some money...?
- The mugging victim
  - Help! I've just been mugged and need to settle my hotel bill. Please could you lend me some money…?
- Via email, social media, instant messaging

WhatsApp Fake Vouchers Scam



What has changed since 2009

- ✓ The scale
- ✓ Sophistication
- ✓ More targeted
- ✓ Ethical SE tests are mostly phishing

Why social engineering works

- People want to help
  - Customer service focussed society (e.g. call centres)
- Greed
  - Passwords for chocolate
- Tendency to trust
- Complacency
  - It's easier to give people information to get rid of them
- Fear (of getting into trouble for not doing their job)
- People don't like confrontations
  - The yes rule

Remote vs On Site vs Real World

- Remote
  - Email
  - Fax
  - Telephone
- On site
  - Extreme social engineering
  - Very effective but may be easier to get caught
- Next generation: real world attacks
  - Traffic ticket incident, February 2009

Different types of attacks

- Mumble attack
- Reverse social engineering
- Road apples
- 10 attack
- Phishing
- Remote vs On Site vs Real World

Is Social Engineering a real problem?

October 29, 2007

Online raiders fool banks into handing over customers' details

Adam Fresco, Crime Correspondent

A gang of online bank robbers that has taken at least ten people and stolen hundreds of tho being hunted by an anti-fraud unit.

The gang hacked into private bank accounts a details to order new debit and credit cards wh buy expensive jewellery, electronic goods and

The gang managed to get enough information have £60,000 transferred from his mortgage re current account, which it then spent.

Barclays Bank managed to intercept much of believed to have stopped at least £500,000 be clients. But officers from the Dedicated Chequ Unit say that there may be many more victims

RELATED LINKS

- Government to police virtual worlds
- Online criminals target Facebook

Detective Con Harrington sai favourite meth known as 'account take over', in which the thieves got enough private information to convince a bank that they were the custome and then ordered a new card and PIN.

Thief woos bank staff with chocolates - then steals diamonds worth £14m

By Stephen Castle in Brussels
Sunday, 18 March 2007

A thief has evaded one of the world's most expensive hi-tech security systems diamonds - than staff: personal c

In what may be the conman burg in Antwerp's dia carats. Posing a the bank frequer their confidence to one diamond

Now, embarrass wondering how with a false Arge

mcast hackers come forward

/06/2008

hackers who successfully shut down the internet hours have

d that the d said they selves into'.

age shutting million

Print Email

Boy tries to talk his way onto plane again

(No Ratings Yet)

Posted on: May 29th, 2008 by John Morgan

Last year, a 10-year old boy succeeded in boarding a flight to Texas with nothing but his wits and his smart mouth as a passport. On Tuesday, he tried it again, but was caught and stopped at the boarding gate, according to authorities.

Security tapes at Seattle-Tacoma International Airport show Semaj Boooker successfully going through airport security before 05:00. The checkpoint and metal detector were operated by the Transport Security Administration.

At 03:00, Semaj's mother reported him missing to police in Tacoma.

Police are looking into how the boy was able to get so far in the airport through security without showing a boarding pass, according to the Northwest region spokesperson for the TSA in Salt Lake City, Dwayne Baird.

Semaj attempted to board a flight to Sacramento, California, operated by Southwest Airlines but was detained before he could do so, according to a statement from Perry Cooper, a spokesperson from the airport.

In January last year, Semaj successfully lied himself a seat on a flight operated by Southwest Airlines, claiming that his mother was in the boarding area. He changed planes in Phoenix and landed in San Antonio before he was caught. Days earlier, the boy stole and crashed a car.


Semaj Booker made national
headlines at age 9 for running away.
He hasn't stopped running since.

GEZOCHT

Politie

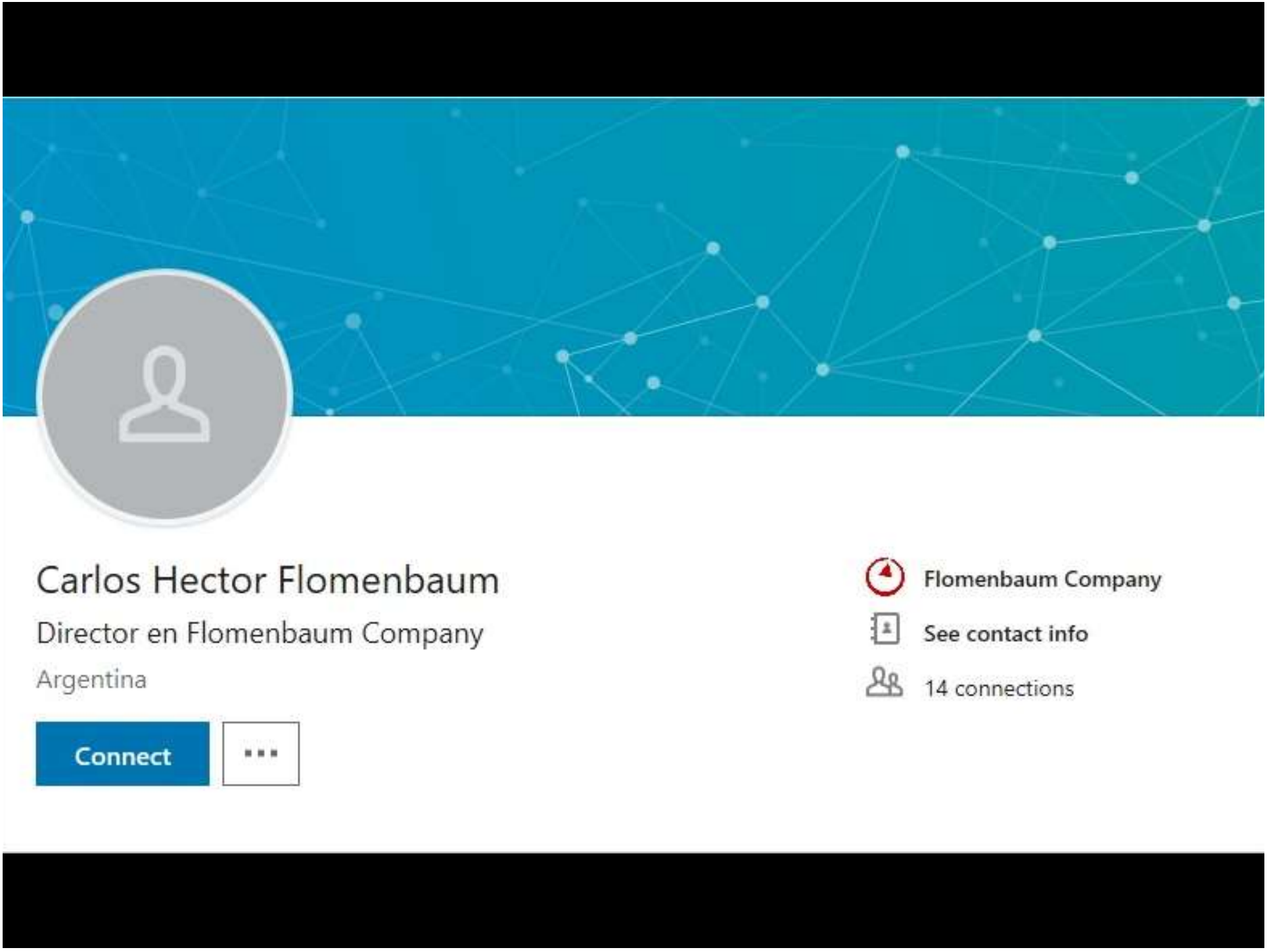
ONDERWERP:

DGJ/DJT/ROBOT

Notitienummer :
Eenheid :

Beschrijving :

- **C**arlos **H**ector **F**lomenbaum
- CHF = Switzerland?


Carlos Hector Flomenbaum
Director en Flomenbaum Company
Argentina
Connect
Flomenbaum Company
See contact info
14 connections

A decade of diamond heists

- Amsterdam Airport heist, $77m
  - Stolen KLM uniforms and trucks (and guns)
- Harry Winston Store, Paris, $102m
  - Men dressed as women
- Graff Diamonds, London, $65m
  - Visited a professional make up artist to change their appearance
- Damiani showroom, Milan, $20m
  - Neighbour complained about the drilling
- Brussels Airport, $50m
  - Thieves wore police uniforms*

The Telegraph

Police arrest stripper 22 times for impersonating an officer

A police force has been criticised after spending £170,000 to arrest a stripper 22 times for impersonating an officer.

Stuart Kennedy: so far none of the cases brought against him have yielded a successful prosecution Photo: NORTHSCOT

By Ben Leach
11:15AM GMT 21 Jan 2009

How about that?
News » UK News »

In How About That?

Pictures of the day

Pictures of the day


MICHAEL CAINE
JIM BROADBENT
TOM COURTENAY
CHARLIE COX
PAUL WHITEHOUSE
WITH MICHAEL GAMBON
WITH RAY WINSTONE
FROM THE PRODUCERS OF
DARKEST HOUR & LEGEND
KING OF THIEVES
THE UNBELIEVABLE TRUE STORY OF THE HATTON GARDEN HEIST

Why perform a social engineering test?

- ✓ To test the effectiveness of physical security controls
- ✓ To test the level of (and even improve) security awareness among staff
- ✓ To give your staff practice at identifying the techniques that social engineers may use and at learning how to deal with social engineering situations
- ✓ To provide valuable recommendations on both security awareness and physical security
- ✓ Often combined with a technical penetration test

The stages of the attack

1. Target identification
2. Reconnaissance
3. Creating your scenario
4. Going in for the attack
5. Getting out again
6. (Writing the report)

Before you start

Reconnaissance (1) *

Passive information gathering

- ✓ Search engines
- ✓ Social networking sites for employees and organisations
- ✓ Company website / Annual reports
- ✓ Job ads / Employee resumes
- ✓ Online developers forums
- ~~✓ Whois records (Mumble attack example)~~
- ✓ Maltego
- ✓ Etc

* Now called OSINT

Reconnaissance (2)

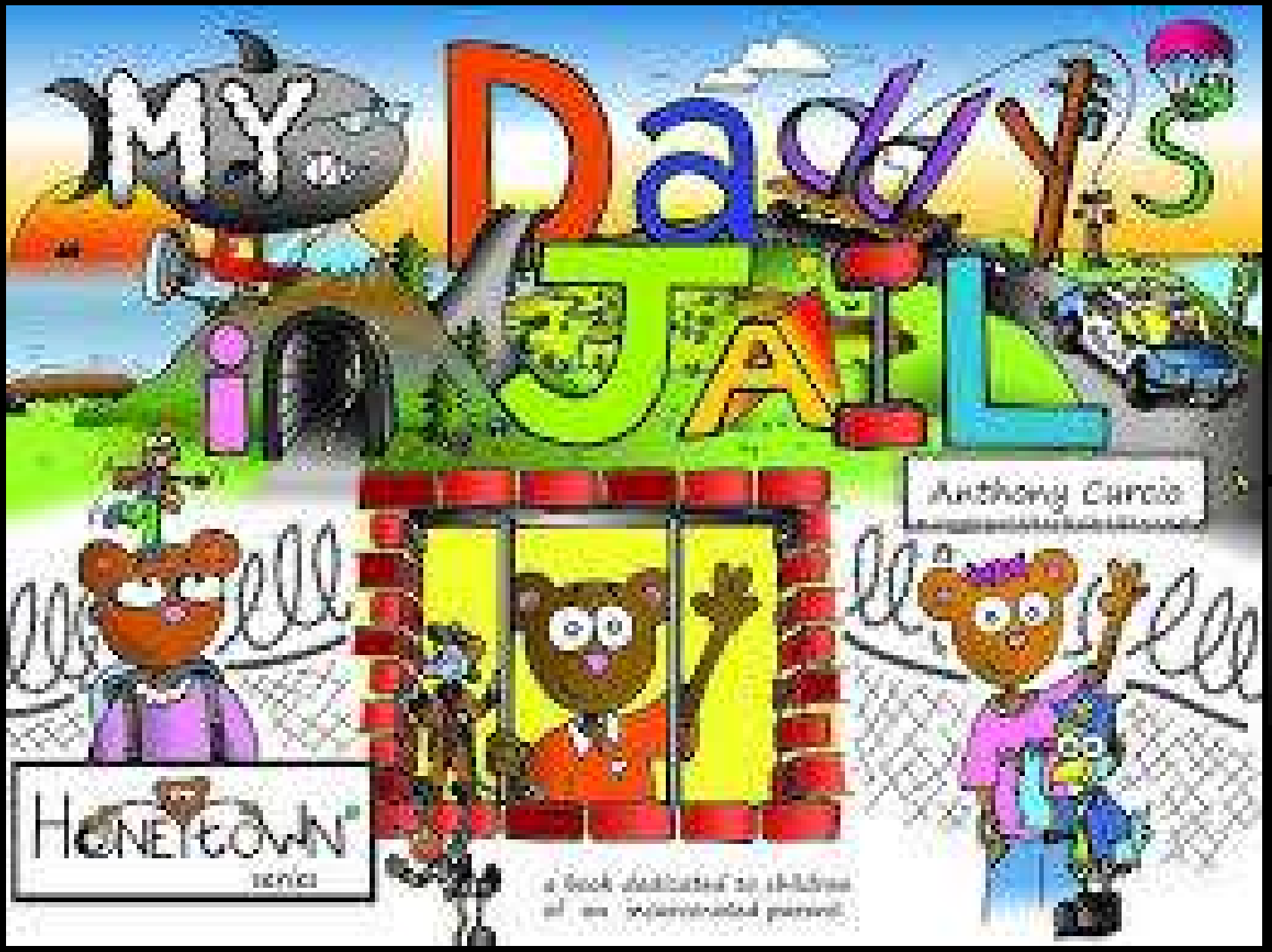
Physical reconnaissance

- ✓ Google Maps
- ✓ Where are the security guards?
- ✓ Do smokers congregate in a certain area outside?
- ✓ Where are the CCTV cameras?
- ✓ Watch staff movements. What time do employees go in / leave the office? What time do staff have lunch?
- ✓ Do staff wear and/or show passes? Can you copy them?
- ✓ Any unusual ways in? Fire escapes / garages /etc.

Creating Your Scenario

- ✓ Think about how sophisticated your attack needs to be
- ✓ More security focused organisations, eg, banks, will require a more complex attack
- ✓ Use props
  - mobile phones, recording devices, ID cards, cups of coffee, folders/documents to deliver...
  - costumes: security jackets, hard hats, cleaners overalls, clipboard, suit, courier, pest control...


ANTHONY CURCIO
CHILDREN'S BOOKS
COLORING BOOKS
SPEAKING
MEDIA
ABOUT
Life-Saving Arrest
AUTHOR. SPEAKER. YOUTH ADVOCATE.
COLORING BOOKS
CHILDREN'S BOOKS
Robbery of Life


MY
Daddy's
JAIL
Anthony Curcio
HONEYTOWN
series

Sample scenarios - phone

- ✓ Internal IT support
- ✓ Freelance IT journalist
- ✓ Recruitment agent
- ✓ Charity worker
- ✓ ISP abuse team member

Sample scenarios – on site

- ✓ Tailgate (not really a scenario but often works – try carrying two cups of coffee)
- ✓ Employee / Temp
- ✓ Delivery guy
- ✓ GirlfriendIboyfriend
- ✓ Workman / engineer
- ✓ Fire warden
- ✓ Cleaner/security/maintenance
- ✓ **Do not impersonate real people or organisations!**

Going in for the attack

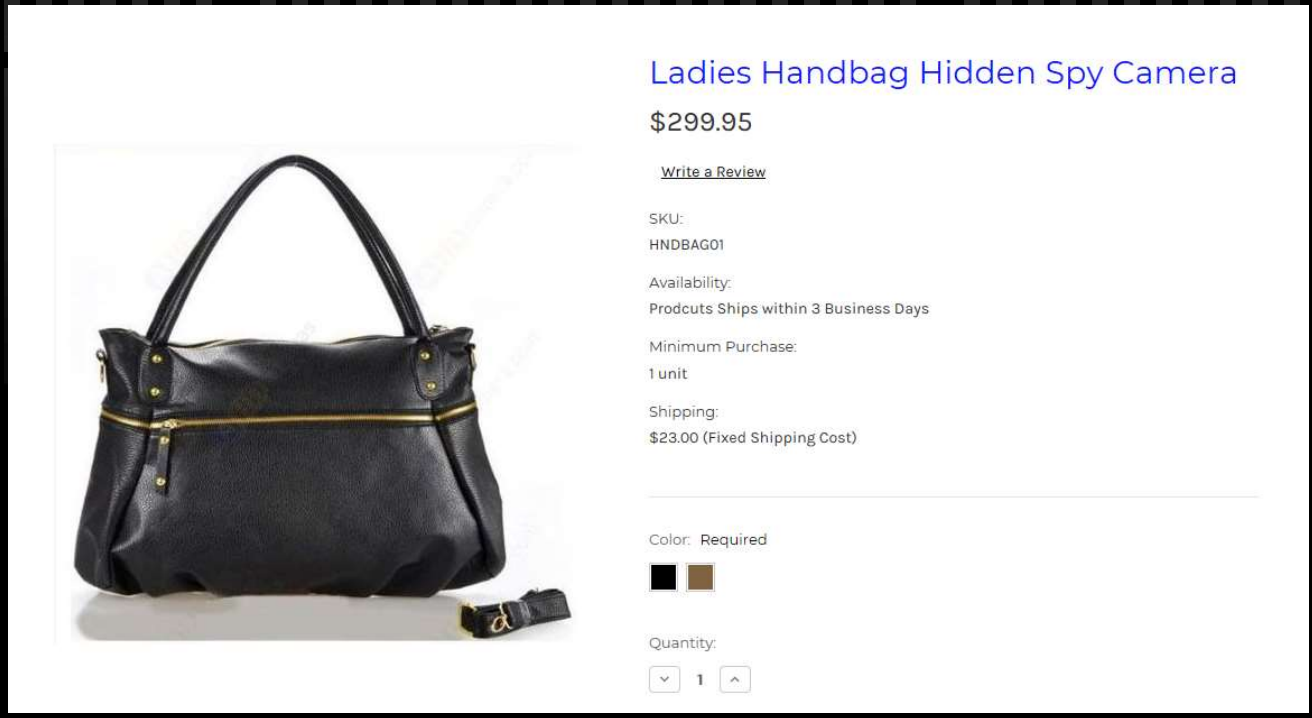
- Use your scenario to get in
- Gain access to network
- Prove you were there
  - Trophy gathering – physical and electronic
  - Leave a token
  - Take photos
  - Make some internal phone calls
- Have an exit strategy

The Times Top Ten Real-Life Spy Gadgets

1. Poison-tipped umbrella
2. Dart gun
3. Compass buttons
4. Exploding briefcase
5. Exploding rats
6. Cigarette-case gun
7. Hollowed-out lighter
8. Wallet document camera
9. Microphone in an olive
10. Rock bug

SE tools

- ✓ Loads of tools
- ✓ Cheaper kit



Reporting

- ✓ Tell the story
- ✓ Standard pen test report with methods used, vulnerabilities, recommendations
- ✓ Use photos and other evidence
- ✓ Don’t name individuals

A few tips

- ✓ Use a false name, but use your own first name.
- ✓ Consider using a surname that sounds like your own
- ✓ Be a woman (preferably a foreign one)
- ✓ Flirt / use flattery
- ✓ Offer an incentive (but not a bribe)
- ✓ Get a job

What can go wrong?

- ✓ You are recognised
- ✓ Balance of power backfires / you have played the wrong role
- ✓ Overcompensate by giving too much detail
- ✓ Laws you might break
  - Trespass, Deception, Breaking and Entering, Going equipped, Theft, Vandalism, Impersonating a government official, etc…
- ✓ BE PREPARED!

How to prevent SE attacks

- ✓ We still don't know
- ✓ Some combination of people, process, technology?

How to prevent social engineering attacks

- ✓ Education & Awareness
- ✓ Social engineering testing
- ✓ Security policy
- ✓ Vet your staff
- ✓ Get your staff involved
- ✓ Don’t trust anyone!

Questions

Social Engineering for Penetration Testers
Sharon Conheady

Brucon 2009, 2018