



# Social Engineering

Graeme Huddy, Manager: Information Security and IT Internal Audit  
Technology Advisory, KPMG South Africa



# Why is there a problem?

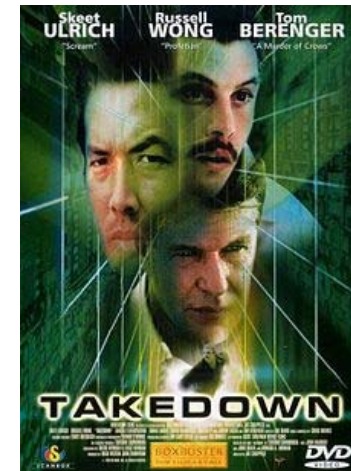
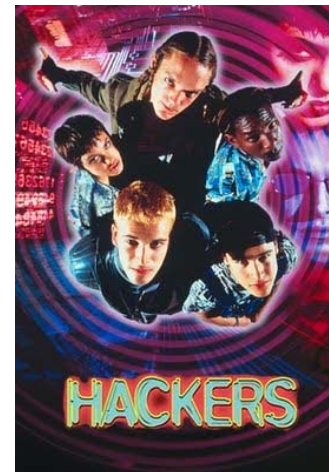
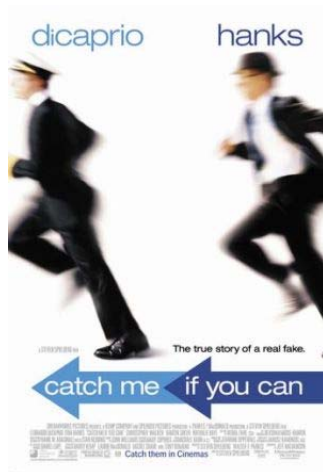
- “Accessing” people is easy:
  - If you look nice or sound nice you must be nice
  - Confidence counts
  - Default trust
  - Emotions and urgency make people make mistakes
  - People like exclusive opportunities
  - People like to feel important
  - People like to “share”
  - People are inquisitive
  - People like to help

# Agenda

- Why is there a problem
- The human weakness
- So what is out there (real life example)
- Choosing a target
- Sources of information
- Potential engineering attacks

# Wetware Hacking: Caper and Heists

- All computer systems are made up of three essential elements which are all co-dependent: Hardware, Software and Wetware - the users of the systems
- Wetware hackers exploit vulnerabilities in people. If successful it grants access quicker, easier, and is often harder to trace. It is also the most difficult to defend against



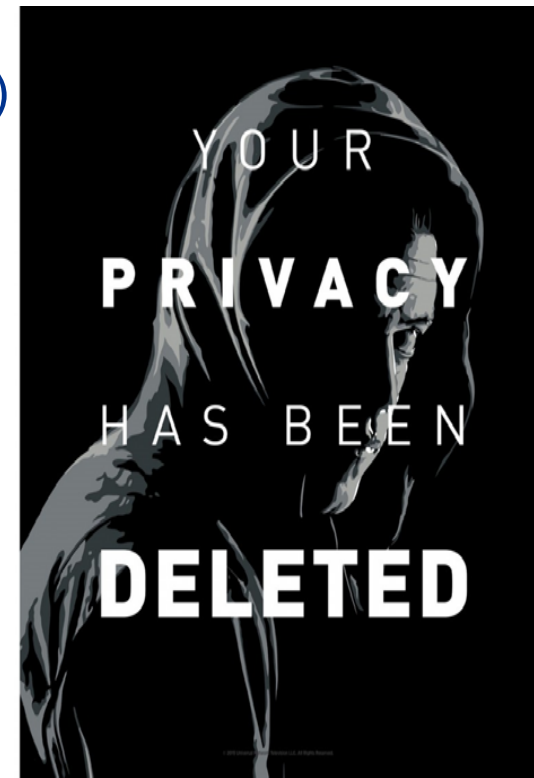
# Human attack payloads are simple

- Ask and ye shall receive – people are inherently helpful
- Impersonation – pray on the inability to verify
- Misleading – valid story, wrong intent (e.g. audit, here for a delivery, here to meet a friend etc.)
- Emotion – throws you off balance
- Flattery – a need to live up to the “hype” of your knowledge
- Terminology – know the company “slang”



# So what is out there (real life example)

- In 15 minutes, we were able to gather:
  - 30 individual's corporate email addresses
  - 2 personal mobile numbers
  - 2 passwords (part of larger password dump)
  - Various official letters with signatures
  - 1 home address



# Now lets choose a target

- A simple search in LinkedIn will provide us with a number of possible targets:
  - Managers?
  - User with system access?
  - Impersonation targets?
  - Disgruntles employees?
  - Whaling?

702 results for IITPSA



**Moira De Roche** 1st

E-Learning Project Leader at Freelance  
Cape Town Area, South Africa • E-Learning  
▶ 11 shared connections • Similar • 500+

Message

Current: Honorary Treasurer & Director at IITPSA - Institute of Information ...



**Gail Sturgess** 2nd

Helping IT organisations create an architecture for effective Career  
Pathing and Talent Management at TalentAlign.  
Cape Town Area, South Africa • Information Technology and  
Services  
▶ 11 shared connections • Similar

Connect

Current: EXCO member and Director at IITPSA (formerly CCSA)



**Darin Morris** 1st

Senior Software Engineer, Entrepreneur  
Cape Town Area, South Africa • Information Technology and  
Services  
▶ 15 shared connections • Similar • 500+

Message

Past: Western Cape Chapter Chairperson at Institute of IT Professional...  
...Professionals of South Africa (IITPSA) is a professional... Industry.  
IITPSA's aims are to further the study...

# Lets go down the rabbit hole

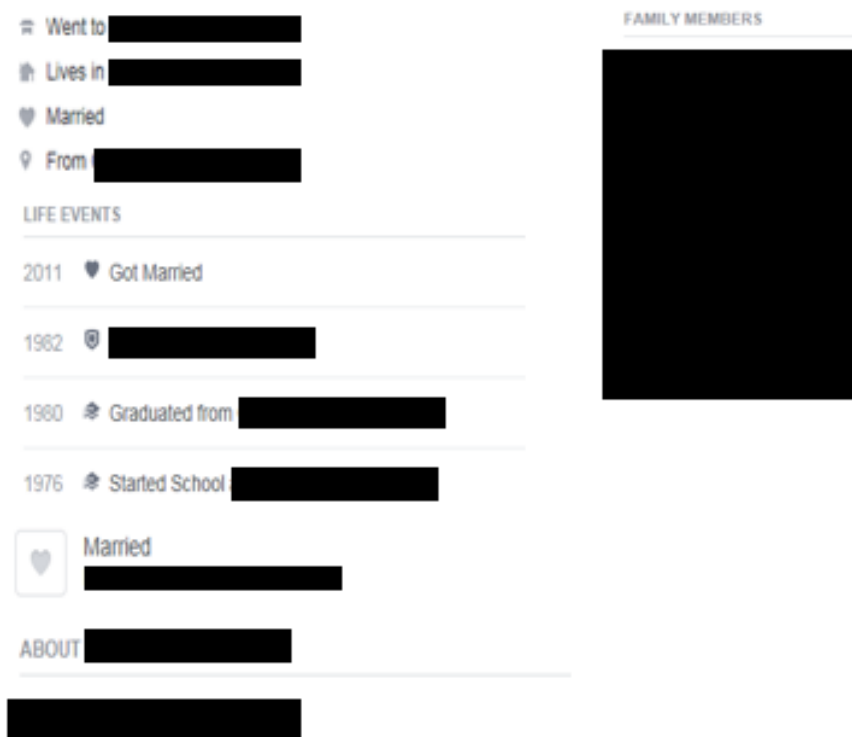
- LinkedIn trawling reveals a sensitive Systems Administrator
  - High levels of access
  - Potential for immediate financial gain
  - Further data access possibilities
  - Multiple exploitation opportunities
    - Change employee bank details
    - Add 'ghost' employees
    - Identify highly paid employees for further attacks
    - Etc.





# Social media is all about sharing

- Facebook is just the beginning, but it's a rich source of data
  - Location
  - School
  - Home town
  - Family
  - Friends
  - Events



# Other sources of information

- Google (always!)
- Public records
- Newsletters
- Genealogy sites
- Geo-data
- Societies
- Church committees
- Whois (especially SME's)

# What would someone do with this?

- Phishing, using email to harvest a persons sensitive details using crafted emails, websites and anything else
- ID theft, using information about a person to impersonate them in order to steal money, credit, even -in one case- a house
- Privacy Invasion, selling personal information to other people for purposes ranging from marketing to robbery
- Malware, using cleverly crafted emails, corporate USB gifts or hijacking of commonly visited web pages to get users to install software - or allow it to be installed - which gives an attacker access
- Syndicate targeting – blackmailing using information available or physical threats against friends and family to extort users



# An example of a phishing email

Exciting opportunity - Signup now! - Message (HTML)

FILE MESSAGE INSERT OPTIONS FORMAT TEXT REVIEW ADOBE PDF

Cut Copy Paste Format Painter Clipboard

Basic Text

Names

Include

Tags

Zoom

Follow Up High Importance Low Importance

To... <target>

Cc...

Bcc...

Send

Subject Exciting opportunity - Signup now!

Dear member

In our continuing efforts to ensure that we are equipped to provide services to our members in an increasing connected environment, we is in the process of evaluating a number of **mobility solutions** that we feel will be of **great benefit to our members**. One of the solutions that we are in the process of trialling is the use of products in the **Apple© technology suite** (e.g. iPhones, iPads, iWatches etc). We believe that **Apple© devices** offer a secure application ecosystem, reliability and easy to use user interface which will help **to improve efficiencies** and provides opportunities to **innovate at a reduced cost** in the long term.



In order to ensure that these products are aligned to our member's requirements, **Apple© has sponsored a number of devices** and we are requesting members to **volunteer to receive an Apple© device** and to test various applications over the 3 month trial period. You have been selected to participate in this process and are requested to register on the [IITPSA website](#).

Please note that we do expect that some members will choose not to participate in this testing process - **devices numbers are limited** and will be allocated on a **first-come-first-serve basis**.

In addition to registering, a member of the **IITPSA Mobi Team** will be contacting you during the course of **25 – 29 July 2016** to discuss further exciting mobility initiative.

Should you have any questions regarding this process please do not hesitate to contact us at [mobiteam@iitpsa.mobi](mailto:mobiteam@iitpsa.mobi).

Regards  
**IITPSA Mobi Team**

# An example of a phishing email

https://www.iitpsa.mobi/membersform.html

Search

**IITPSA**  
Institute of Information Technology Professionals  
South Africa

**Application Form**

Membership Details:

Full name	<input type="text"/>	Employer	<input type="text"/>
Please enter your names correctly as per the sequence in your passport (First name, Middle names, Last name (Surname))		Branch	<input type="text"/>
Title	<input type="text"/>	Industry	<input type="text"/>
Job Title:	<input type="text"/>	ID Number	<input type="text"/>
Date of Birth	<input type="text" value="dd/mm/yyyy"/>	Passport Number	<input type="text"/>
Postal Address	<input type="text"/>	Language	<input type="text"/>
	<input type="text"/>	Invoice Address	<input type="text"/>
	<input type="text"/>		<input type="text"/>
City	<input type="text"/>	City	<input type="text"/>
Postal Code	<input type="text"/>	Postal Code	<input type="text"/>
Province	<input type="text"/>	How did you hear about IITPSA?	<input type="text"/>
Office Tel	<input type="text"/>	Email	<input type="text"/>
Cell No:	<input type="text"/>	Website	<input type="text"/>

# USB Candy Drop

- If a USB drive labelled “Staff increases 2016” or “Restructuring plans” etc. was left lying around the office – what would happen?
- Our hit rate is currently 50 – 70%
  - i.e. More than half of those that find our planted USB devices can’t resist the temptation to see what is on them
- What can happen when you open the contents of the USB?





# How do I protect myself?

- Change your privacy settings immediately, and retrospectively apply it to all prior content
- Don't list your personal information on any service that displays it publically or to other members without your consent or notification
- Don't use your corporate email address for personal services
- Be careful what you share
- Be cautious of anyone, ANYONE, asking for your details
- Keep everything up to date, and browse carefully
- Clean any pictures of EXIF data



Thank you



[kpmg.com/socialmedia](http://kpmg.com/socialmedia)



[kpmg.com/app](http://kpmg.com/app)

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2016 KPMG Services (Pty) Ltd, the South African member firm of KPMG International, a Swiss cooperative. All rights reserved.

The KPMG name, logo are registered trademarks or trademarks of KPMG International.