

Information & Communication Security (SS 2020)

Social Engineering

Dr. Sebastian Pape

Chair of Mobile Business & Multilateral Security
Johann Wolfgang Goethe University Frankfurt a. M.



SOcial
Engineering
Academy

- Dr. Kristian Beckers
- Peter Schaab
- Veronika Fries
- Daniel Schosser
- Dr. Dennis-Kenji Kipker
- Stefanie Wojak
- Michael Sailer
- Corina Hoppenz



SOcial
Engineering
Academy



Icons: Flaticon, 123RF, Pixabay

- Social Engineering
 - Definition + Examples
 - Tools
 - Counteracting Training Strategies
 - Serious Games



definition social engineering

All Images Videos News Shopping Maps Books

About 12,600,000 results

Any time

Past hour

Past 24 hours

Past week

Past month

Past year

social engineering

noun

1. the use of centralized planning in an attempt to manage social change and regulate the future development and behaviour of a society.
2. (in the context of information security) the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

[Source: Google.com]

Social Engineering - Background

Social Engineering



The clever
manipulation
of the natural human
tendency to trust!

Source: cybertec-security.com

Breach vectors leading to compromise:



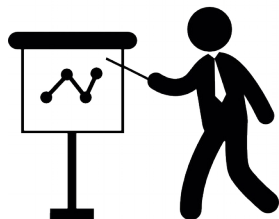
Source: PWC Information Security Breaches Survey 2017



Who has already applied Social Engineering?



Who has been attacked by Social Engineering?



Who had a training on Social Engineering?

Historic Example (1925) Victor Lustig

'SMOOTHEST CON MAN EVER BORN!'



"Count" Victor Lustig, in center (even the title is bogus), is shown being questioned by Robert L. Godby (right), U. S. agent in charge in New York, and Peter A. Rubano, Secret Service Agent, concerning the \$52,000 counterfeit money found cached in a subway locker at Times Square. Other agents described Lustig as the "slickest bunko man who ever lived." Picture by Evening Journal

EVENING PUBLIC LEDGER—PHILADELPHIA,

LUSTIG GETS 20-YEAR TERM IN ALCATRAZ

Count Victor Lustig, king of con men and counterfeiters, yesterday was doomed to join Al Capone and other deluded underworld Napoleons in the federal "tomb" on Alcatraz Island.

Lustig will be exiled in the impregnable fortress in the Pacific for twenty years. He will serve five



"Count" Victor Lustig Gets twenty years sentence.

years for his desperate escape from the Federal House of Detention in West St., and fifteen years for counterfeiting. He is now 46. While Federal Judge Alfred C. Coxie did not specify that Lustig should go to Alcatraz, other Government officials said the king con man's fate had already been decided.

Lustig took the sentence calmly and glanced stonily at spectators who filled the courtroom to standing. Seeking leniency, Lustig's counsel pointed out that the "Count" had generally victimized persons whose own practices were sharp—such as Chicago rangers, Arnold Rothstein, and other under-

world leaders in New York and Boston."

"I understand," commented Judge Coxie, "that the law is no respecter of persons."

He was arrested last May on a counterfeiting charge and sent to the House of Detention in default of \$50,000 bail. He escaped Sept. 1 by sliding from a window on the third floor on a rope of knotted sheets.

He was re-captured in Pittsburgh Sept. 28, and returned here to the Tomb. He pleaded guilty to the escape and counterfeiting charges on Nov. 20.

Sentenced with Lustig yesterday on the counterfeiting charge was William Watts of Union City, N. J. He will go to the Federal Northeastern Penitentiary at Lewisburg, Pa., for ten years. Watts and Lustig were also fined \$1,000 each.

'THE COUNT' ESCAPES JAIL ON SHEET ROPE

International Crook Drops 50 Feet to Street in Sight of Hundreds on West Side.

BOASTED HE WOULD FLEE

Had \$51,000 in Counterfeit Bills When Arrested—Faced Trial Tomorrow.

Sept. 2, 1925

Victor (The Count) Lustig, the dignified 46-year-old confidence man whose money-making schemes have kept the police at two continents busy for twenty-seven years, escaped from the Federal Detention Headquarters at 407 West Street shortly before 1 o'clock yesterday afternoon.

He made his exit in full view of perhaps a hundred persons via a rope of nine bedsteads knotted together, sliding fifty feet from a third-floor dormitory window into oblation West Eleventh Street, in Greenwich Village.

The Count had been in the detention prison under \$50,000 bail since May 12, when secret service agents caught up with him at Seventy-fourth Street and Broadway, and with a key they said they found on him, opened a locker in the Times Square subway station that contained \$51,000 in counterfeit banknotes and the engraved plates from which they were made. He was to have been brought to trial tomorrow for possession of the notes.

Boasted He Would Escape.

'THE COUNT' FLEES JAIL ON SHEET ROPE

Continued From Page One.

In almost frightened the witness away, but he summoned up his courage.

"Mister," he said, "did you know that a man just escaped from the third floor?"

The wicket alarmed shut, and a few moments later the swinging rope of sheets was hauled back into the jail. Detective Frank Campbell of the Charles Street police station responded to the call for police. He said later that the prisoner apparently had cut his way through a wire cutting with a sharp instrument. The bed sheets, collected from nine of the forty beds in the dormitory, were fastened to a brace inside the window.

Beginning at 1:17 P. M., the following police alarm was broadcast at intervals over the police radio system, and over the teletype machines to the Eastern States, eventually to be relayed nationally.

"Code Signal a reckless streets patrolman to watch ferries, bridges and avenues of escape from the city."

"Escaped from the Federal Detention prison at Eleventh Street and West Street, N. Y. C., Robert V. Miller, alias Count Lustig, 46, 5 feet 7, 140 pounds, blond, partly bald, brown eyes, scar over right eye, was being held in \$50,000 bail for possession of counterfeit money. Wanted by the Sixth Squad."

Believe Aisle Was Walling.

The police advanced the theory that the escape was well planned, and that one of the count's friends had picked him up in an automobile on West Street. They said that the blue knickerbocker and slippers that constitute the prison garb would have brought about his capture by the first patrolman he met if he had tried to escape further afoot.

At the jail a voice told inspectors that the superintendent was away, talked the policeman about the incident—how, for example, the Count had been able to collect nine sheets and bend them together, cut a hole in the mesh covering the window, and escape while he was supposed to be relaxing on the roof—the voice said, "I'm sorry."

Under so many aliases that the police have never been able to determine his real name, Lustig has peddled his trade all over Europe and the United States since 1906, serving short terms in Europe in the old days for petty swindles. Of the dozens of aliases with the police in the United States only one conviction appears on the imposing record sheet. That was in Oklahoma City in 1920, when he was fined \$10 and costs over a matter of morals. He has jumped bail in a half dozen instances, and has at least one previous jail break to his credit. In 1927, as Albert Gramman,



FLEES FEDERAL PRISON.

Victor (The Count) Lustig.

he saved his way out of Lake County jail at Crown Point, Ind., the same jail that John Dillinger escaped from with a wooden pistol. He started his career in Prague, under the name of Lustig, where in 1908 he served two months in jail for a petty theft. Up to 1912 he had served a half dozen terms in Austria and Switzerland. In 1917, as Robert Lamsky, a "salesman," he was arrested in St. Louis for Denver authorities, and jumped his bail in Denver.

The next year Denver got him again, this time as Volter Lustig, and the crime was a confidence card game. He left town and his bond was again forfeited. Omaha had him for a swindle, but couldn't prove a case against him.

Through the Nineteen Twenties, as George Shabo, Victor Gross, Charles Gruber, Robert Duval, Charles Gruber, Albert Phillips and Albert Gramman, he saw the inside of detention cells from San Francisco and Los Angeles, via Chicago, Detroit, Indianapolis and Crown Point to New York.

Complaints charged he sold them money-making machines, interested them in card games of stock pools, and passed bad checks.

Swindled a Texas Sheriff.

The Count moved in the best circles, dressed in dignified clothes and talked with a clipped accent. His jokes won most victims over readily. He sold one of his money-making machines to a Texas sheriff for \$125,000 in cash.

In 1920 he ran out of funds in Paris while he was in Europe buying choice vineyards for the Jack (Lep) Diamond interests and got into difficulties with the French authorities that resulted in his expulsion from the country by governmental decree.

As Robert V. Miller he was arrested in New York for Newark authorities in 1920, but was released. In the next several years he was arrested for various swindles in South Eagle Pass, Texas, as J. H. Richards as G. H. Werner in Fort Worth and as Robert G. Wagner in Miami. In no case was there sufficient evidence to hold him.

He was reputed, although this was never substantiated, to have

been the count mentioned in the cover of Jules W. (Nooky) Armstrong. The counterfeiting equipment found in the Times Square locker in May was responsible for a flood of nearly perfect \$100, \$20, \$10 and \$5 bills throughout this country and Canada, according to the authorities.

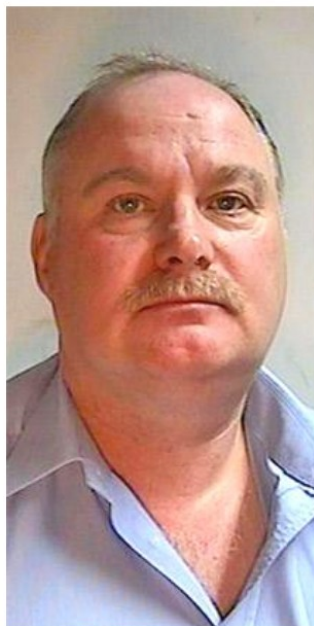
[Source: Updated newspaper reports (Courtesy of the US Secret Service) via <http://numismatics.org/>]

News > UK > Crime

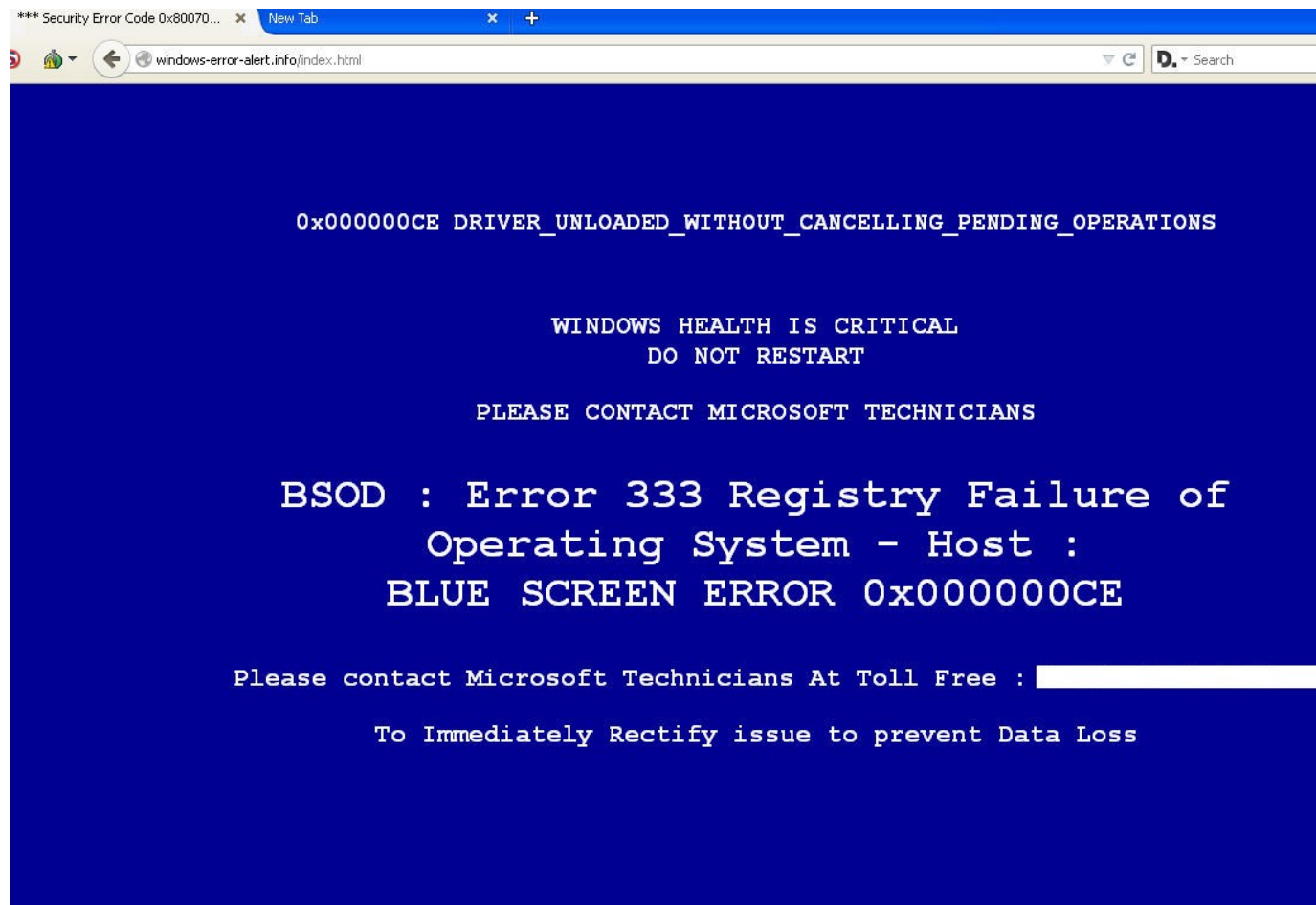
The man who tried to sell the Ritz

When Anthony Lee offered buyers the hotel on the cheap, the deal looked too good to be true. It was — he didn't own it

By Mark Hughes | Wednesday 28 July 2010



[Source: <https://www.independent.co.uk/news/uk/crime/the-man-who-tried-to-sell-the-ritz-2036914.html>]



Source: <https://blog.malwarebytes.com>

From Prof. Dr. Kai Rannenberg <departmenthead31@gmail.com> ☆

Subject **Are you available?**

To Me <sebastian.pape@m-chair.de> ★

Hello,

I need a favour from you kindly email me back soon as possible.

Regards,

Prof. Dr. Kai Rannenberg

Chair of Mobile Business & Multilateral Security

Deutsche Telekom

Sent from my iPad

From Robert Miller <robert.miller@education1.teaching-research-group.com> ☆

Subject **Contact request for faculty application**

To Me <sebastian.pape@m-chair.de> ★

Date Mon, 21 Jan 2019 18:33:22 +0100

Message ID <cc84e326e33df1619ee59bd88c23870a@teaching-research-group.com>

Mime-Version 1.0

Hello, my name is Robert Miller. I am a professor interested to apply to your institution. Could you please provide me with an email address for your human resources manager and academic affairs director (dean of faculty)? Thank you very much in advance for your support. Kind regards
Robert Miller

What happened here?

Hey I know you don't know me, but many years ago I used to have your number. I'm trying to log in to an old account that is still tied to XXXXXXXXXXX but it's telling me that it will send me a verification code. I'd like to know if it'd be okay with you if I request the code and if you can just text it back to me? If not, that's totally fine.

Thank you so much!!

I just requested it

You're a life saver. Thank you so much and sorry for bothering

Ok

6637946

Example: Vishing (Video)



[Source: <https://www.youtube.com/watch?v=lc7scxvKQOo>
<https://www.youtube.com/watch?v=F78UdORII-Q>]

INVESTMENT SCAMS

Common investment scams may include lucrative investment opportunities such as shares, bonds, cryptocurrencies, rare metals, overseas land investments or alternative energy.

WHAT ARE THE SIGNS?

- You are promised quick returns and assured that the investment is safe.
- The offer is only available for limited time.
- You receive an unsolicited call, repeatedly.
- The offer is only available to you and you are asked not to share it.



[Source: <https://www.europol.europa.eu/sites/default/files/documents/uk.pdf>]

Social Engineering Components

Technical, non-technical
means

Social interaction to
manipulate

Disclosure of sensitive
information or other
damage

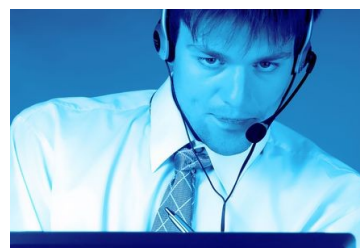


- Mass attacks, Phishing
 - Attack large number of people
 - Less sophisticated
 - Less successful (per attack)
 - More potential victims



- Targeted attacks, Spear Phishing
 - Attacks on specified individuals
 - More sophisticated
 - More promising (per attack)
 - Less victims
 - Can target a specific aim better

- Pre Engagement Interactions
- Intelligence Gathering
- Pretexting / Relation
- Exploitation
- Post-Exploitation



[Source: Milosevic. Introduction to Social Engineering, 2013.]



INTERPOL

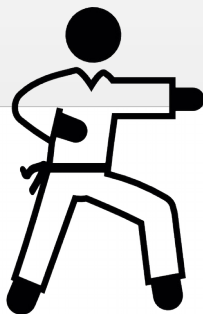
4 WHY DO PEOPLE LET THEMSELVES GET TRICKED?

Social engineering techniques are becoming extremely sophisticated and messages often appear to be very professional. The criminals know how to manipulate people and can be very convincing.

Criminals exploit a person's trust or their willingness to help others, or simply use intimidation to achieve their results.

Despite this, there are some simple steps you can take in order to protect your data.

Why does it work?



INTERPOL
MSELSVES GET TRIC



Social Engineering Attack Scenarios

Popup window

Generates a pop up window stating some problem and requests your victims to reenter their credentials to continue with their work.

1



Social Engineering Principles

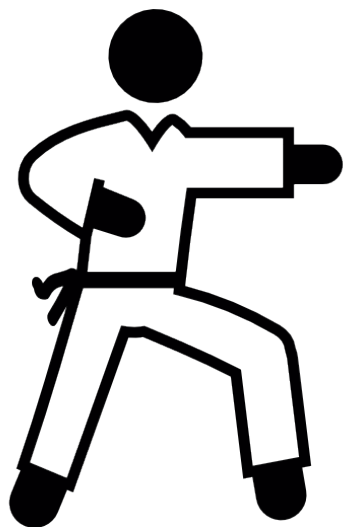
The Need and Greed Principle

Their needs and desires make your victims vulnerable. Find out what your victims really want and use it to exploit them.

2

[Source: www.interpol.int]

Social Engineering Attacks



- Gulati, R.: The threat of social engineering and your defense against it. SANS Reading Room (2003)
- Peltier, T.R.: Social engineering: Concepts and solutions. Information Systems Security 15(5) (2006) 13–216
- Krombholz, K., Hobel, H., Huber, M., Weippl, E.: Social engineering attacks on the knowledge worker. In: Proceedings of the 6th International Conference on Security of Information and Networks. SIN '13, New York, NY, USA, ACM (2013) 28–35
- Chitrey, A., Singh, D., Singh, V.: A comprehensive study of social engineering based attacks in india to develop a conceptual model. International Journal of Information and Network Security (IJINS) 1(2) (2012) 45–53

- Phishing
- Shoulder Surfing
- Dumpster Diving
- Reverse Social Engineering
- Baiting
- Direct approach
- Tailgating
- Support Staff
- Voice of Authority
- Mail attachment
- Popup window
- Third-Party Authorization
- Impersonation

Psychological Principles

- Distraction Principle
- Social Compliance Principle
- Herd Principle
- Dishonesty Principle
- Deception Principle
- Need and Greed Principle
- Time Principle
- Desire to be Helpful
- Laziness
- Fear of Getting Into Trouble
- Tendency to Trust People
- Curiosity
- Guilt
- Fear of the unknown
- Fear of losing something
- Diffusion of Responsibility
- Ignorance / Carelessness

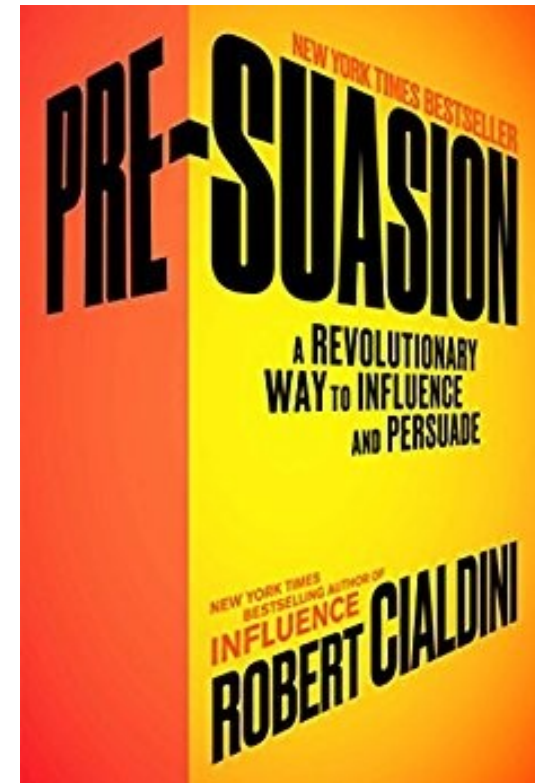


Stajano, F., Wilson, P.: Understanding scam victims: Seven principles for systems security. *Commun. ACM* 54(3) (March 2011) 70–75

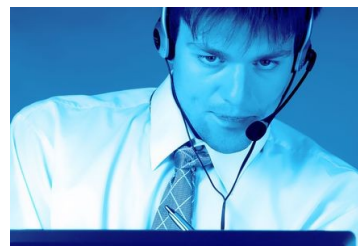
Gulati, R.: The threat of social engineering and your defense against it. *SANS Reading Room* (2003)

Peltier, T.R.: Social engineering: Concepts and solutions. *Information Systems Security* 15(5) (2006) 13–216

- List of “yes”-questions
- Story of vacuum cleaner sales representative



- Pre Engagement Interactions
- Intelligence Gathering
- Pretexting / Relation
- Exploitation
- Post-Exploitation



[Source: Milosevic. Introduction to Social Engineering, 2013.]

Social Engineering Information

Communication Channels



LinkedIn



WhatsApp



Relations



User Credentials



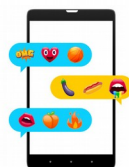
Locations



Job Positions

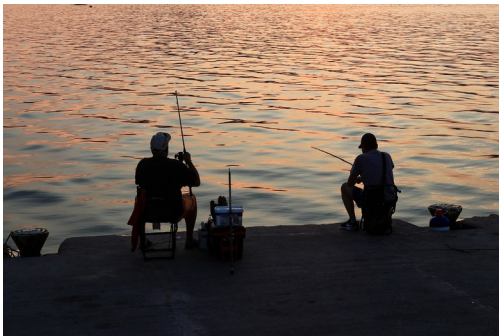


Company Lingo



Personal Information





Phishing

- Communication channels
- Company knowledge



Baiting

- Locations (walking routes)
- Company knowledge



Impersonation

- Information about a single person
- Company knowledge

- Input

- Google Search "social engineering and tool or application or script or webpage"
- List by Hadnagy
- Consents of 3 researchers

- Analysis

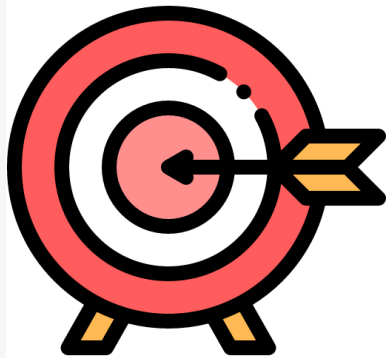
- General Overview of Tool

- Mapping to Attack Types

- Output of tools' information types
- Mapped information types to Attack types (Phishing, Baiting, Impersonation)
- Mapped Tools to Attack Types

C. Hadnagy. Social engineering: The art of human hacking. John Wiley & Sons, Indianapolis, 2010.





Purpose



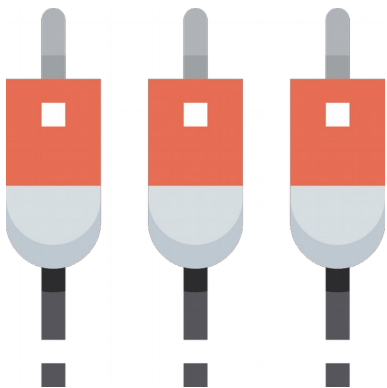
Price



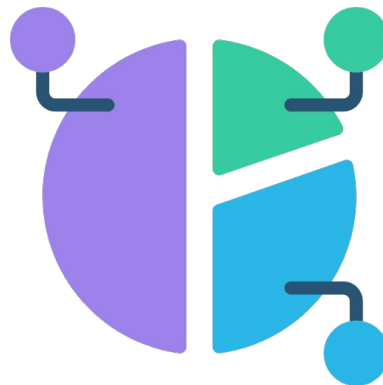
Usability



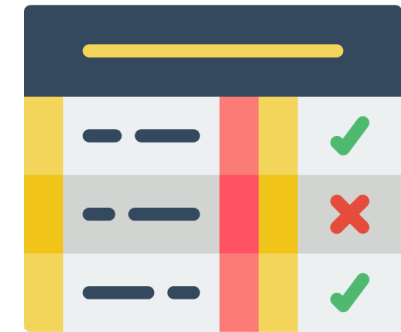
Counter Measures



Input Parameters



Output Visualisation

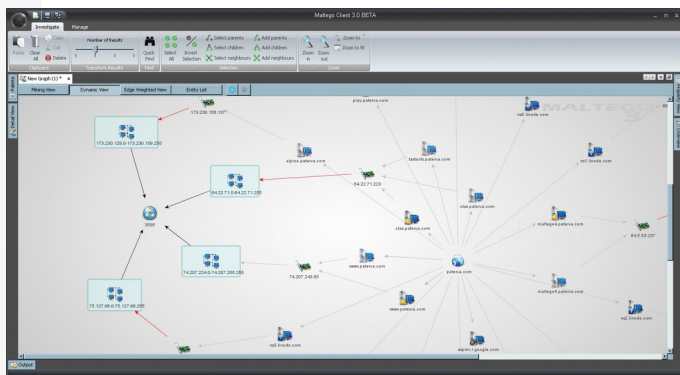


Sorting & Ranking

Mapping of SE Characteristics to Attack Types

		Attack Type		
		Phishing	Baiting	Impersonation
Communication	Telephone Number	x		
	Friends	x		x
	Personal Information	x		x
	Private Locations	x		x
	EMail	x		
	Instant Messenger	x		
	Co-Workers: Communication			x
Company Knowledge	Co-Workers: New Employee			x
	Co-Workers: Hierarchies			x
	Lingo	x		x
	Facilities: Security-Measures		x	x
	Facilities: Company Location		x	x
	Websites	x		
	Policies: Software		x	
	Policies: Network		x	
	Policies: Organization		x	

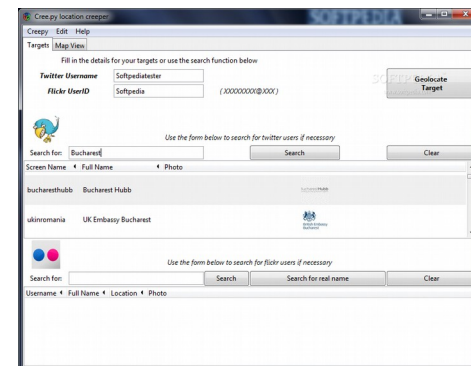
Social Engineering Tools



Maltego



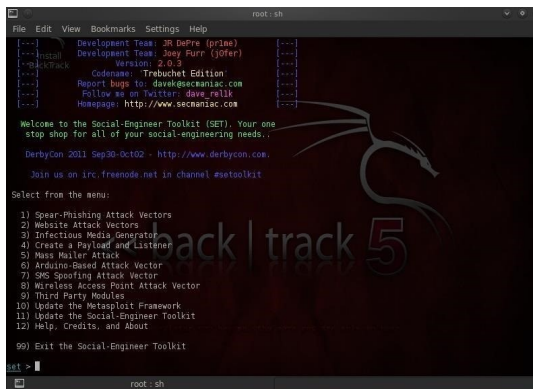
Recon-ng



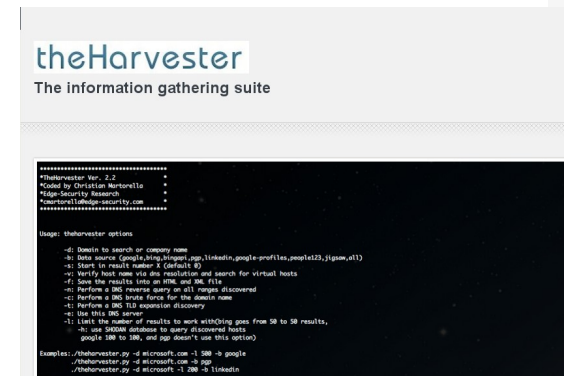
Cree.py



Spokeo

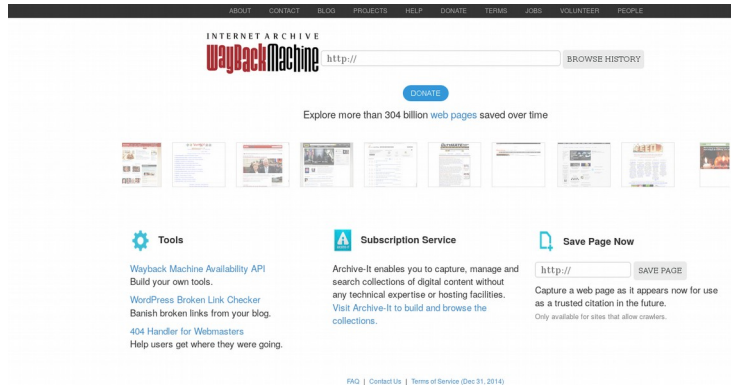


SET

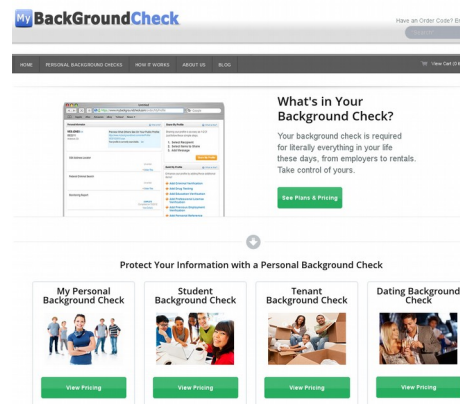


theHarvester

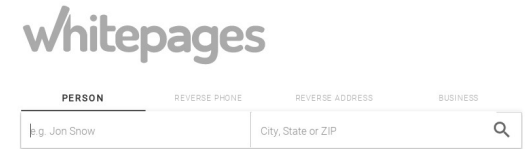
Social Engineering: Webpages + X



Wayback Machine

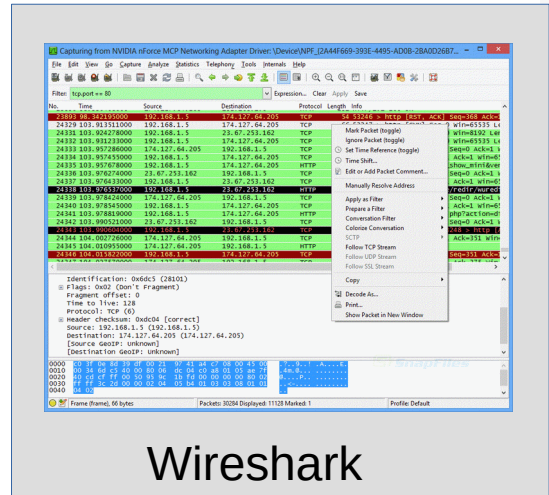


Background Checks



Whitepages
People Search
Find Contact Information on yourself or anyone else.

- Tax Records (e.g. US, Sweden)



Wireshark

Social Engineering Attack Potential

	SET	Maltego	Recon-ng	Cree.py	Spokeo	Wayback Machine	theHarvester	knowem.com	Whitepages	Instant Checkmate	freebackgroundcheck.org
Search by Person/ Company	○	+++	+++	+++	+++	+++	+++	+	+++	+++	+++
Retrieve E-Mail Address	○	+++	+++	○	○	○	+++	○	○	○	○
Retrieve Username/ Password	○	○	+++	○	○	○	○	○	○	○	○
Retrieve Job-Title	○	○	+++	○	○	○	○	○	○	+++	+++
Retrieve Locations	○	+	+	+++	+	○	○	○	+++	+++	+++
Retrieve Personal Data	○	○	○	○	+++	○	○	+	+	+++	+++
Usability	+	+	+	+++	+++	+++	+	+++	+++	+++	+++
Visualize Output	+	+++	+	+++	+++	+++	+	+++	+++	+++	+++
Retrieve Company Lingo	○	○	○	○	○	○	○	○	○	○	○
Free to use	+++	+++	+++	+++	○	+++	+++	+++	+++	○	○

Tool Coverage of Communication Channels

	Cree.py	Gitrob	KnowEm	LinkedIn	Maltego	Namechk	Recon-ng	Spokeo	theHarvester	Wayback Machine	Wireshark	Xing
Telephone Number							x					x
EMail				x	x		x		x			x
Instant Messenger			x		x	x		x				x
Friends			x	x	x	x						x
Personal Information	x		x	x		x		x				x
Private Locations	x							x				x

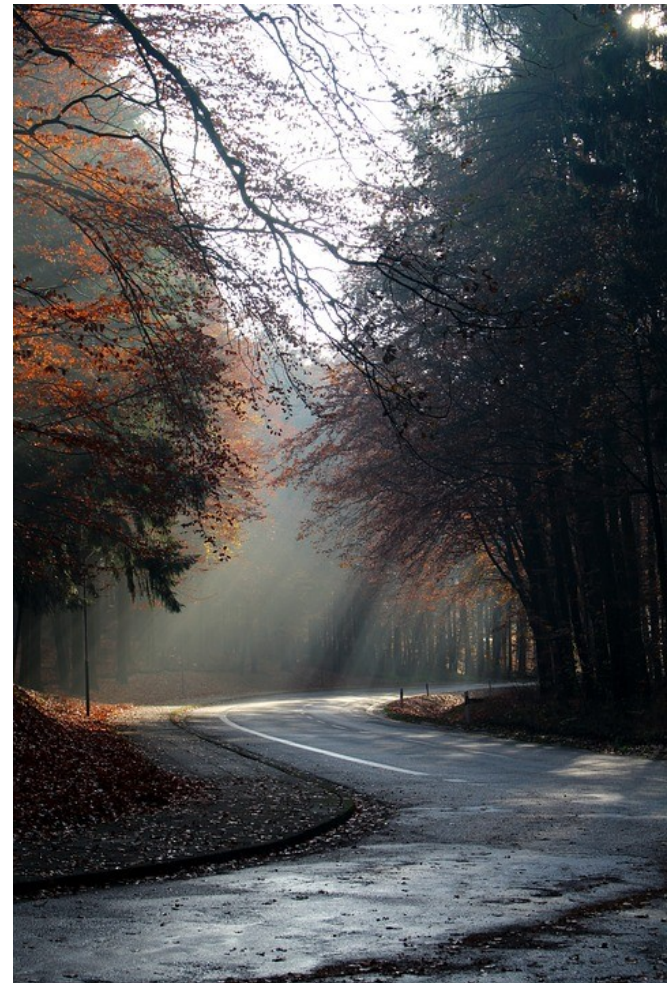
Tool Coverage of Company Data

	Cree.py	Gitrob	KnowEm	LinkedIn	Maltego	Namechk	Recon-ng	Spokeo	theHarvester	Wayback Machine	Wireshark	Xing
Company Locations	x			x			x	x	x			x
Company Lingo												
Special Knowledge				x	x		x					x
New Employees				x	x							x
Hierarchies				x	x							x
Websites					x		x		x	x		
Facility Security Measures		x									x	
Security Policies		x							x		x	
Software Policies		x					x				x	

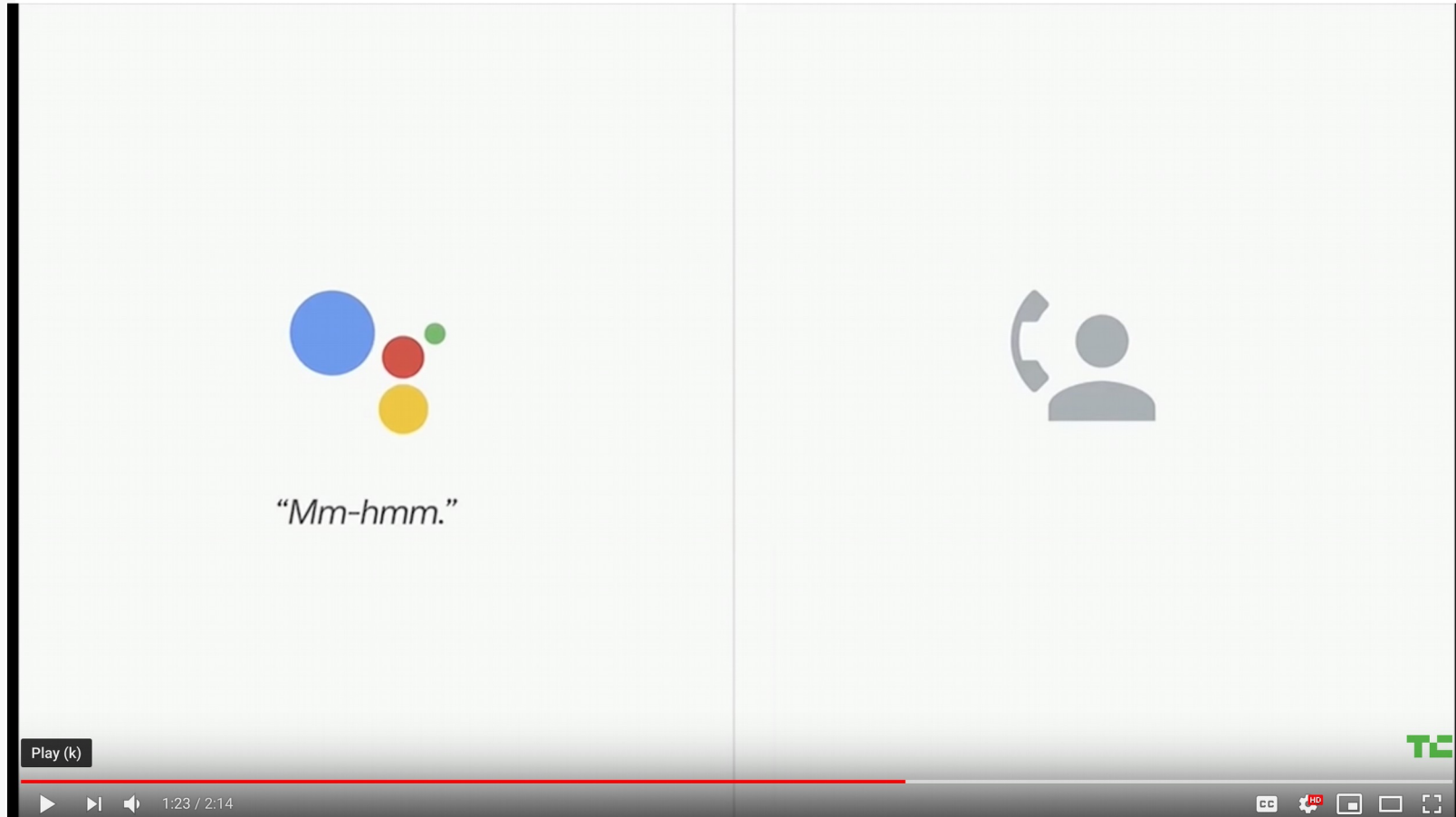
Tools Mapped to Attacks

	Cree.py	Gitrob	KnowEm	LinkedIn	Maltego	Namechk	Recon-ng	Spokeo	theHarvester	Wayback Machine	Wireshark	Xing
Telephone Number							P					P
Friends			P,I	P,I	P,I	P,I						P,I
Personal Information	P,I		P,I	P,I		P,I		P,I				P,I
Private Locations	P,I							P,I				P,I
E-Mail				P	P		P		P			P
InstantMessenger			P		P	P		P				P
Co-Workers: NewEmployee				I	I							I
Co-Workers: Hierarchies				I			I					I
Lingo												
Facilities: Security-Measures		B,I										B,I
Facilities: Company Location	B,I			B,I			B,I	B,I	B,I			B,I
Websites					P		P		P	P		

- Variety of tools exist
 - Allow non-experts to gather information
 - Company Lingo not covered
- None of the tools refers to countermeasures
 - Risk Assessment of available information
 - Propose policies depending on outcome
- Outlook
 - More tools
 - More data
 - Machine learning / Automated attacks



Robocalls: Google-Assistant



Source: https://youtu.be/7gh6_U7Nfs?t=44



- Training
- Policies
 - e.g. 4 eyes principle
- Awareness Campaigns
- Audits / Penetrations Testing

Indications of Social Engineering

- No contact information
- Haste
- Naming known persons
- Intimidation
- Small mistakes
- Asking for secrets or confidential information



- Social engineering attacks are difficult to predict:
 - Based on human behaviour
- Awareness trainings are
 - often forced
 - have no lasting effect
 - not specific





- The policy should ...
 - ... refer only to available standards
 - ... contain instructions and no vetos
 - ... be short, clear and consistent
 - ... be updated regularly

“Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly.” [NIST Special Publication 800-16]



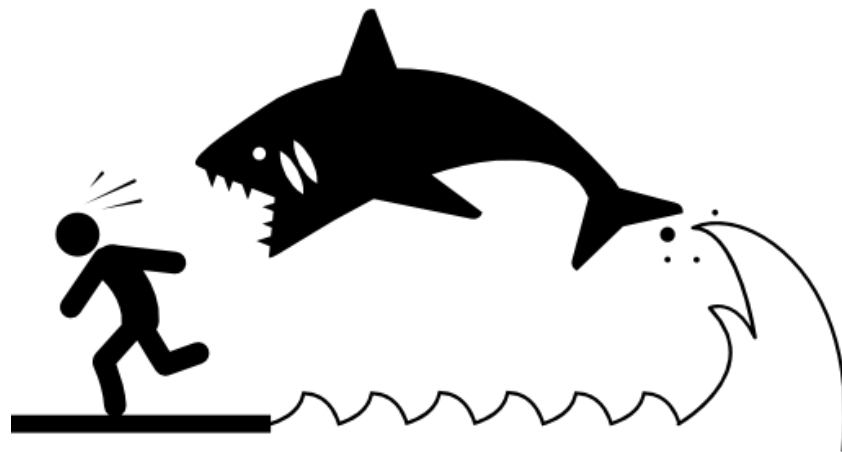
Important success factors:

- 1) professionally prepared and organised
- 2) invoking fear in people is not an effective tactic
- 3) security education has to be more than providing information to users – it needs to be targeted, actionable, doable and provide feedback
- 4) once people are willing to change, training and continuous feedback is needed
- 5) emphasis is necessary on different cultural contexts and characteristics when creating cybersecurity awareness campaigns

[Maria Bada, Angela M. Sasse, Jason R. C. Nurse: “Cyber Security Awareness Campaigns: Why do they fail to change behaviour?”, <https://arxiv.org/abs/1901.02672>]

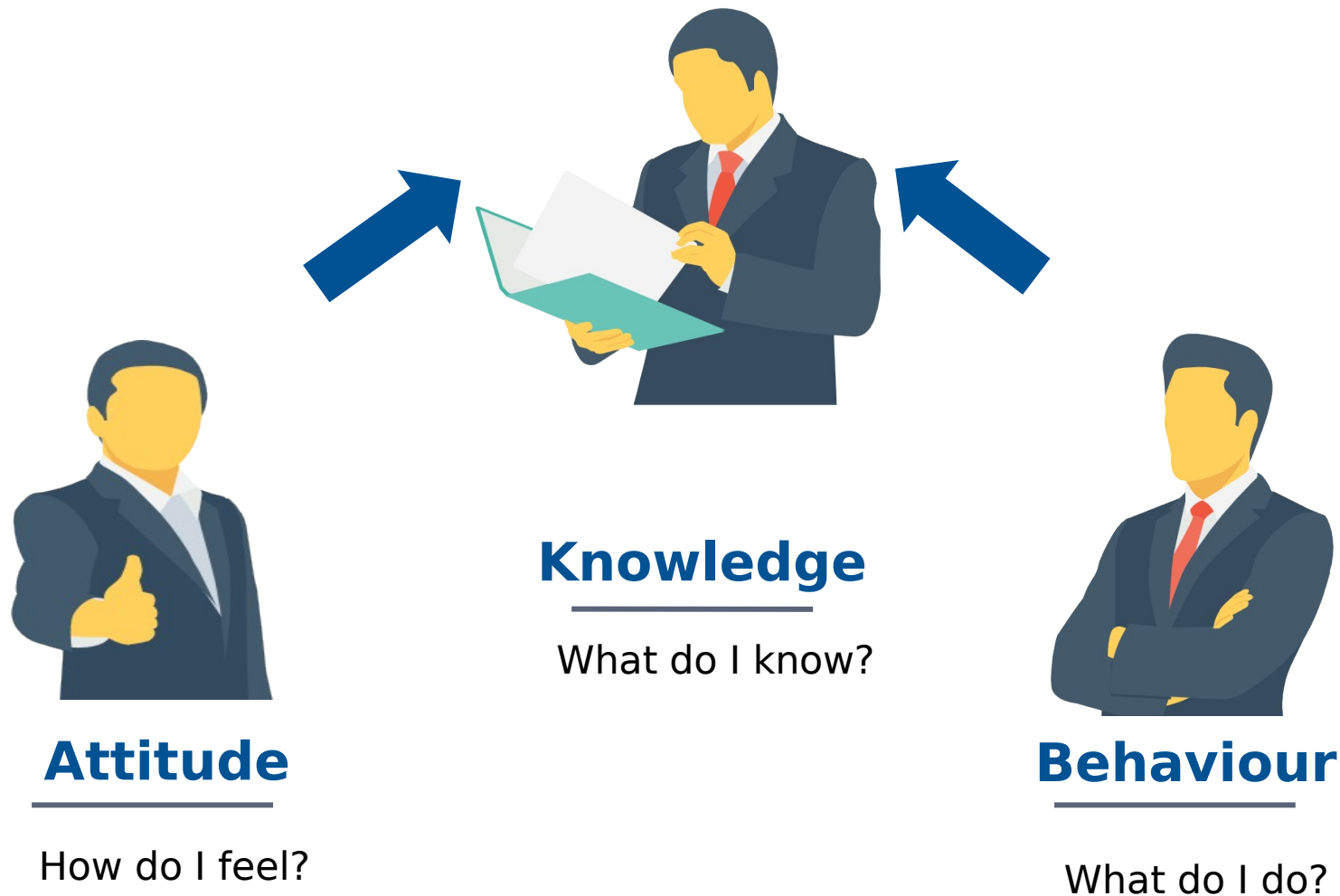
Problems with Social Engineering Pentesting

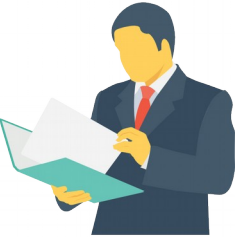


- Lots of effort beforehand to address legal issues
- Involves the deception of employees and a possible violation of their privacy rights
- Provides only a small fraction of all attack vectors.
- Humans can easily be demotivated when confronted with the results






G. Watson, A. Mason, and R. Ackroyd, *Social Engineering Penetration Testing: Executing Social Engineering Pen Tests, Assessments and Defense*. Syngress, 2011.

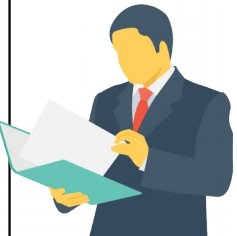

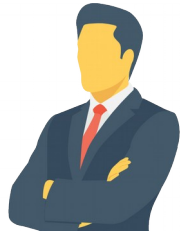
T. Dimkov, A. van Cleeff, W. Pieters, and P. Hartel, "Two methodologies for physical penetration testing using social engineering," in *Proceedings of the 26th Annual Computer Security Applications Conference*, ser. ACSAC '10. ACM, 2010, pp. 399–408.



Dimension	Defence Mechanism	Description
 Knowledge	 Attitude	Policy Compliance <ul style="list-style-type: none"> - Foundation of information security - System standards and user guidelines
		Security Awareness Program <ul style="list-style-type: none"> - Familiarity with policy - Information about sensitive data - Information about social engineering
	 Behaviour	Audit <ul style="list-style-type: none"> - Test susceptibility to social engineering - Identify weaknesses

Defense Mechanisms (Social Psychology)

Dimension		Defence Mechanism	Description
 <p>Knowledge</p>	 <p>Attitude</p>	<p>Persuasion Knowledge</p>	<ul style="list-style-type: none"> - Strategies to persuade - Coping strategies
		<p>Forewarning</p>	<ul style="list-style-type: none"> - Warning about manipulation - Black and white illustration
		<p>Attitude Bolstering</p>	<ul style="list-style-type: none"> - Knowledge of corporate security policy - Strengthening existing knowledge
		<p>Reality Check</p>	<ul style="list-style-type: none"> - Demonstration of vulnerability - Perception of risks
	 <p>Behaviour</p>	<p>Inoculation</p>	<ul style="list-style-type: none"> - Exposition to persuasion - Same effects as medical inoculation
		<p>Decision Making</p>	<ul style="list-style-type: none"> - Modification of decision making - Recurring exposition to persuasion

Dimension		IT Defence Mechanism	Psychological Defense Mechanism
 Knowledge	 Attitude	Policy Compliance	---
		Security Awareness Program	Forewarning
		---	Persuasion Knowledge
		---	Attitude Bolstering
		---	Reality Check
	 Behaviour	Audit	---
		---	Inoculation
		---	Decision Making

Training Strategies Summary

- Defenses:
 - Training
 - Policies
 - Awareness Campaigns



- Defense based on traditional recommendations
- Dismissal of human / psychological element
- Inadequate representation of awareness dimensions

Idea: A Serious Game

- Games can be fun
-> gets employees involved
- Games provide a realm
-> encourages employees to be creative
- Fictional situations are discussed in the game
-> no one is to blame
- Games are intended to be engaging and entertaining
-> which gets employees to play again





This is the easiest difficulty level. It is guaranteed that for a drawn Attack card the corresponding Defense card is always on the player's hand. You have plenty of time to finish the game and three lives you can lose. You also have one Joker card which repels every Attack card.

Play Beginner

15 mins



This level is more advanced. The corresponding Defense card for a drawn Attack card is not necessarily on the player's hand anymore. Thus, the game has to be played proactively by using the special action cards. You still have three lives and one Joker card.

Play Normal

15 mins



In this level, the corresponding Defense card for a drawn Attack card is also not necessarily on the player's hand. Compared to the Normal level, you have less special action cards for a proactive game play. Additionally, you have less time and lives and no Joker card anymore.

Play Expert

12 mins



This is the most difficult level. It is similar to Expert but you have less time and only one life. Accordingly, you are not allowed to repel any Attack card incorrectly.

Play Nerd

9 mins

PROTECT



Attack Card

Defense

- Do not click on the Pop-Up window.
- If possible, close the Pop-Up window.
- Inform the CISO or the internal IT about the Pop-Up window and ask for its origin.

Defense

- Interrupt your work immediately.
- Prevent the person from looking on your screen.
- Do not process any confidential information during this period.

PROTECT

Social Engeneering Academy

Score: 10

8:10

PROTECT Pause Restart Tutorial Privacy Glossary

Play PROTECT:

<https://hsd.social-engineering.academy/>

Feedback / Study:

- Takes ca. 15min
- We used the game in industry for awareness raising and are interested if / how useful the game is in higher education
- If you play, please participate in the study
- Survey is fully anonymous

<https://m-chair.survey.uni-frankfurt.de/index.php/276597?lang=en>

- Social Engineering is a real threat
- Tools
 - Are not sophisticated yet
 - Don't cover defense so far
- Defense Strategies
 - Should be more aligned with results from psychology
 - Serious Games / Gamification is in vogue
- Measurement is still difficult
 - Scientifically
 - Management Perspective (KPI)



Questions?

Open Topics for MA-Thesis:

- A Framework for the Risk-Assessment of Inference Attacks on Automotive Data
- A Serious Game to Foster a Better Understanding of the GDPR
- A Serious Game to Detect Attacks in Log Files

- Maybe your own idea?

DILBERT



BY SCOTT ADAMS



DilbertCartoonist@gmail.com

©2014 Scott Adams, Inc. /Dist. by Universal Uclick

www.dilbert.com
1-12-14

[Source: Scott Adams
<https://dilbert.com/strip/2014-01-12>]