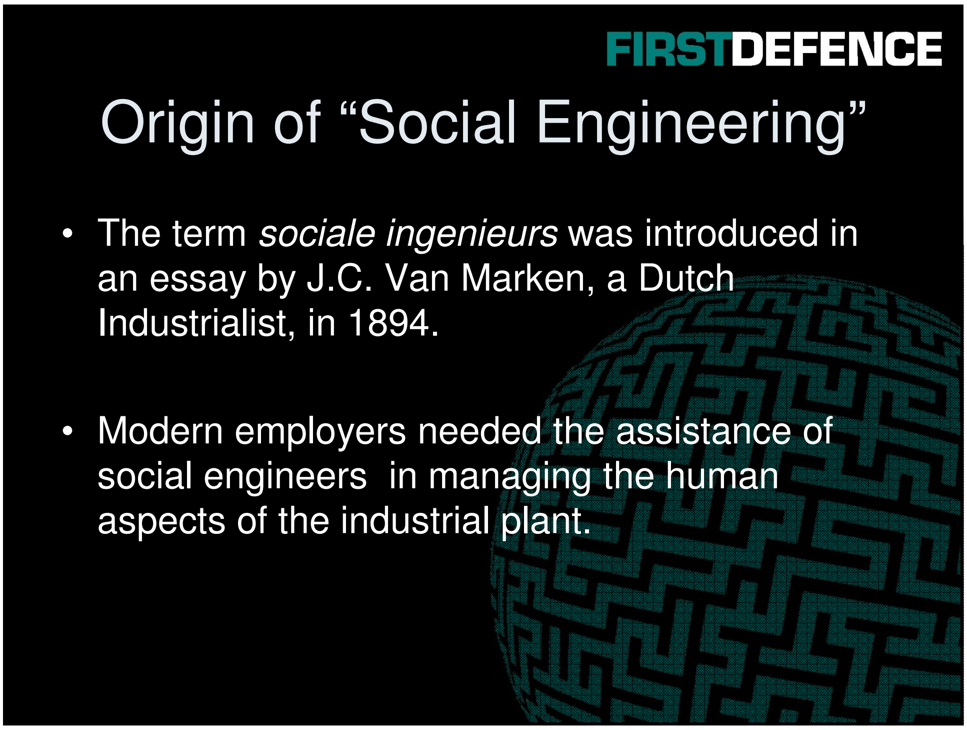
The Future of Social Engineering

Sharon Conheady

sconheady@FirstDefenceIS.com

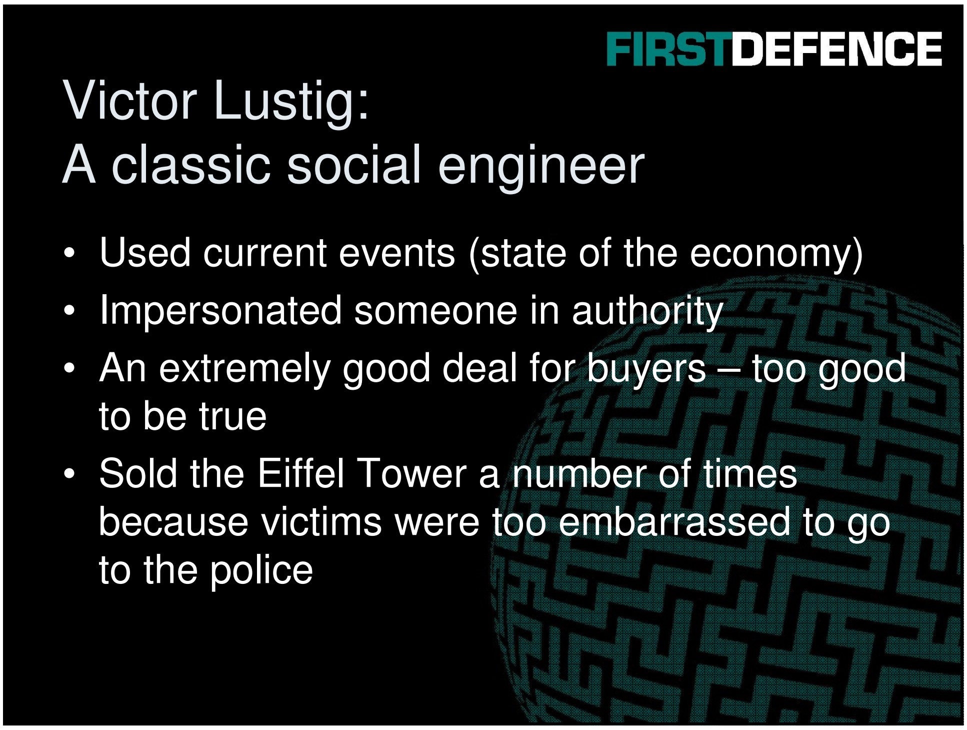


Origin of “Social Engineering”

- The term *sociale ingenieurs* was introduced in an essay by J.C. Van Marken, a Dutch Industrialist, in 1894.
- Modern employers needed the assistance of social engineers in managing the human aspects of the industrial plant.

FIRSTDEFENCE

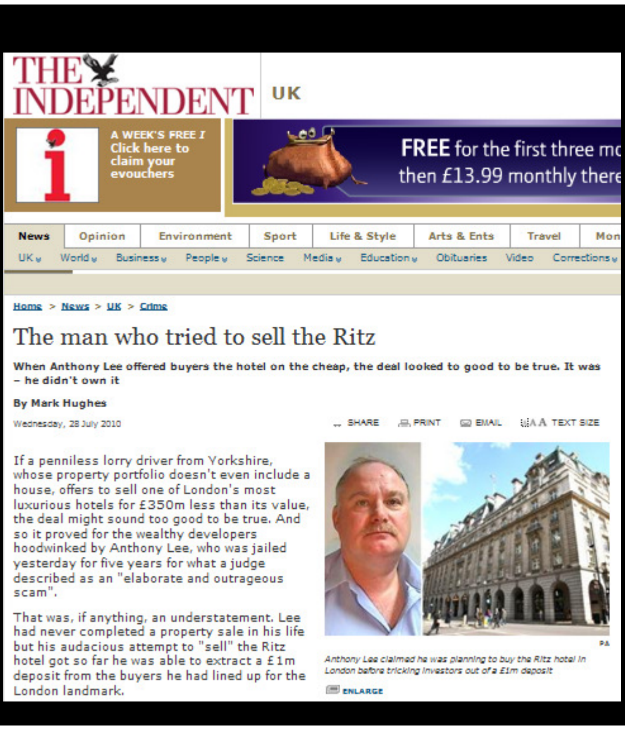
Social Engineering 100 years ago



FIRSTDEFENCE

Victor Lustig: A classic social engineer

- Used current events (state of the economy)
- Impersonated someone in authority
- An extremely good deal for buyers – too good to be true
- Sold the Eiffel Tower a number of times because victims were too embarrassed to go to the police



The man who tried to sell the Ritz

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

By Mark Hughes

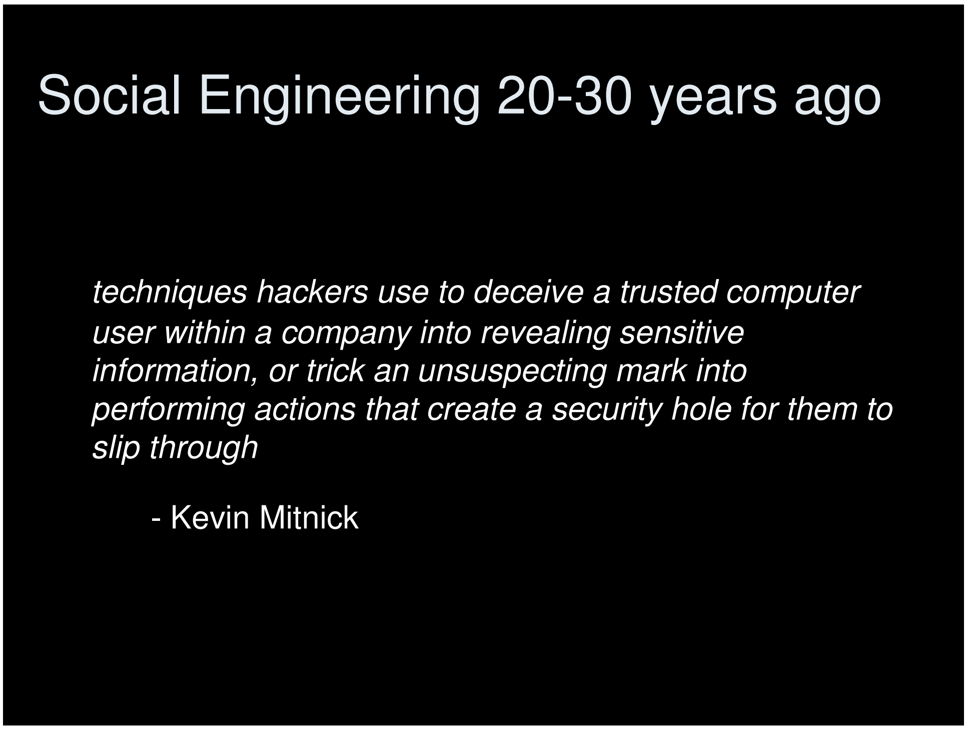
Wednesday, 28 July 2010

If a penniless lorry driver from Yorkshire, whose property portfolio doesn't even include a house, offers to sell one of London's most luxurious hotels for £350m less than its value, the deal might sound too good to be true. And so it proved for the wealthy developers hoodwinked by Anthony Lee, who was jailed yesterday for five years for what a judge described as an "elaborate and outrageous scam".

That was, if anything, an understatement. Lee had never completed a property sale in his life but his audacious attempt to "sell" the Ritz hotel got so far he was able to extract a £1m deposit from the buyers he had lined up for the London landmark.

Anthony Lee claimed he was planning to buy the Ritz hotel in London before tricking investors out of a £1m deposit

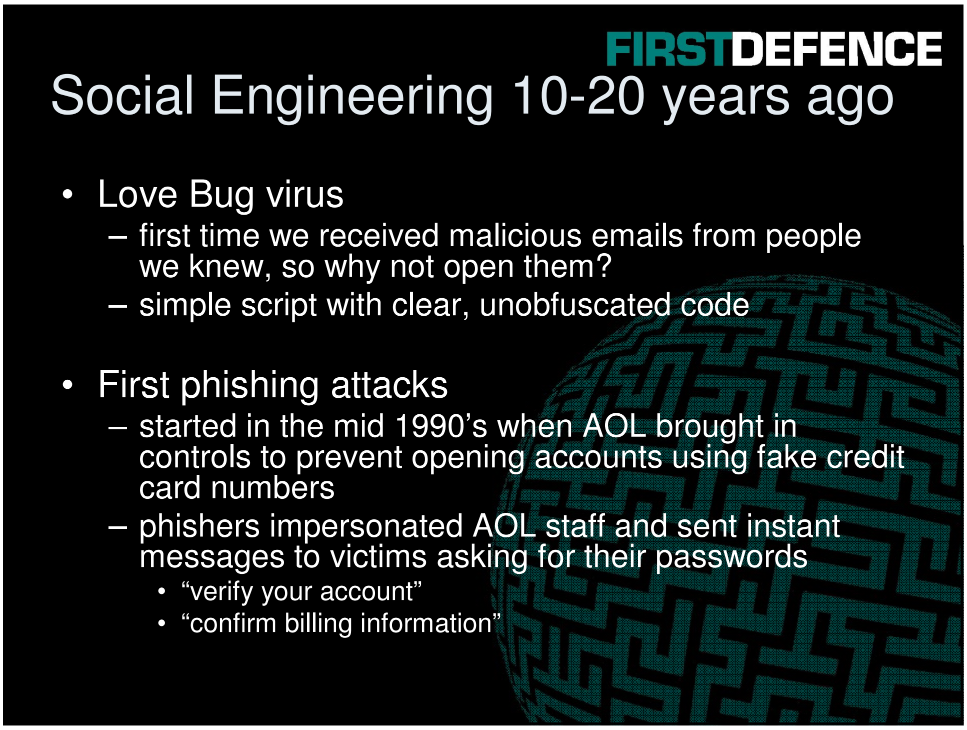
Social Engineering 40-50 years ago



Social Engineering 20-30 years ago

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

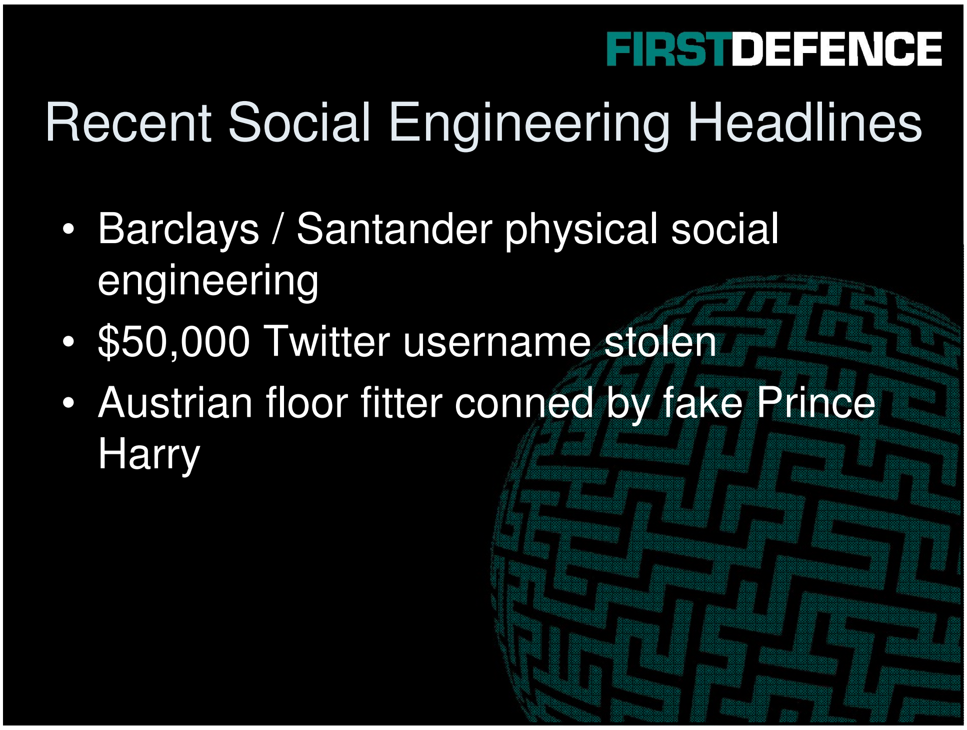
- Kevin Mitnick



FIRSTDEFENCE

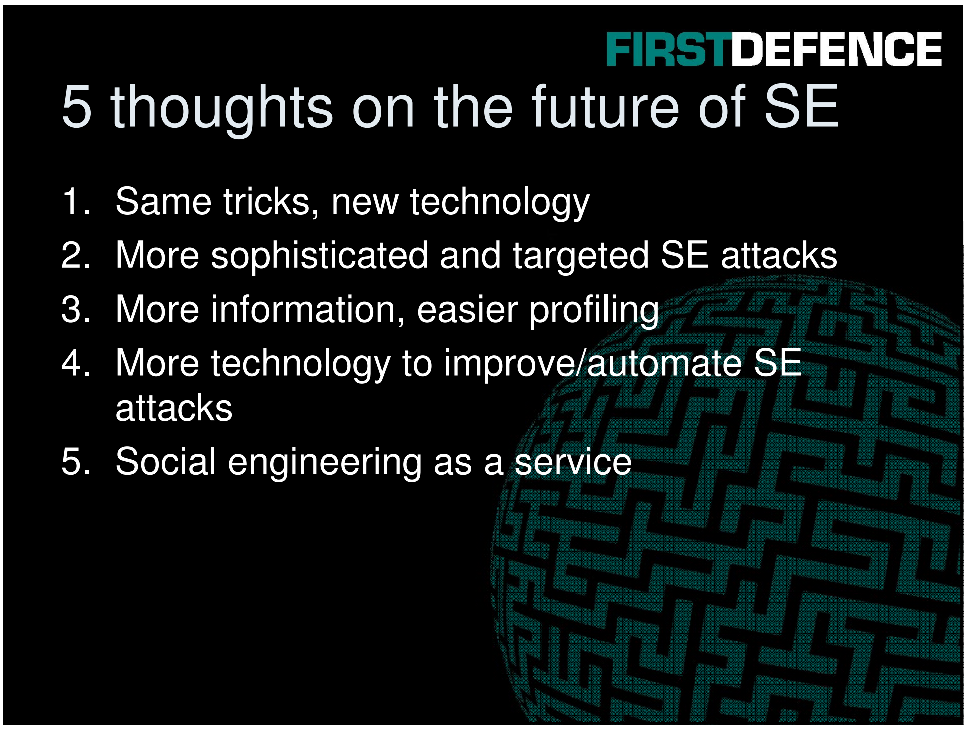
Social Engineering 10-20 years ago

- Love Bug virus
  - first time we received malicious emails from people we knew, so why not open them?
  - simple script with clear, unobfuscated code
- First phishing attacks
  - started in the mid 1990’s when AOL brought in controls to prevent opening accounts using fake credit card numbers
  - phishers impersonated AOL staff and sent instant messages to victims asking for their passwords
    - “verify your account”
    - “confirm billing information”



Recent Social Engineering Headlines

- Barclays / Santander physical social engineering
- $50,000 Twitter username stolen
- Austrian floor fitter conned by fake Prince Harry

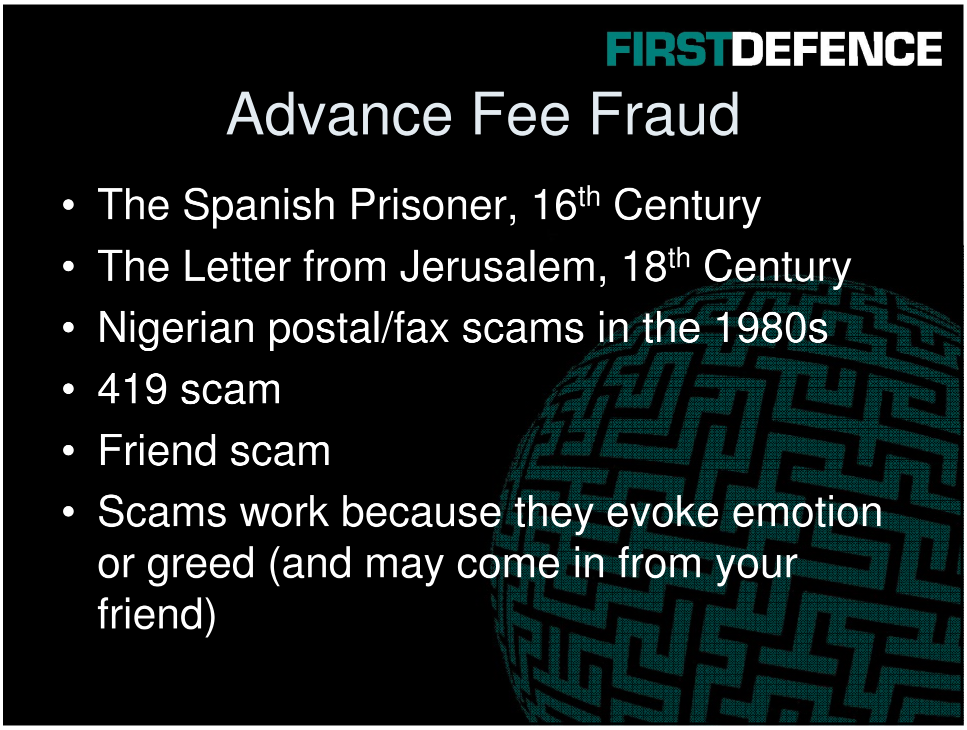


5 thoughts on the future of SE

1. Same tricks, new technology
2. More sophisticated and targeted SE attacks
3. More information, easier profiling
4. More technology to improve/automate SE attacks
5. Social engineering as a service

FIRSTDEFENCE

#1 Same tricks, new technology



FIRSTDEFENCE

Advance Fee Fraud

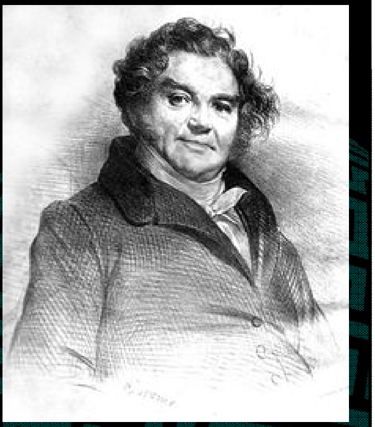
- The Spanish Prisoner, 16th Century
- The Letter from Jerusalem, 18th Century
- Nigerian postal/fax scams in the 1980s
- 419 scam
- Friend scam
- Scams work because they evoke emotion or greed (and may come in from your friend)

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!



Eugène François Vidocq

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.

419 Scam – Dec 2009

Greetings,

This message might meet you in utmost surprise; however, it is just my urgent need for foreign partner that made me to contact you for this transaction. I am a banker by profession from Burkina Faso in West Africa and currently holding the post of Director Auditing and Accounting unit of the bank. I have the opportunity of transferring the left over funds ($12.5million) of one of my bank clients who died along with his entire family on 31 July 2000 in a plane crash. You can confirm the geniuses of the deceased death by clicking on this web site http://news.bbc.co.uk/1/hi/world/europe/859479.stm hence; I am inviting you for a business deal where this money can be shared between us in the ratio of 60/38 while 2% will be mapped out for expenses. If you agree to my business proposal. Further details of the transfer will be forwarded to you as soon as i receive your return mail.

1.Your name..................
2.Your phone..................
3.Age........................
4.Sex.........................
5.Profession.................
6.Address....................

Best regards.

Mr. Salam Ahmed

Friend Scam

How are you doing today? I am sorry i didn't inform you about my traveling to Nigeria for a program.It as been a very sad and bad moment for me over here and the present condition that i found myself is very hard for me to explain.

I am really stranded in Nigeria because I forgot my little bag in the Taxi where my money, passport,documents and other valuable things were kept on my way to the Hotel am staying, I am facing a hard time here because i have no money on me to clear my Hotel bill, I am now owning a sum $2,000 of my Hotel bill.

I need you to help me out with a sum of $3,500 urgently so that i can arrange and travel back home,I need this help so much and on time because i am in a terrible and tight situation here, understand how important and urgent i need your help.

I will appreciate what so ever you can afford to send me immediately through Western Union and I promise to pay back your money as soon as i return home.please use the below information to transfer me the money.

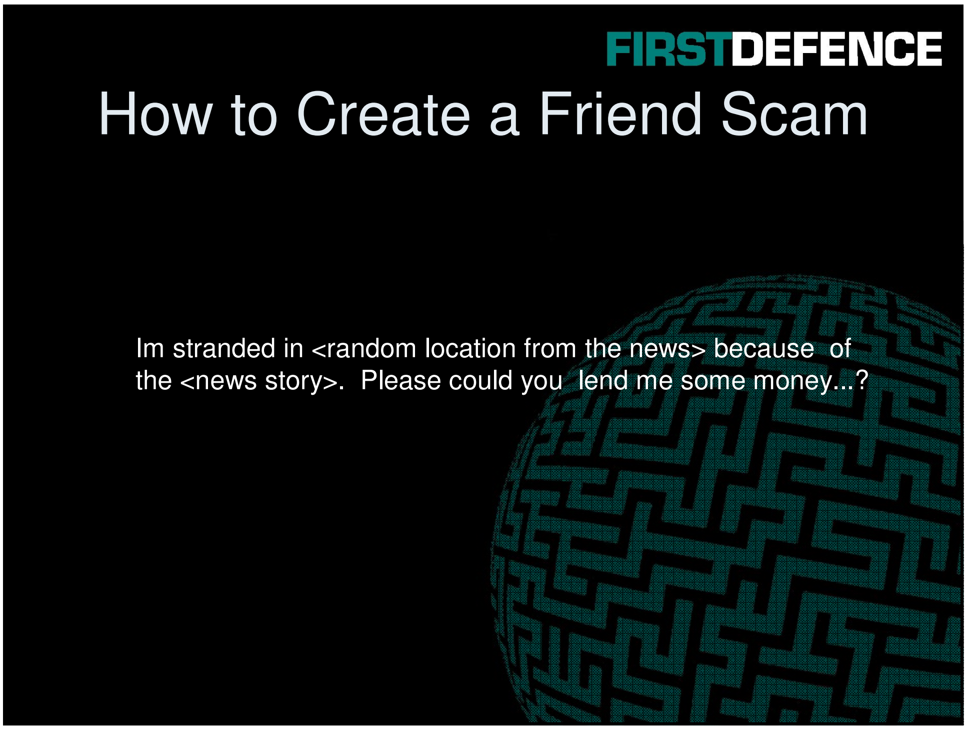
Name : XXXXXXXXX
Address : XXXXXXXXX
State : XXXXXXXXX
Country : XXXXXXXXX
Zip code: XXXXXXXXX

Question : please
Answer : Urgent
kindly get back to me with the scan copy of the transfer receipt so i will be able to go and pick up the money.

I will be waiting to hear from you soon.

Old attacks reworked on Social Networks

- Instead of coming from a stranger in Nigeria attack comes from your friend
- Instead of receiving an email you are contacted via a social networking site
- Naturally, you want to help your friend



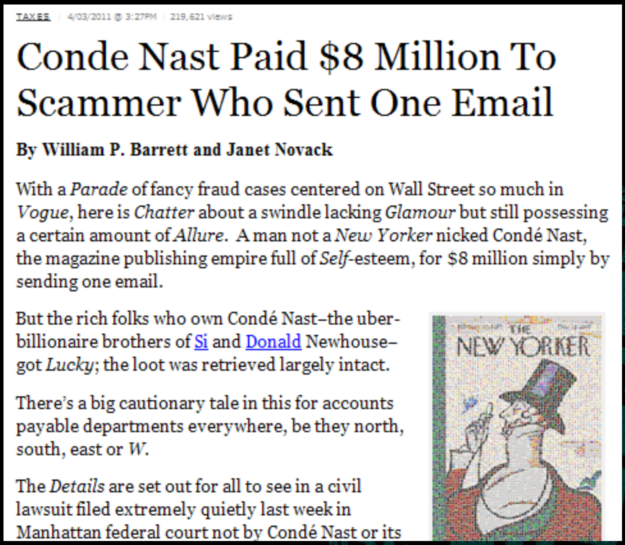
How to Create a Friend Scam

Im stranded in <random location from the news> because of the <news story>. Please could you lend me some money...?

#2 More sophisticated and targeted SE attacks

Targeted phishing attacks

- Spear phishing: phishing attack aimed at a particular person
- Whaling: phishing attack aimed at the rich and powerful
- These attacks are often believable because they offer some information that is personal to the victim.



TAXES | 4/03/2011 @ 3:27PM | 219,621 views

Conde Nast Paid $8 Million To Scammer Who Sent One Email

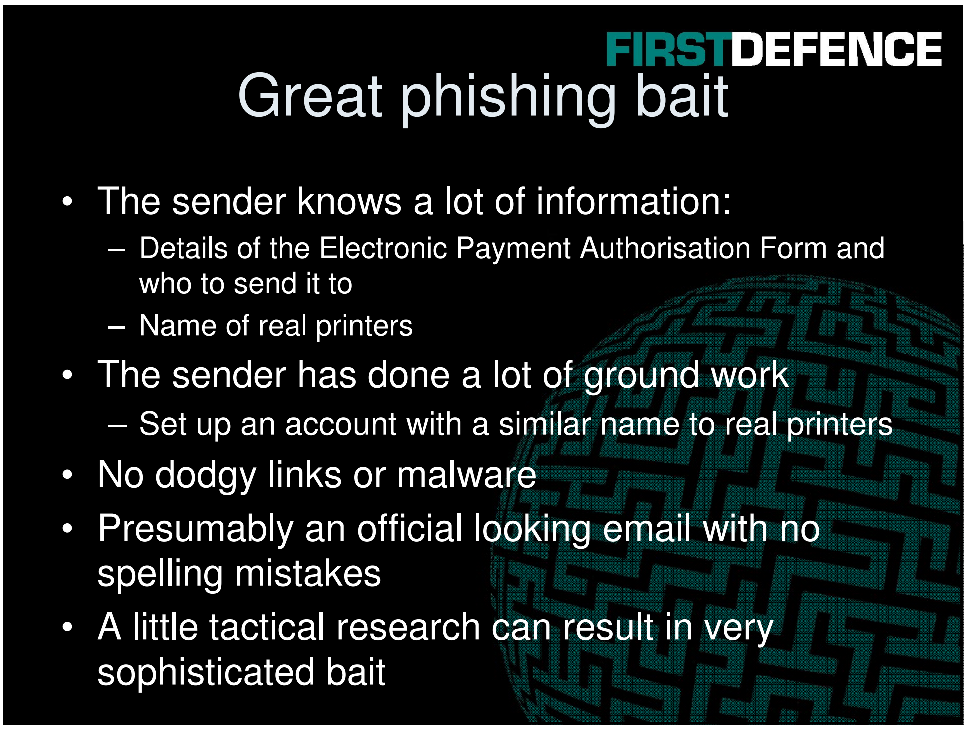
By William P. Barrett and Janet Novack

With a *Parade* of fancy fraud cases centered on Wall Street so much in *Vogue*, here is *Chatter* about a swindle lacking *Glamour* but still possessing a certain amount of *Allure*. A man not a *New Yorker* nicked Condé Nast, the magazine publishing empire full of *Self*-esteem, for $8 million simply by sending one email.

But the rich folks who own Condé Nast–the uber-billionaire brothers of Si and Donald Newhouse–got *Lucky*; the loot was retrieved largely intact.

There's a big cautionary tale in this for accounts payable departments everywhere, be they north, south, east or *W*.

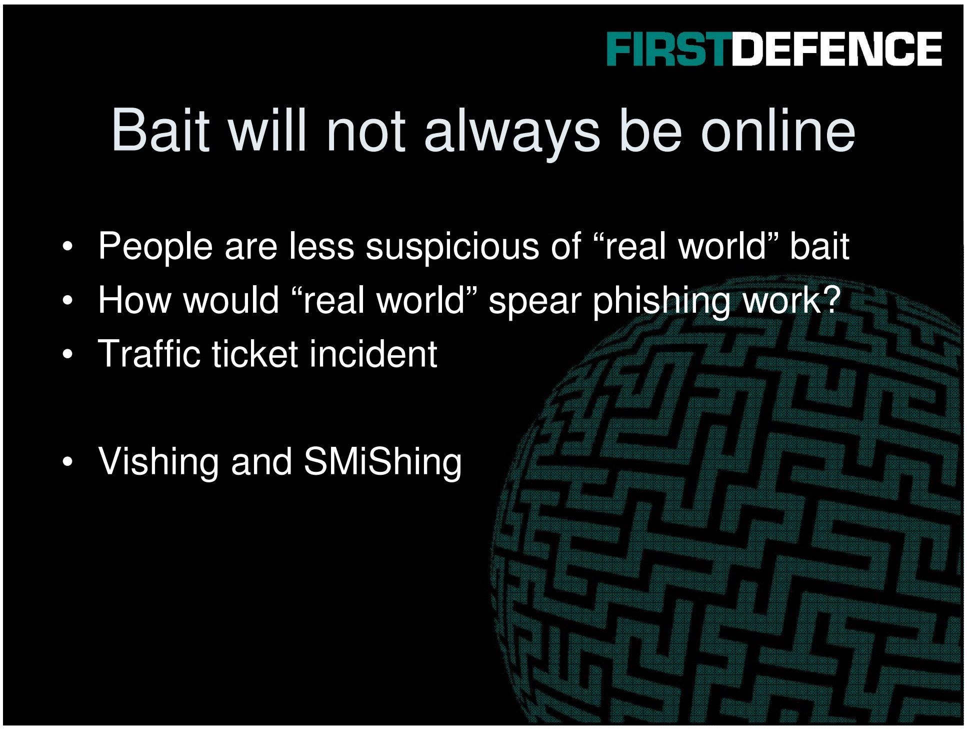
The *Details* are set out for all to see in a civil lawsuit filed extremely quietly last week in Manhattan federal court not by Condé Nast or its



FIRSTDEFENCE

Great phishing bait

- The sender knows a lot of information:
  - Details of the Electronic Payment Authorisation Form and who to send it to
  - Name of real printers
- The sender has done a lot of ground work
  - Set up an account with a similar name to real printers
- No dodgy links or malware
- Presumably an official looking email with no spelling mistakes
- A little tactical research can result in very sophisticated bait

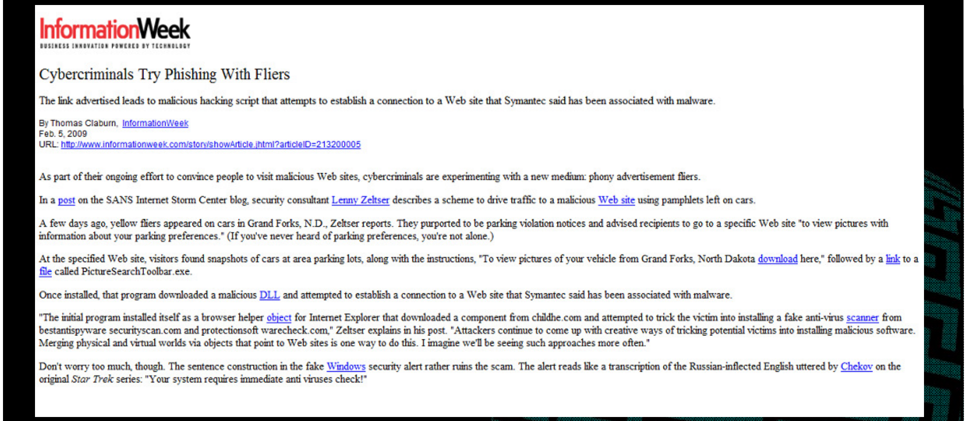


FIRSTDEFENCE

Bait will not always be online

- People are less suspicious of “real world” bait
- How would “real world” spear phishing work?
- Traffic ticket incident

- Vishing and SMiShing



InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Cybercriminals Try Phishing With Fliers

The link advertised leads to malicious hacking script that attempts to establish a connection to a Web site that Symantec said has been associated with malware.

By Thomas Claburn, InformationWeek
Feb. 5, 2009
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=213200005

As part of their ongoing effort to convince people to visit malicious Web sites, cybercriminals are experimenting with a new medium: phony advertisement fliers.

In a post on the SANS Internet Storm Center blog, security consultant Lenny Zeltser describes a scheme to drive traffic to a malicious Web site using pamphlets left on cars.

A few days ago, yellow fliers appeared on cars in Grand Forks, N.D., Zeltser reports. They purported to be parking violation notices and advised recipients to go to a specific Web site "to view pictures with information about your parking preferences." (If you've never heard of parking preferences, you're not alone.)

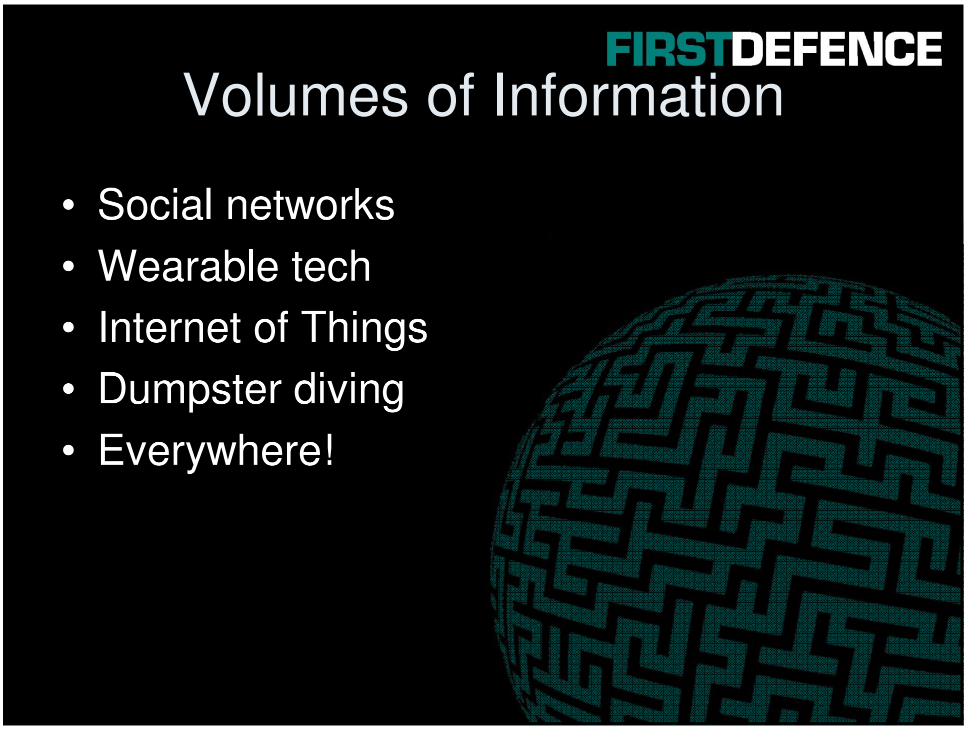
At the specified Web site, visitors found snapshots of cars at area parking lots, along with the instructions, "To view pictures of your vehicle from Grand Forks, North Dakota download here," followed by a link to a file called PictureSearchToolbar.exe.

Once installed, that program downloaded a malicious DLL and attempted to establish a connection to a Web site that Symantec said has been associated with malware.

"The initial program installed itself as a browser helper object for Internet Explorer that downloaded a component from childhe.com and attempted to trick the victim into installing a fake anti-virus scanner from bestantispyware securityscan.com and protectionsoft warecheck.com," Zeltser explains in his post. "Attackers continue to come up with creative ways of tricking potential victims into installing malicious software. Merging physical and virtual worlds via objects that point to Web sites is one way to do this. I imagine we'll be seeing such approaches more often."

Don't worry too much, though. The sentence construction in the fake Windows security alert rather ruins the scam. The alert reads like a transcription of the Russian-inflected English uttered by Chekov on the original *Star Trek* series: "Your system requires immediate anti viruses check!"

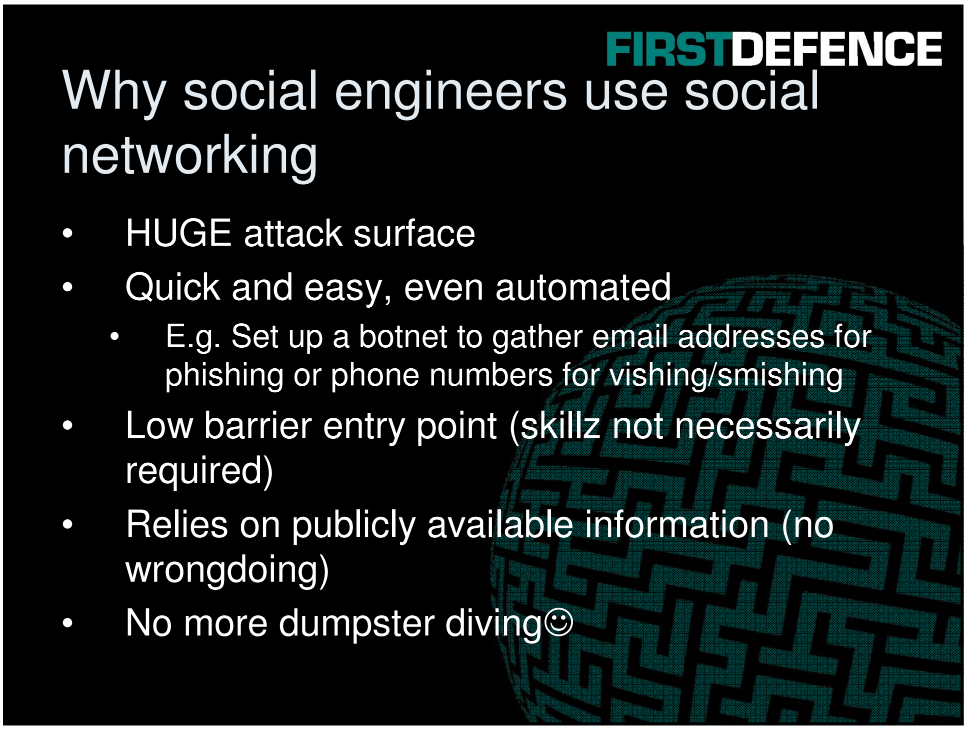
#3
More information, easier profiling



FIRSTDEFENCE

Volumes of Information

- Social networks
- Wearable tech
- Internet of Things
- Dumpster diving
- Everywhere!



FIRSTDEFENCE

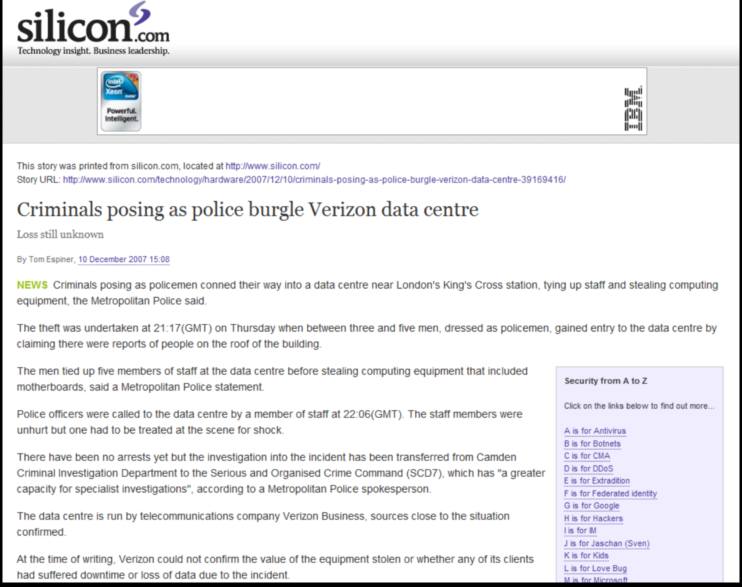
Why social engineers use social networking

- HUGE attack surface
- Quick and easy, even automated
  - E.g. Set up a botnet to gather email addresses for phishing or phone numbers for vishing/smishing
- Low barrier entry point (skillz not necessarily required)
- Relies on publicly available information (no wrongdoing)
- No more dumpster diving☺

Why Social Engineering over Social Networking works

- Trust model
- No real authentication
  - Easy to impersonate someone else or set up a fake profile
- Influential (Cialdini's principles of influence)
  - Social proof: people do things that other people are doing
  - Similarity: people are influenced by people they like
  - Hey, look at this. John says it's cool.

Impersonation in the Real World



silicon.com
Technology insight. Business leadership.

This story was printed from silicon.com, located at http://www.silicon.com/
Story URL: http://www.silicon.com/technology/hardware/2007/12/10/criminals-posing-as-police-burgle-verizon-data-centre-39169416/

Criminals posing as police burgle Verizon data centre

Loss still unknown

By Tom Espiner, 10 December 2007 15:08

NEWS Criminals posing as policemen conned their way into a data centre near London's King's Cross station, tying up staff and stealing computing equipment, the Metropolitan Police said.

The theft was undertaken at 21:17(GMT) on Thursday when between three and five men, dressed as policemen, gained entry to the data centre by claiming there were reports of people on the roof of the building.

The men tied up five members of staff at the data centre before stealing computing equipment that included motherboards, said a Metropolitan Police statement.

Police officers were called to the data centre by a member of staff at 22:06(GMT). The staff members were unhurt but one had to be treated at the scene for shock.

There have been no arrests yet but the investigation into the incident has been transferred from Camden Criminal Investigation Department to the Serious and Organised Crime Command (SCD7), which has "a greater capacity for specialist investigations", according to a Metropolitan Police spokesperson.

The data centre is run by telecommunications company Verizon Business, sources close to the situation confirmed.

At the time of writing, Verizon could not confirm the value of the equipment stolen or whether any of its clients had suffered downtime or loss of data due to the incident.

Security from A to Z

Click on the links below to find out more...

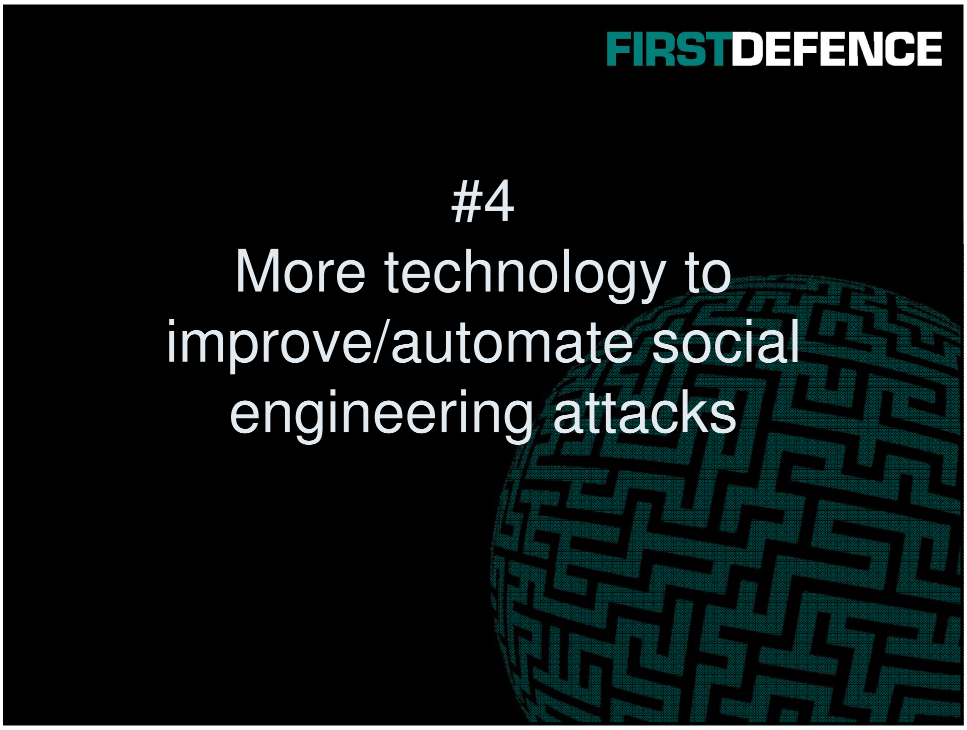
A is for Antivirus
B is for Botnets
C is for CMA
D is for DDoS
E is for Extradition
F is for Federated identity
G is for Google
H is for Hackers
I is for IM
J is for Jaschan (Sven)
K is for Kids
L is for Love Bug
M is for Microsoft

FIRSTDEFENCE

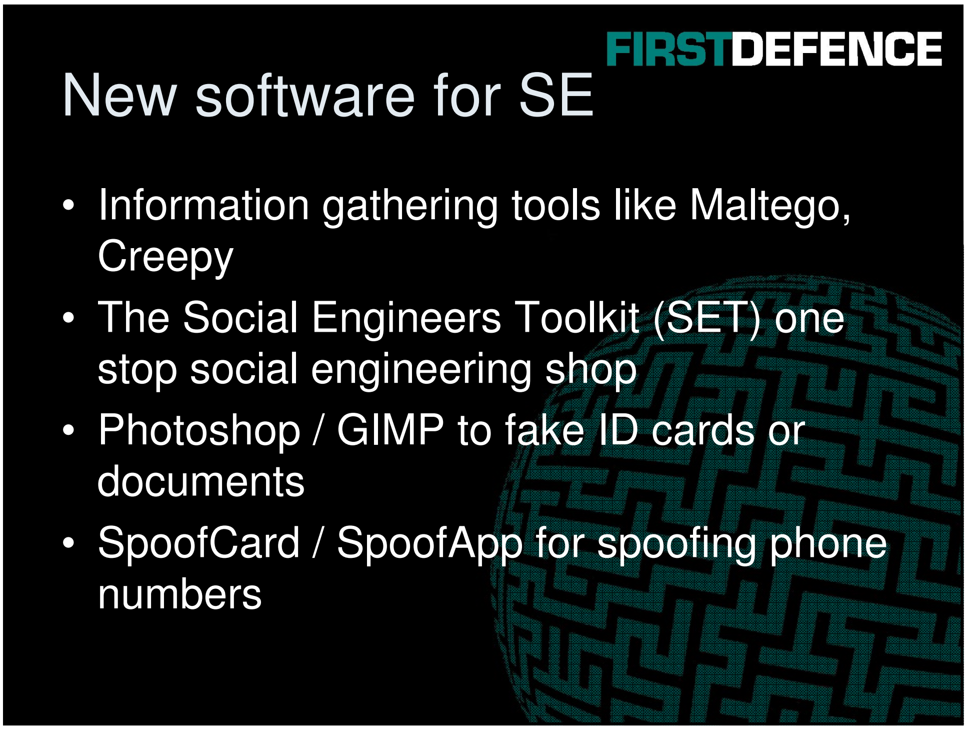
Impersonation in the Real World

- Takes money (to buy police costumes)
- May involve other criminal activities ("procuring" police costumes, impersonating a public official, physically harming victims)
- Takes a lot of planning
- Usually involves several people (5 people in this instance)
- Much easier to get caught

Photo from Provide Security



#4
More technology to improve/automate social engineering attacks



New software for SE

- Information gathering tools like Maltego, Creepy
- The Social Engineers Toolkit (SET) one stop social engineering shop
- Photoshop / GIMP to fake ID cards or documents
- SpoofCard / SpoofApp for spoofing phone numbers

New hardware for SE

- Pwnphone
  - $960 from pwnieexpress.com (or download software to your own phone)
  - Commercially available pen test platform on a phone: Aircrack, Kismet, Metasploit, nmap…

#5
Social Engineering as a Service

Social Engineering as a Service

- It it’s still too much work, outsource it!
- SE telephone services offer:
  - professional callers (male and female) fluent in numerous languages
  - caller-ID spoofing
  - available to make calls during business hours across the world
- Cost: $7-15 per call

#6
More social engineering testing

Physical Penetration Testing Tools, Tactics & Techniques
Social Engineering in IT Security
Sharon Conheady

FIRSTDEFENCE

The Future of Social Engineering

Sharon Conheady

sconheady@FirstDefenceIS.com

FIRSTDEFENCE