# Social Engineering

The Future of Social Engineering

# 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.

# Social Engineering 100 years ago

# Victor Lustig: A classic social engineer

- Used current events (state of the economy)
- Impersonated someone in authority
- Made the deal an extremely attractive 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

# 28 July 2010

THE INDEPENDENT UK

A WEEK'S FREE *i*
Click here to claim your evouchers

FREE for the first three mo
then £13.99 monthly there



# 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

SHARE PRINT EMAIL A A TEXT SIZE

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".

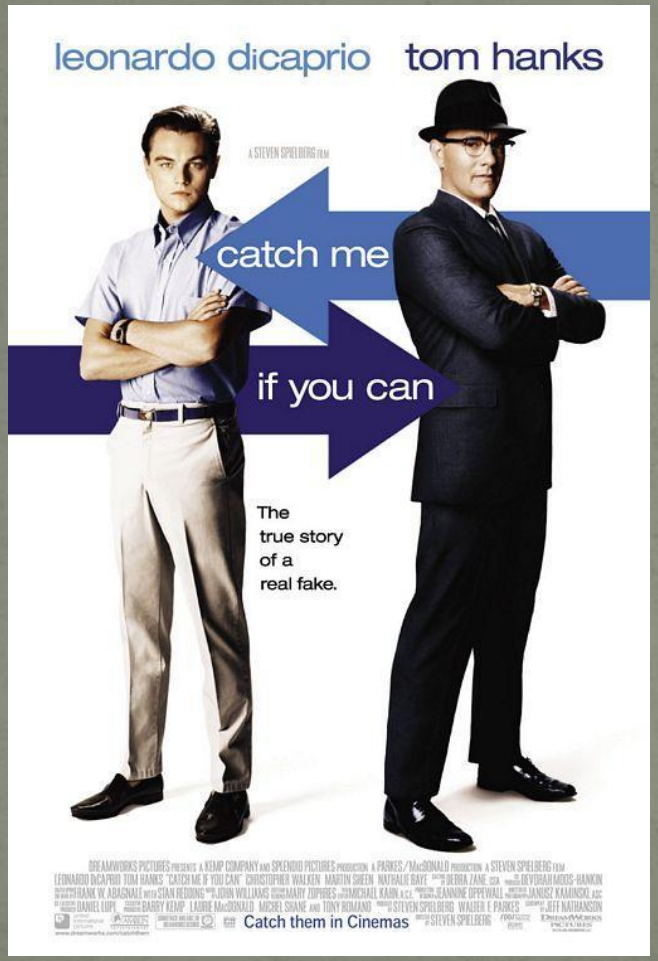
That was, if anything, an understatement. Lee had never completed a property sale in his life but his audacious attempt to "sell" the Ritz hotel got so far he was able to extract a £1m deposit from the buyers he had lined up for the London landmark.

PA

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

ENLARGE

# Impersonation (40 – 50 years ago)




- This worked because:
  - Conveyed authority
  - Sufficient research performed
  - Acted and **looked** the part
- Would it still work today?

# June 2007

BBC NEWS

## Chinese man fakes it as a pilot

**An unemployed Chinese man boarded an aeroplane disguised as a pilot, in order to get a free flight home, according to state media.**

His actions mimicked the exploits of a fraudster portrayed in a Hollywood film starring Leonardo DiCaprio.

Shu Shi, 23, turned up at Beijing's international airport dressed as a pilot, carrying fake identification, according to the Beijing News.

He had reportedly bought the uniform on the internet.

The relevant fake documents had been also been downloaded from the internet.

**Caught out**

His plan was only foiled when the plane's real pilot discovered his limited knowledge of aviation issues.

He was handed over to police when the aircraft arrived in his home province of Guizhou.

Shu Shi was detained for 10 days and fined 500 yuan ($65), the Beijing News said.

In the film Catch Me If You Can, Leonardo DiCaprio plays a character inspired by a real master of deception who passes himself off as a pilot, and as other professionals, before his trick is eventually discovered.

# March 2010

BBC NEWS

## 'Fake pilot' arrested in cockpit

**A Swedish pilot without a valid licence to fly has been arrested at Amsterdam as he was about to fly a jet with 101 passengers to Turkey, Dutch police say.**

The 41-year-old man said he had been flying for European airlines for 13 years and had logged 10,000 hours.

Police said he once had a licence to fly small planes but it had expired and it did not allow him to fly large jets.

Reports say the man was relieved his long deception was uncovered and tore off his pilot's stripes in the cockpit.

Turkey's Corendon Airlines said he had been flying for the airline for two years and had "expertly misled the company with his false papers".

The airline said it had been alerted by police and had a pilot standing by to fly the Boeing 737 from Amsterdam's Schiphol airport to Ankara.

Dutch police were acting on a tip-off from Swedish authorities.

The man is in custody awaiting trial for forging documents and flying without a licence.

# February 2012

## Fake pilot arrested from Sanganer in Jaipur

0 0 Tweet Recommend Submit

TNN Feb 17, 2012, 01.57AM IST

**Tags:** State Anti-Corruption Bureau | Randhir Singh

JAIPUR/NEW DELHI: The state anti-corruption bureau (ACB) arrested a Delhi-based man on Monday for allegedly obtaining a commercial pilot licence in a fraudulent manner from the Directorate General of Civil Aviation (DGCA). Accused Rakesh Mehta is a former student of Rajasthan Flying School.

This is the third arrest by ACB in this case, while the Delhi Police has arrested 18 people - including fake pilots and DGCA officials - so far.

---

Mehta was arrested from Sanganer near Jaipur. "Mehta was a student of the state flying school in Jaipur, whose chief flying instructor, M K Chaudhary, and others were arrested in the fake pilot scam in 2010. Mehta's claim of 150 flying hours was found to be fake," additional SP (ACB) Randhir Singh said.

He was produced in an ACB court in Jaipur which released him on bail.

"Mehta worked at a flying school in Delhi," said Singh.

TOI had carried a report in November 2010 revealing at least 14 pilots, who had fraudulently secured licenses, were flying passenger planes in the country.

The crime branch has decided to file the final chargesheet in the case by the end of this month. "We have collected all the necessary evidence and hope to file the chargesheet soon. The DGCA was the main complainant and they have always cooperated with us," said a senior crime branch officer.

Twenty-one people, including DGCA officials, have been arrested. "While investigating cases of granting of commercial pilot licence (CPL) through fake marksheets in the Mumbai zone, we had busted a module led by Eknath Patil, a tout from Ahmedabad. Busting of this module led to the arrest of captain Abhishek Kaushik, captain Hiren Nagar and two DGCA officials," said Ashok Chand, DCP (crime).

# September 2012

theguardian

News | Sport | Comment | Culture | Business | Money | Life & sty
Jobs

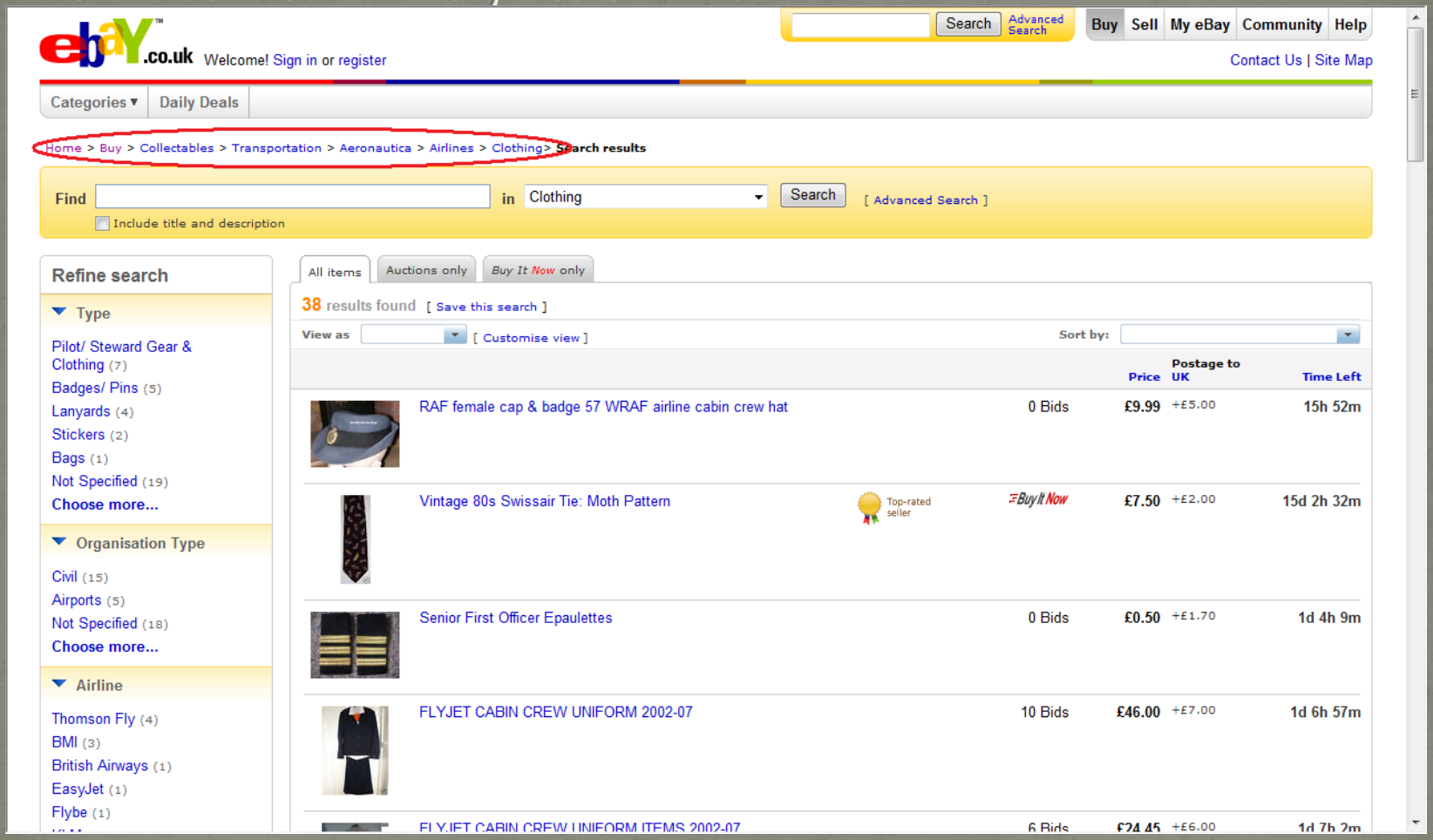
Culture › Film › Catch Me If You Can

## Fake pilot inspired by Spielberg's Catch Me If You Can

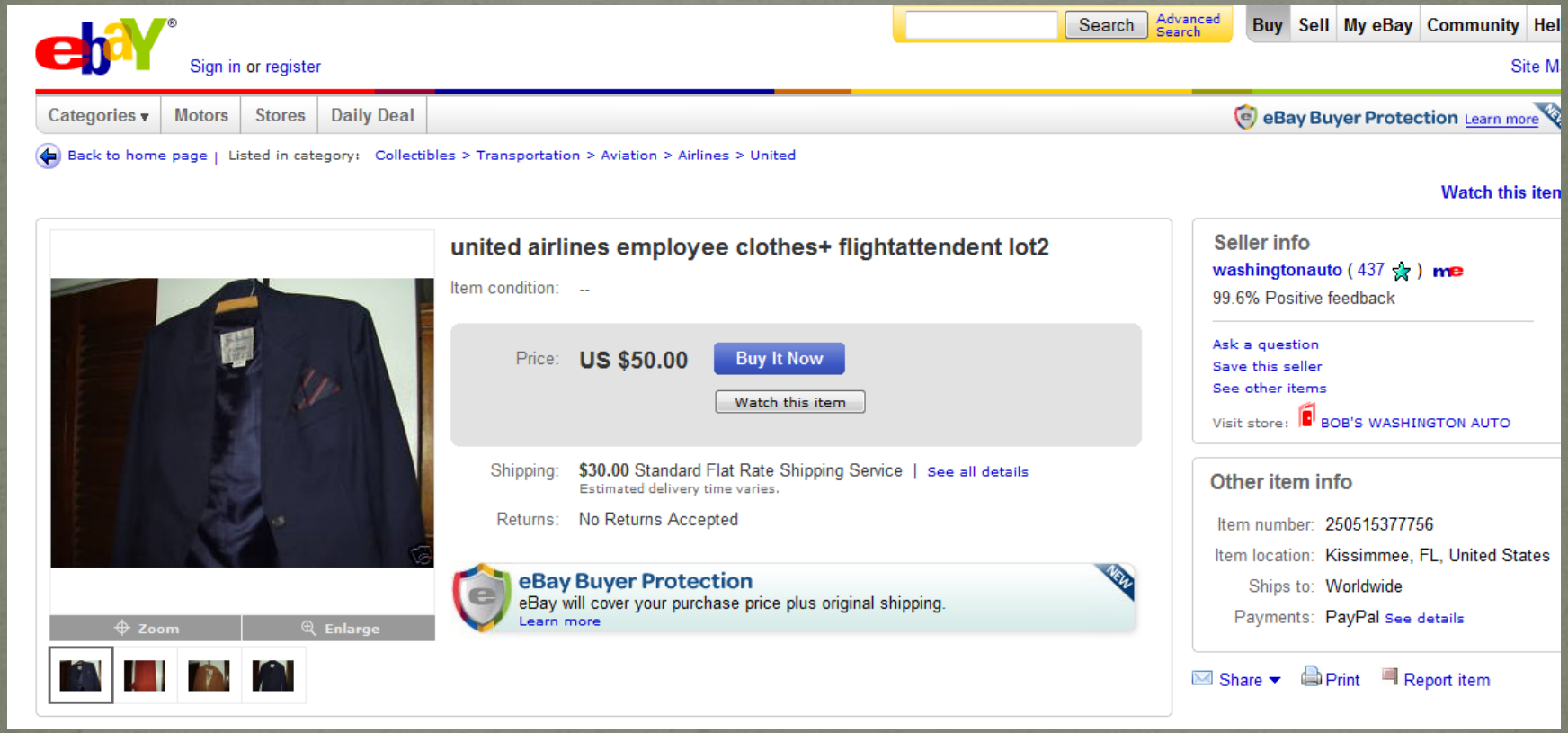
Italian 'Andrea Sirlo' reportedly told police he was motivated to pose as captain by Steven Spielberg's 2002 film

Ben Child
guardian.co.uk, Monday 24 September 2012 11.34 BST
Jump to comments (5)

# How did they do it?



# How did they do it?



# Social Engineering 20 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

# Social Engineering 10 years ago

- Love Bug virus
  - First time we received malicious emails from people, 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

- August 2012: Tech journalist, Mat Honan's digital life erased as hackers social engineer Apple and Amazon call centers
- May 2012: Czech thieves steal a 10-tonne bridge with forged documents to say they were working on a new bicycle path
- January 2012: Paul Allen's credit card details stolen by social engineering Citibank call centers
- December 2011: Wells Fargo wire $2.1m to a bogus bank account in Hong Kong following a series of fraudulent faxes

# The future of Social Engineering

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

# #1
# Same tricks, new technology

# Advance Fee Fraud

- Nigerian posta/fax scams in the 80s
- 419 scam
- Friend scam

- Scams work because they evoke emotion or greed (recently coming from your friends)

# Nigerians scams in the 80s

- 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, sending messages via postal letters, fax …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

# It is reported on BBC, this must be genuine

# 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

# Friend Scams of the Future

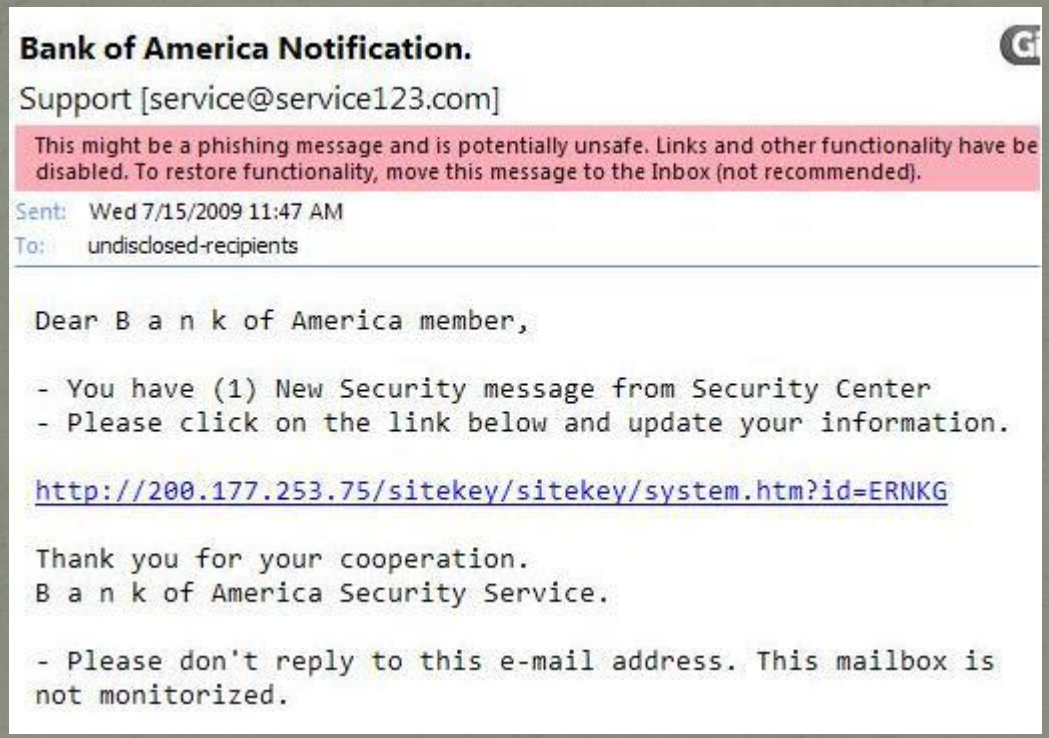
I'm stranded in London because of the snow. All flights have been cancelled. Please could you lend me some money so I can buy a train ticket instead…?

# #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.

# Bad Examples (but they still work)



**Bank of America Notification.**

Support [service@service123.com]

This might be a phishing message and is potentially unsafe. Links and other functionality have be disabled. To restore functionality, move this message to the Inbox (not recommended).

Sent: Wed 7/15/2009 11:47 AM

To: undisclosed-recipients

Dear B a n k of America member,

- You have (1) New Security message from Security Center
- Please click on the link below and update your information.

http://200.177.253.75/sitekey/sitekey/system.htm?id=ERNKG

Thank you for your cooperation.
B a n k of America Security Service.

- Please don't reply to this e-mail address. This mailbox is not monitorized.

# ISSA 2013

**From:** Elin Perez [mailto:e.perez@papers-ieee.org]
**Sent:** 02 August 2013 06:21 PM
**To:** [redacted]
**Subject:** Research Paper Collaboration

IEEE
Advancing Technology for Humanity

Dear [redacted]

I recently had the pleasure of reading your paper on "Protecting E-mail Anonymity with an Anonymizer Bouncer" that you presented at IISA 2012. Your research posed some interesting and novel ideas.

I would be interested in doing further research with you. You can view my current work and publications here.

I look forward to hearing from you.

Sincerely,

Elane Perez
IEEE Member

IEEE • 445 Hoes Lane, Piscataway, NJ 08854 USA

# Bait will not always be online

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

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."

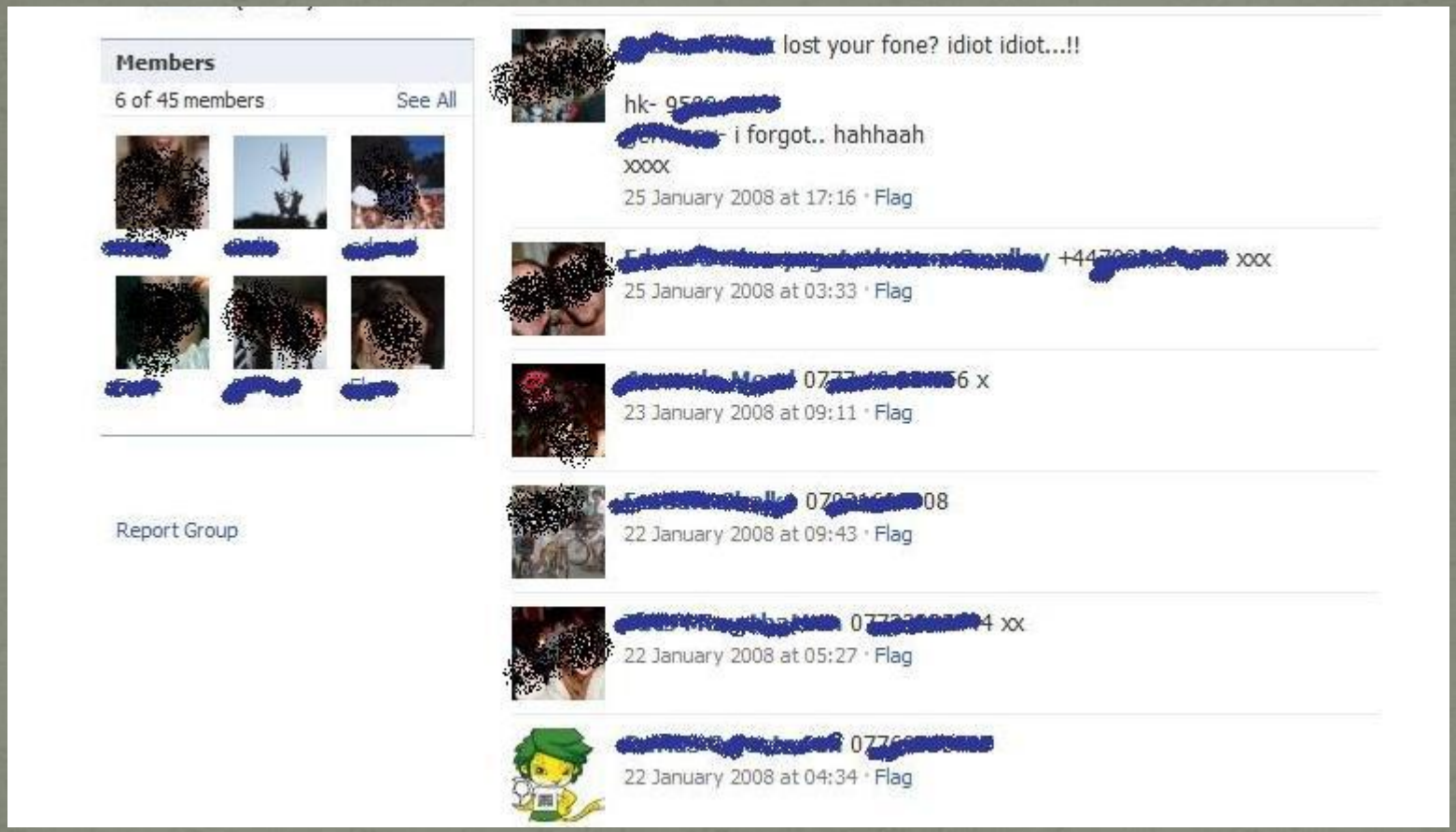
Don't worry too much, though. The sentence construction in the fake Windows security alert rather ruins the scam. The alert reads like a transcription of the Russian-inflected English uttered by Chekov on the original *Star Trek* series: "Your system requires immediate anti viruses check!"

# #3
# Social networking as an enabler to social engineering

# 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
- Relies on publicly available information (no wrongdoing)

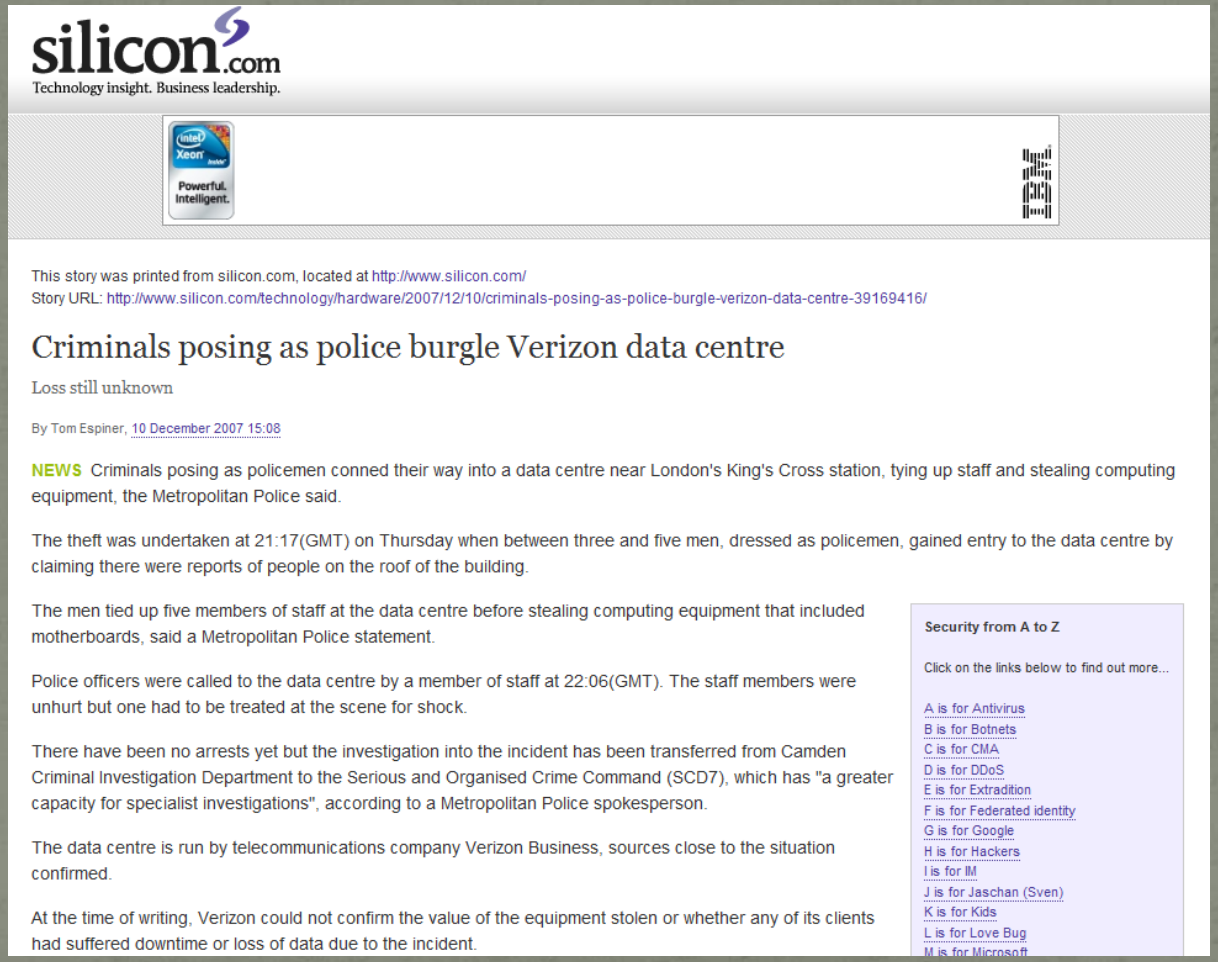
# Gathering phone numbers has never been easier



# Why Social Engineering over Social Networking works

- Trust model
- No real authentication
  - Easy to impersonate someone else or set up a fake profile
- Influential
  - 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.

Powerful. Intelligent.

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**

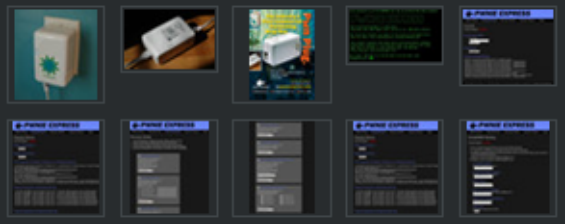
Click on the links below to find out more...

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

# #4
# More technology to improve/automate social engineering attacks

# Software for SE

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



# Pwn Plug Elite

The industry's first enterprise-class penetration testing drop box.

- Includes all release 1.1 features
- Includes 3G, Wireless, & USB-Ethernet adapters
- Fully-automated NAC/802.1x/RADIUS bypass!
- Out-of-band SSH access over 3G/GSM cell networks!
- Text-to-Bash: text in bash commands via SMS!
- Simple web-based administration with "Plug UI"
- One-click Evil AP, stealth mode, & passive recon
- Maintains persistent, covert, encrypted SSH access to your target network [Details]
- Tunnels through application-aware firewalls & IPS
- Supports HTTP proxies, SSH-VPN, & OpenVPN
- Sends email/SMS alerts when SSH tunnels are activated
- Preloaded with Debian 6, Metasploit, SET, Fast-Track, w3af, Kismet, Aircrack, SSLstrip, nmap, Hydra, dsniff, Scapy, Ettercap, Bluetooth/VoIP/IPv6 tools, & more!
- Unpingable and no listening ports in stealth mode
- Includes 16GB SDHC card for extra storage
- Includes stealthy decal stickers

CAMERA LENS
ON SIDE OF
BAG

4 November 2010 Last updated at 00:11

# Invisibility cloak closer with flexible 'metamaterial'

By Jason Palmer
Science and technology reporter, BBC News

**Scientists in the UK have demonstrated a flexible film that represents a big step toward the "invisibility cloak" made famous by Harry Potter.**

The film contains tiny structures that together form a "metamaterial", which can, among other tricks, manipulate light to render objects invisible.

Flexible metamaterials have been made before, but only work for light of a colour far beyond that which we see.

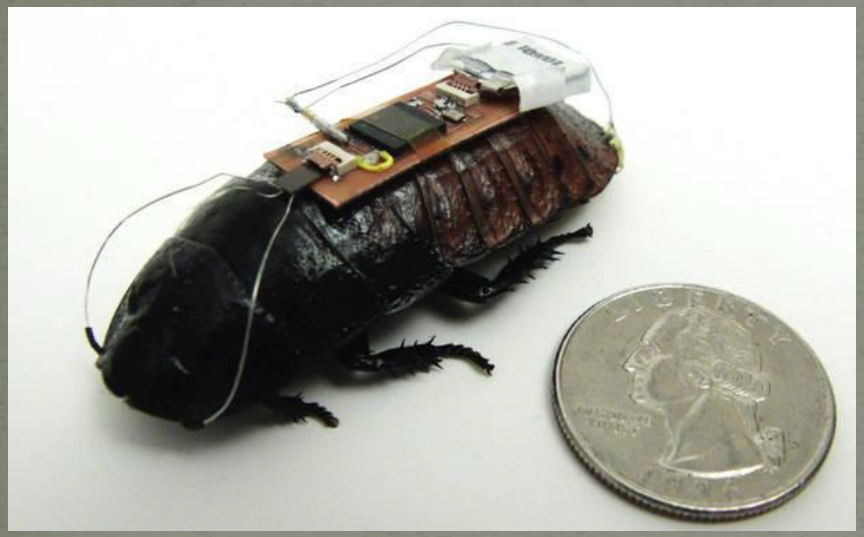
Physicists have hailed the approach a "huge step forward".

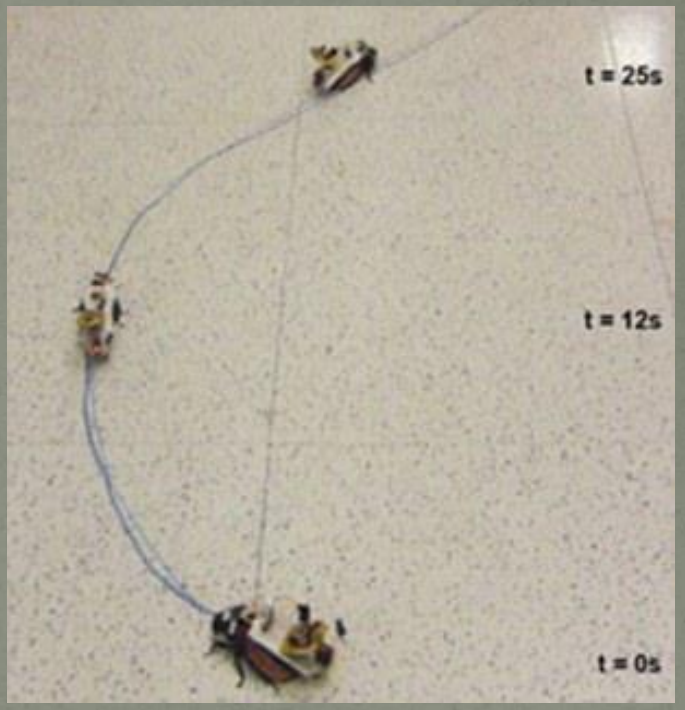
The bendy approach for visible light is reported in the New Journal of Physics.

Metamaterials work by interrupting and channelling the flow of light at a fundamental level; in a sense they can be seen as bouncing light waves around in a prescribed fashion to achieve a particular

Metamaterials work by interrupting and channelling the flow of light

# Cockroach Spies





CAMBRIDGE UNIVERSITY NEWS

**08:50 Friday 18 January 2013** Written by Chris Elliott

Tweet

# Taking a leap towards making teleportation a reality

Scientists in Cambridge have made a quantum leap that could lead to the creation of futuristic, superfast computers capable of teleportation.

Sergii Strelchuk

Experts from Cambridge University and other researchers around the world are trying to find a way of teleporting quantum information – sending huge amounts of data at incredible speed from one place to another.

Quantum teleportation, as it is known, relies on an aspect of physics known as "entanglement", where the properties of two particles can be linked together even when they are far apart.

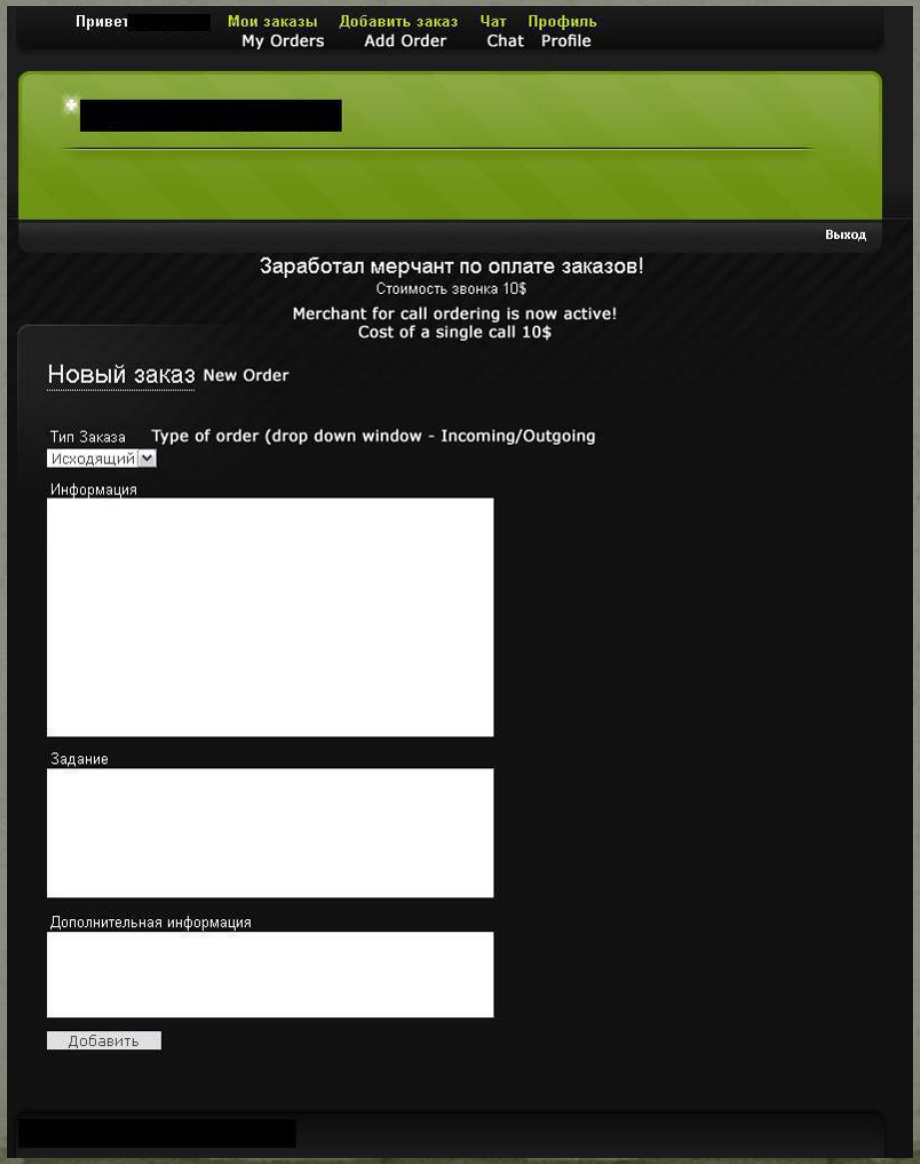
# #5
# Social Engineering as a Service

# 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

# Example

- Fraudster buys the credit card information of a 77-year old Italian woman from an underground forum.
- The fraudster wants to purchase expensive goods online (e.g. Laptops) to resell for cash.
- A credit card can cost as little as $2. A laptop might sell for $500. Big profit!
- To make the purchase, the fraudster must change the credit card's billing/delivery address. So he needs to call the card issuer.
- BUT he doesn't sound like a 77-year old Italian woman.


Привет [redacted]
Мои заказы
My Orders
Добавить заказ
Add Order
Чат
Chat
Профиль
Profile
[redacted]
Выход
Заработал мерчант по оплате заказов!
Стоимость звонка 10$
Merchant for call ordering is now active!
Cost of a single call 10$
Новый заказ New Order
Тип Заказа Type of order (drop down window - Incoming/Outgoing
Исходящий
Информация
Задание
Дополнительная информация
Добавить
[redacted]

Professional Call Service

Calling: Shops, Drops, Casinos, Banks, Hosting Companies, UPS, FedEX

9 english speaking males. 3 females

Italian: Male (15 WMZ, Calling time etc. May be discussed)

German: Only Female

Spoofing numbers to any number (USA)

Can accept incoming calls on mine or your number.

Can fix up a custom number by state.

Working hours – Mon-Fri. Sat. 18:00-02:00 Moscow Time.

(99% of days I am online until 04:00)

Prices:

Any call 12$

Incoming call 12$

Creating a number:

10$. Time To Live: 1 Week min, probably longer. Almost all area codes.

We accept money only for "full" calls: called the right location, talked with the person we needed to. We don't charge you for answering machines. No additional charge to leave a message. If an operation fails (example: failure in a balance transfer) because of insufficient data provided by customer we hold no responsibility (example: question about cardholder's neighbors, as we didn't have this info) and other reasons.

Its possible to arrange a drop-project phone support.

Returning customers are allowed to delay payment, discounts, etc.

Contact ICQ

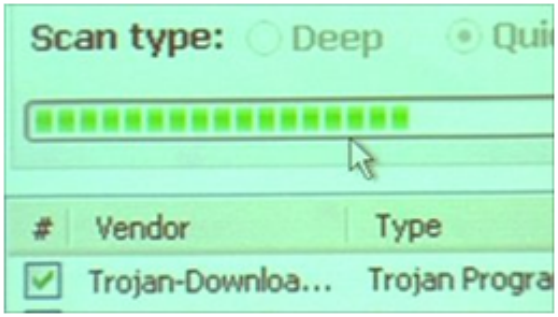
15 November 2010 Last updated at 12:56

# Warning over anti-virus cold-calls to UK internet users

**Internet users are being warned about cold-callers who offer to fix viruses but then install software to steal personal information.**

Campaign group Get Safe Online said a quarter of people it had questioned had received such calls, many suspected to have been from organised crime gangs.

Some gangs, employing up to 400 people, are known to set up their own call centres to target people en masse.



Faking it: One bogus scan uncovered by Soca

Internet users are also urged to be wary of pop-ups offering virus checks.

Earlier this year, search engine giant Google warned it had discovered massive amounts of malicious fake anti-virus software.

The UK warning on such software comes from Get Safe Online, which is backed by the government, police forces and major businesses with a stake in internet security.

## Related stories

Google warning on fake anti-virus

'Scareware' scams trick searchers

# The future of Social Engineering

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

# #6 More social engineering testing

## Dating coach shows how to get classified military intel using social engineering

*Hacking people is easy*

By Adrianne Jeffries *on August 4, 2013 01:00 pm* Email

COMMENTS

DON'T MISS STORIES *FOLLOW THE VERGE* Like 177k Follow 296K followers

Jordan Harbinger, a professional social engineer, gave a talk at Def Con about how to get defense contractors to give up sensitive information.

419

PART OF THIS STORYSTREAM 1

0 UPDATES TO