Ethical Hacking and Countermeasures

Version 6

Module XI

Social Engineering

Scenario

The Internal Revenue Service (IRS) annually processes over 222 million tax returns which are converted into electronic records on various IRS systems. This information is protected by law and considered sensitive. Maintaining this type of information could make the IRS a target for computer hackers.

In recent years, the IRS has successfully completed significant efforts in securing its computer network perimeters from external cyber threats. Because hackers are unable to gain access through these Internet gateways into the IRS, they are likely to seek other ways to gain access to IRS systems and, ultimately, taxpayer data.

One such method is social engineering, which involves exploiting the human aspect of computer security for the purpose of gaining insider information about an organization's computer resources. One of the most common tactics is to convince an organization's employees to reveal their passwords. Along with user account names, passwords are needed to identify and authenticate employees before allowing them access to systems and data.

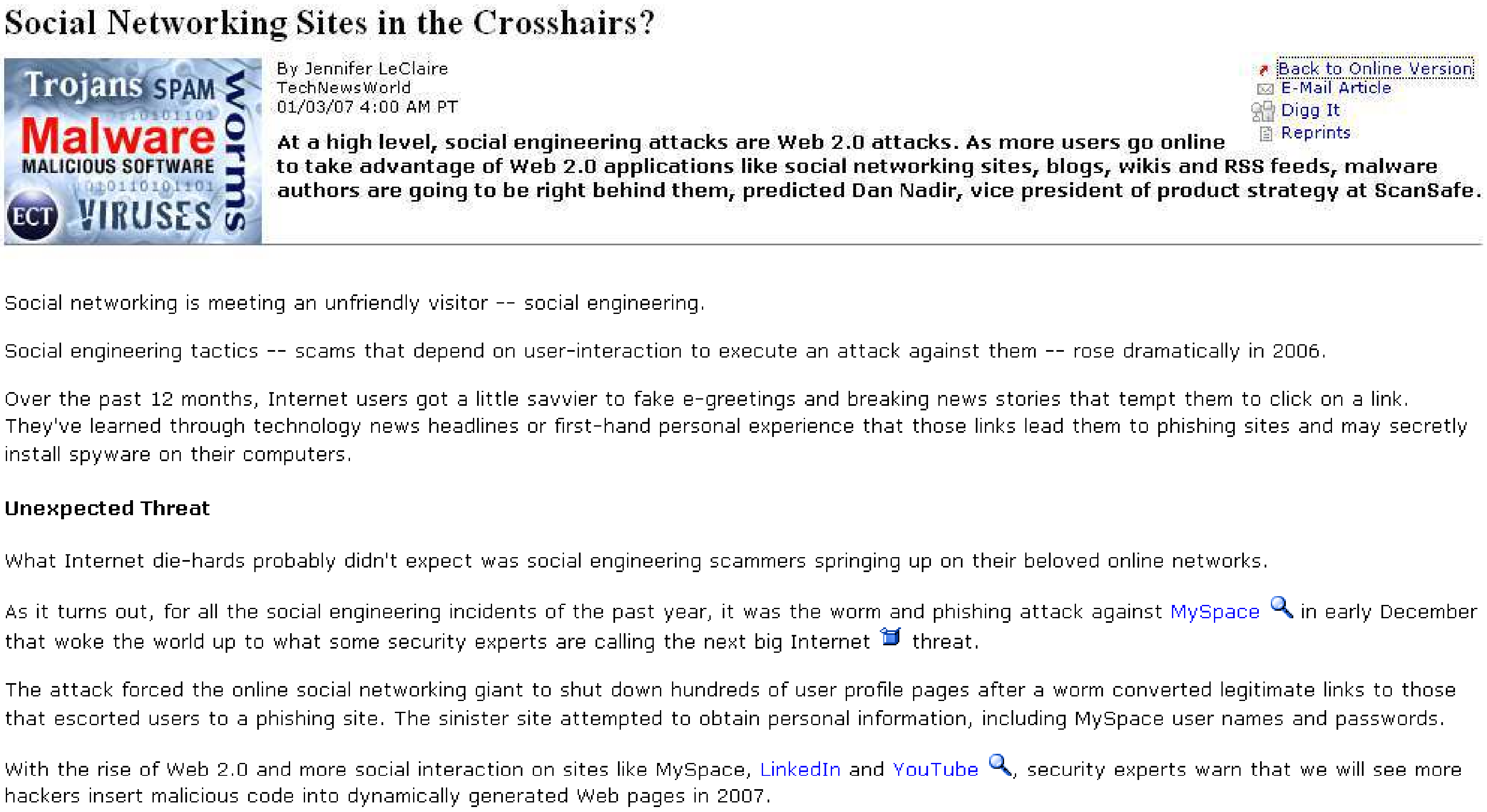
In August 2001, with the assistance of a contractor, we conducted social engineering tests on IRS employees as part of our penetration testing efforts. We placed calls to 100 IRS employees, asking them to change their password to one we suggested, and found 71 employees were willing to accommodate our requests.[1]

This review was conducted from our office in Walnut Creek, California, in December 2004. The audit was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Source: *http://www.treasury.gov/*

CEH™ Certified Ethical Hacker

News



Social Networking Sites in the Crosshairs?

By Jennifer LeClaire
TechNewsWorld
01/03/07 4:00 AM PT

At a high level, social engineering attacks are Web 2.0 attacks. As more users go online to take advantage of Web 2.0 applications like social networking sites, blogs, wikis and RSS feeds, malware authors are going to be right behind them, predicted Dan Nadir, vice president of product strategy at ScanSafe.

Social networking is meeting an unfriendly visitor -- social engineering.

Social engineering tactics -- scams that depend on user-interaction to execute an attack against them -- rose dramatically in 2006.

Over the past 12 months, Internet users got a little savvier to fake e-greetings and breaking news stories that tempt them to click on a link. They've learned through technology news headlines or first-hand personal experience that those links lead them to phishing sites and may secretly install spyware on their computers.

Unexpected Threat

What Internet die-hards probably didn't expect was social engineering scammers springing up on their beloved online networks.

As it turns out, for all the social engineering incidents of the past year, it was the worm and phishing attack against MySpace in early December that woke the world up to what some security experts are calling the next big Internet threat.

The attack forced the online social networking giant to shut down hundreds of user profile pages after a worm converted legitimate links to those that escorted users to a phishing site. The sinister site attempted to obtain personal information, including MySpace user names and passwords.

With the rise of Web 2.0 and more social interaction on sites like MySpace, LinkedIn and YouTube, security experts warn that we will see more hackers insert malicious code into dynamically generated Web pages in 2007.

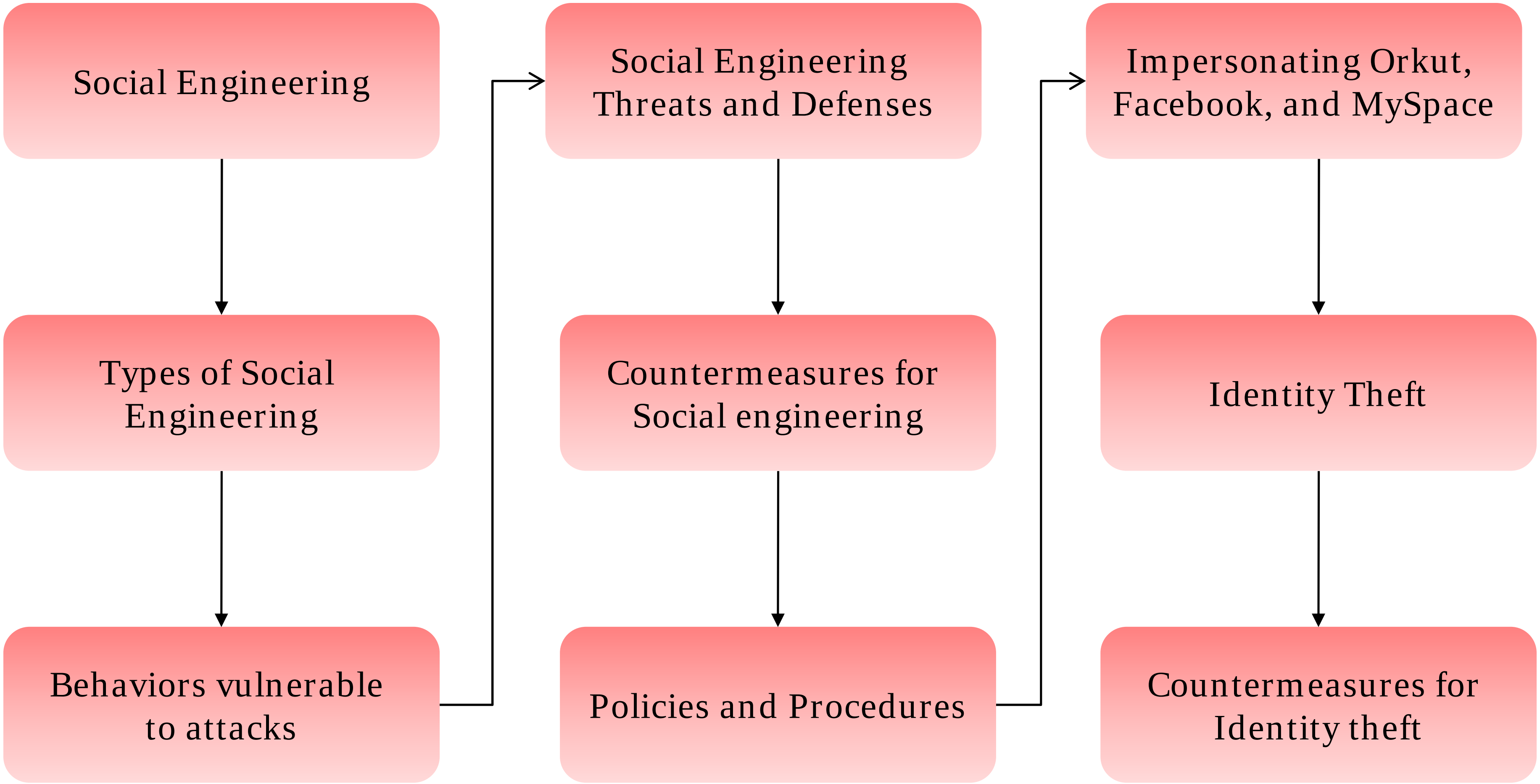
Source: *http://www.technewsworld.com/*

Module Objective

This module will familiarize you with:

- Social Engineering
- Types of Social Engineering
- Behaviors vulnerable to attacks
- Social Engineering Threats and Defenses
- Countermeasures for Social engineering
- Policies and Procedures
- Impersonating Orkut, Facebook, and MySpace
- Identity Theft
- Countermeasures for Identity theft

Module Flow


Social Engineering
Types of Social Engineering
Behaviors vulnerable to attacks
Social Engineering Threats and Defenses
Countermeasures for Social engineering
Policies and Procedures
Impersonating Orkut, Facebook, and MySpace
Identity Theft
Countermeasures for Identity theft

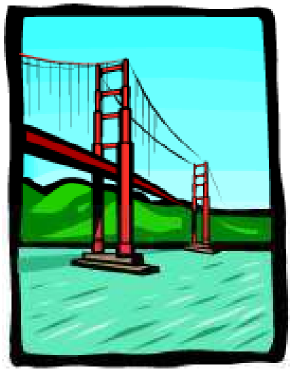
There is No Patch to Human Stupidity

What is Social Engineering

Social Engineering is the human side of breaking into a corporate network

Companies with authentication processes, firewalls, virtual private networks, and network monitoring software are still open to attacks

An employee may unwittingly give away key information in an email or by answering questions over the phone with someone they do not know, or even by talking about a project with coworkers at a local pub after hours



EC-Council

What is Social Engineering (cont’d)

Social engineering is the tactic or trick of gaining sensitive information by exploiting the basic human nature such as:

- Trust
- Fear
- Desire to Help

Social engineers attempt to gather information such as:

- Sensitive information
- Authorization details
- Access details

EC-Council

Human Weakness

People are usually the weakest link in the security chain

A successful defense depends on having good policies and educating employees to follow them

Social Engineering is the hardest form of attack to defend against because it cannot be defended with hardware or software alone

“Rebecca” and “Jessica”

Hackers use the term “Rebecca” and “Jessica” to denote social engineering attacks

Hackers commonly use these terms to social engineer victims

Rebecca and Jessica mean a person who is an easy target for social engineering, such as the receptionist of a company

Example:

- “There was a **Rebecca** at the bank and I am going to call her to extract the privileged information.”
- “I met **Ms. Jessica**, she was an easy target for social engineering.”
- “Do you have any **Rebecca** in your company?”

Office Workers

Despite having the best firewall, intrusion-detection and antivirus systems, technology has to offer, you are still hit with security breaches

One reason for this may be lack of motivation among workers

Hackers can attempt social engineering attack on office workers to extract sensitive data such as:

- Security policies
- Sensitive documents
- Office network infrastructure
- Passwords

Types of Social Engineering

Social Engineering can be divided into two categories:

- Human-based:
  - Gathers sensitive information by interaction
  - Attacks of this category exploitstrust, fear, and helping nature of humans
- Computer-Based:
  - Social engineering is carriedout with the aid of computers

Human-Based Social Engineering

Posing as a Legitimate End User

- Gives identity and asks for the sensitive information
- *"Hi! This is John, from Department X. I have forgotten my password. Can I get it?"*

Posing as an Important User

- Posing as a VIP of a target company, valuable customer, etc.
- *"Hi! This is Kevin, CFO Secretary. I'm working on an urgent project and lost system password. Can you help me out?"*

Human-Based Social Engineering (cont’d)

Posing as Technical Support

- Calls as a technical support staff, and requests id & passwords to retrieve data
- *‘Sir, this is Mathew, Technical support, X company. Last night we had a system crash here, and we are checking for the lost data. Can u give me your ID and Password?’*

Technical Support Example

A man calls a company's help desk and says he's forgotten his password. In a panic, he adds that if he misses the deadline on a big advertising project, his boss might fire him. The help desk worker feels sorry for him and quickly resets the password unwittingly giving the hacker clear entrance into the corporate network

More Social Engineering Examples

"Hi, I'm John Brown. I'm with the external auditors Arthur Sanderson. We've been told by corporate to do a surprise inspection of your disaster recovery procedures. Your department has 10 minutes to show me how you would recover from a Website crash."

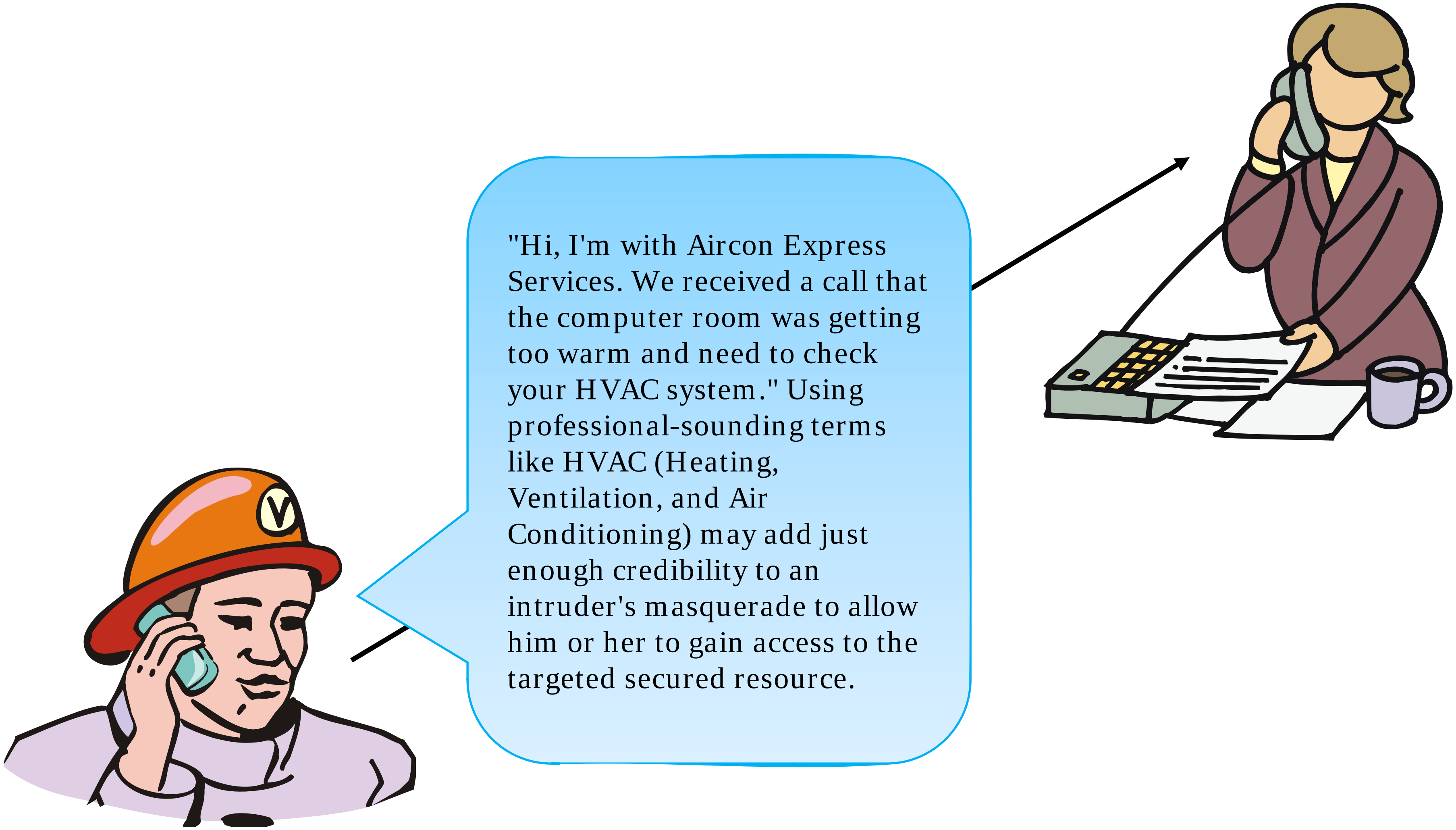
More Social Engineering Examples

"Hi I'm Sharon, a sales rep out of the New York office. I know this is short notice, but I have a group of perspective clients out in the car that I've been trying for months to get to outsource their security training needs to us.

They're located just a few miles away and I think that if I can give them a quick tour of our facilities, it should be enough to push them over the edge and get them to sign up.

Oh yeah, they are particularly interested in what security precautions we've adopted. Seems someone hacked into their Website a while back, which is one of the reasons they're considering our company."

More Social Engineering Examples



"Hi, I'm with Aircon Express Services. We received a call that the computer room was getting too warm and need to check your HVAC system." Using professional-sounding terms like HVAC (Heating, Ventilation, and Air Conditioning) may add just enough credibility to an intruder's masquerade to allow him or her to gain access to the targeted secured resource.

Human-Based Social Engineering: Eavesdropping

Eavesdropping or unauthorized listening of conversations or reading of messages

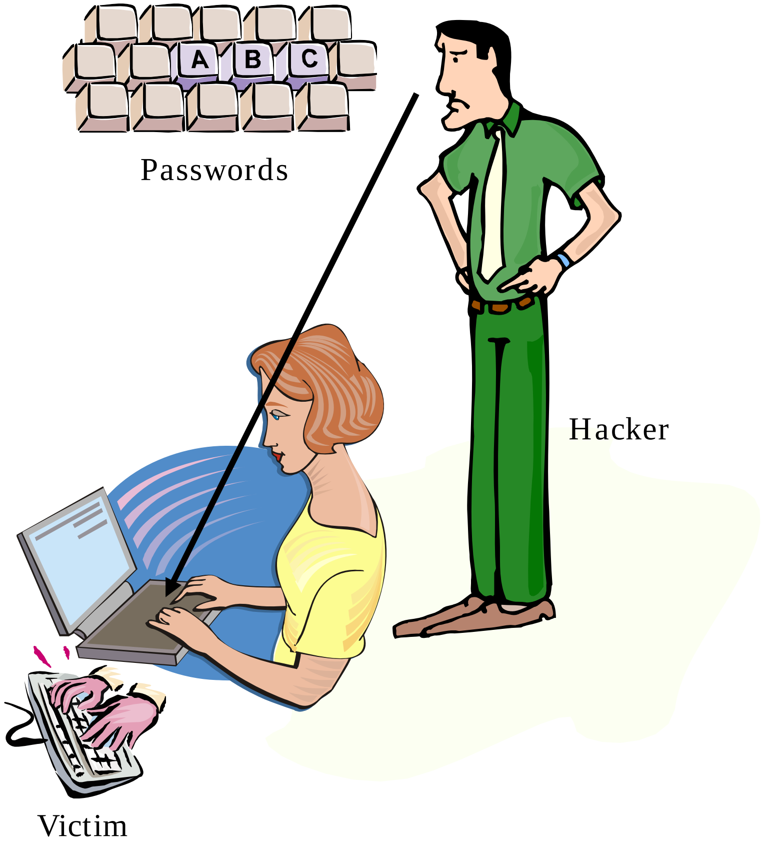
Interception of any form such as audio, video, or written

Human-Based Social Engineering: Shoulder Surfing

Looking over your shoulder as you enter a password

Shoulder surfing is the name given to the procedure that identity thieves use to find out passwords, personal identification number, account numbers, and more

Simply, they look over your shoulder--or even watch from a distance using binoculars, in order to get those pieces of information



Human-Based Social Engineering: Dumpster Diving

Search for sensitive information at target company's:

- Trash-bins
- Printer Trash bins
- user desk for sticky notes etc

Collect:

- Phone Bills
- Contact Information
- Financial Information
- Operations related Information etc

Dumpster Diving Example

A man behind the building is loading the company's paper recycling bins into the back of a truck. Inside the bins are lists of employee titles and phone numbers, marketing plans, and the latest company financials

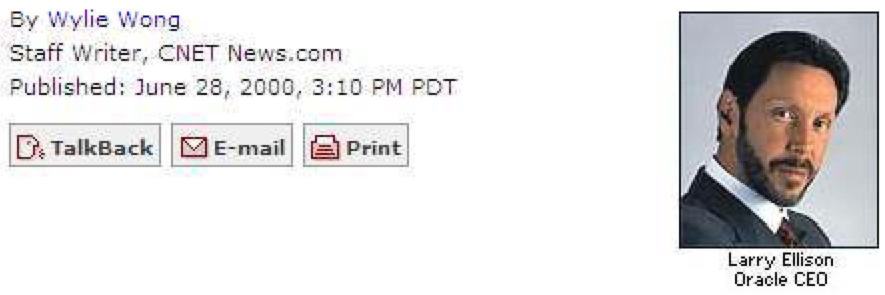
This information is sufficient to launch a social engineering attack on the company

Dumpster Diving Example

For example, if the hacker appears to have a good working knowledge of the staff in a company department, he or she will probably be more successful while making an approach; most staff will assume that someone who knows a lot about the company must be a valid employee

Oracle Snoops Microsoft's Trash Bins

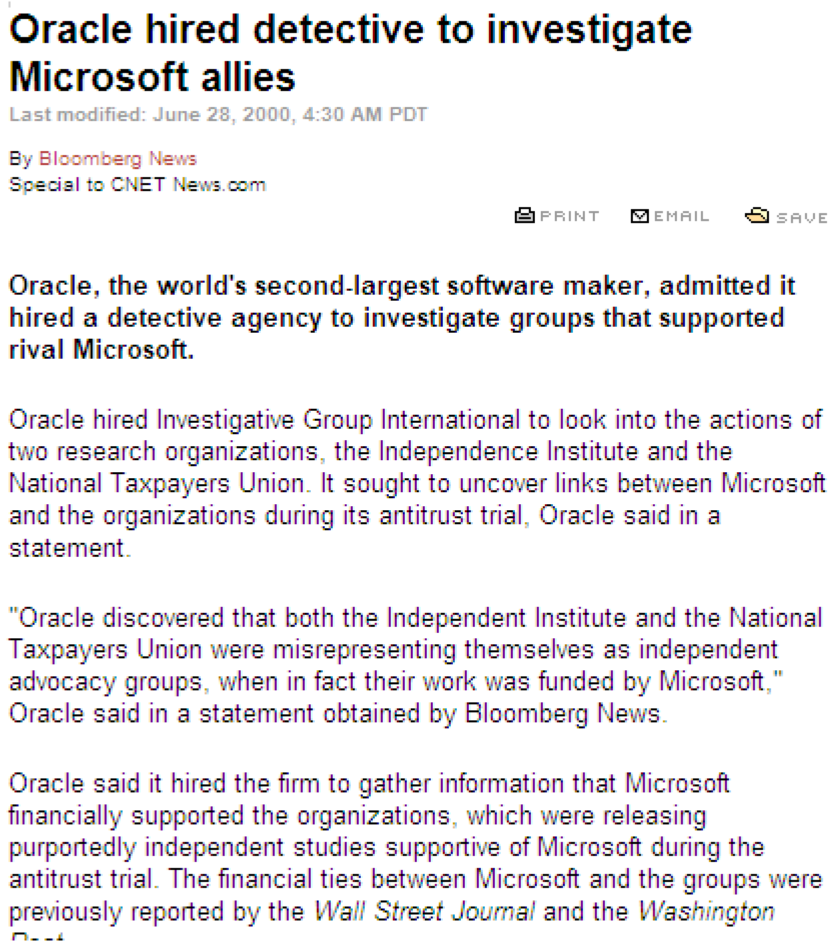
Oracle chief defends Microsoft snooping



By Wylie Wong
Staff Writer, CNET News.com
Published: June 28, 2000, 3:10 PM PDT

Larry Ellison
Oracle CEO

> "We weren't spying. We were trying to expose what Microsoft was doing," said a fiery Ellison when reporters asked repeatedly about the detective agency's attempts at buying garbage.



Oracle hired detective to investigate Microsoft allies

Last modified: June 28, 2000, 4:30 AM PDT

By Bloomberg News
Special to CNET News.com

Oracle, the world's second-largest software maker, admitted it hired a detective agency to investigate groups that supported rival Microsoft.

Oracle hired Investigative Group International to look into the actions of two research organizations, the Independence Institute and the National Taxpayers Union. It sought to uncover links between Microsoft and the organizations during its antitrust trial, Oracle said in a statement.

"Oracle discovered that both the Independent Institute and the National Taxpayers Union were misrepresenting themselves as independent advocacy groups, when in fact their work was funded by Microsoft," Oracle said in a statement obtained by Bloomberg News.

Oracle said it hired the firm to gather information that Microsoft financially supported the organizations, which were releasing purportedly independent studies supportive of Microsoft during the antitrust trial. The financial ties between Microsoft and the groups were previously reported by the *Wall Street Journal* and the *Washington*

Human-Based Social Engineering (cont'd)

In person

- Survey a target company to collect information on
  - Current technologies
  - Contact information, and so on

Third-party Authorization

- Refer to an important person in the organization and try to collect data
- *"Mr. George, our Finance Manager, asked that I pick up the audit reports. Will you please provide them to me?"*

Human-Based Social Engineering (cont'd)

Tailgating

- An unauthorized person, wearing a fake ID badge, enters a secured area by closely following an authorized person through a door requiring key access
- An authorized person may be unawareof providing an unauthorized person access to a secured area

Piggybacking

- *"I forgot my ID badge at home. Please help me."*
- An authorized person provides access toan unauthorized person by keeping the secured door open

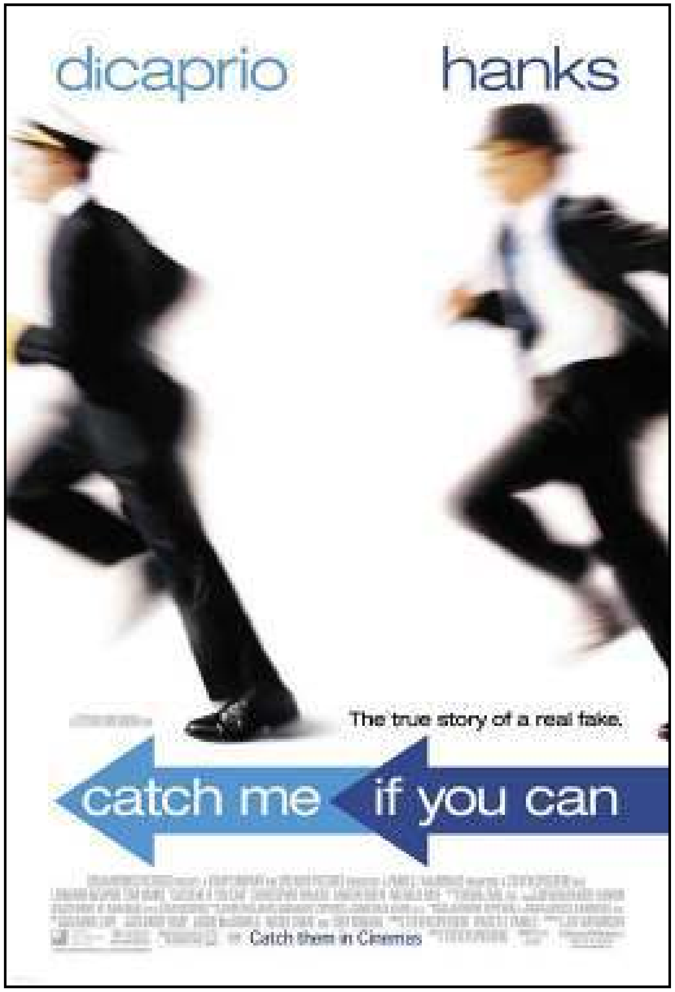
EC-Council

Human-Based Social Engineering (cont'd)

Reverse Social Engineering

- This is when the hacker creates a persona that appears to be in a position of authority so that employees will ask him for information, rather than the other way around
- Reverse Social Engineering attack involves
  - Sabotage
  - Marketing
  - Providing Support

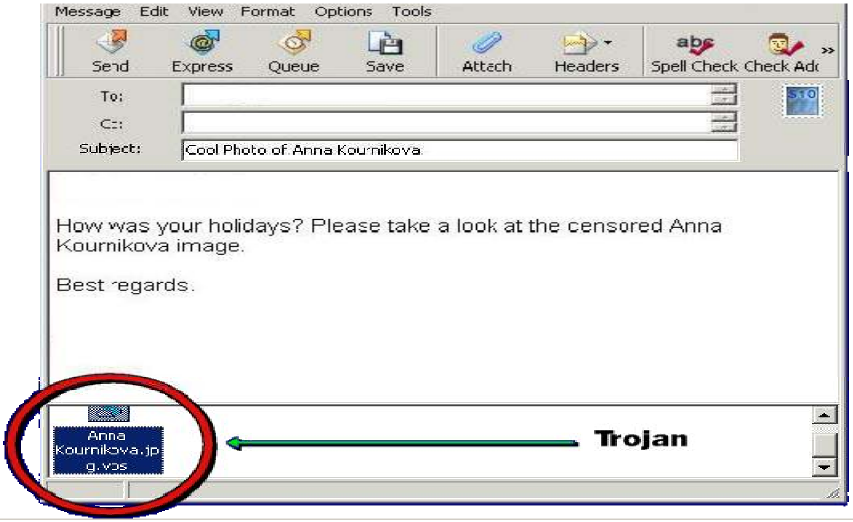
Movies to Watch for Reverse Engineering Examples: The *Italian Job* and *Catch Me If You Can*



Computer-Based Social Engineering

It can be divided:

- Mail / IM attachments
- Pop-up Windows
- Websites / Sweepstakes
- Spam mail

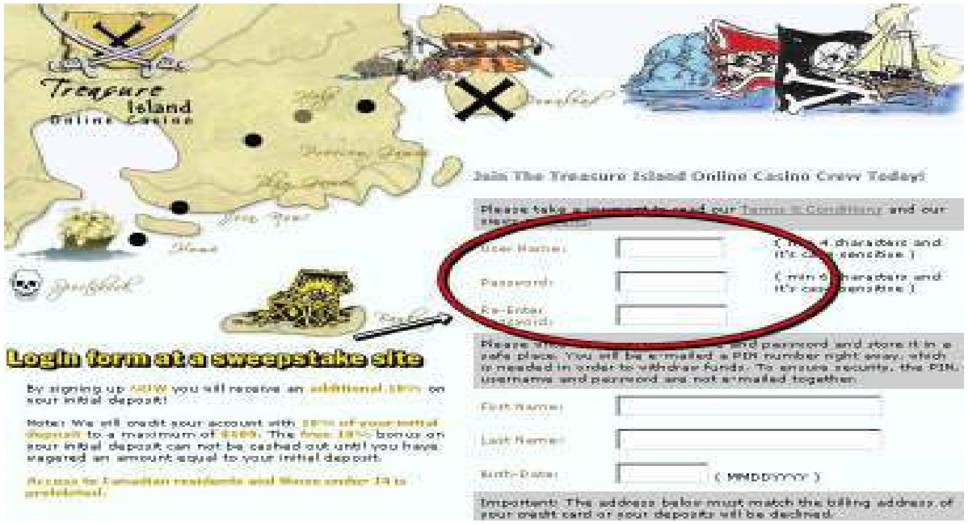


Subject: Cool Photo of Anna Kournikova

How was your holidays? Please take a look at the censored Anna Kournikova image.

Best regards.

Anna Kournikova.jpg.vbs



Join The Treasure Island Online Casino Crew Today!

Please take a moment to read our Terms & Conditions and our [illegible]

User Name: (min 4 characters and it's case sensitive)

Password: (min 6 characters and it's case sensitive)

Re-Enter Password:

Please [illegible] and password and store it in a safe place. You will be e-mailed a PIN number right away, which is needed in order to withdraw funds. To ensure security, the PIN, username and password are not e-mailed together.

First Name:

Last Name:

Birth-Date: (MMDDYYYY)

Important: The address below must match the billing address of your credit card or your deposits will be declined.

By signing up NOW you will receive an additional 10% on your initial deposit!

Note: We will credit your account with 10% of your initial deposit to a maximum of $100. The free 10% bonus on your initial deposit can not be cashed out until you have wagered an amount equal to your initial deposit.

Access to Canadian residents and those under 19 is prohibited.

Login form at a sweepstake site

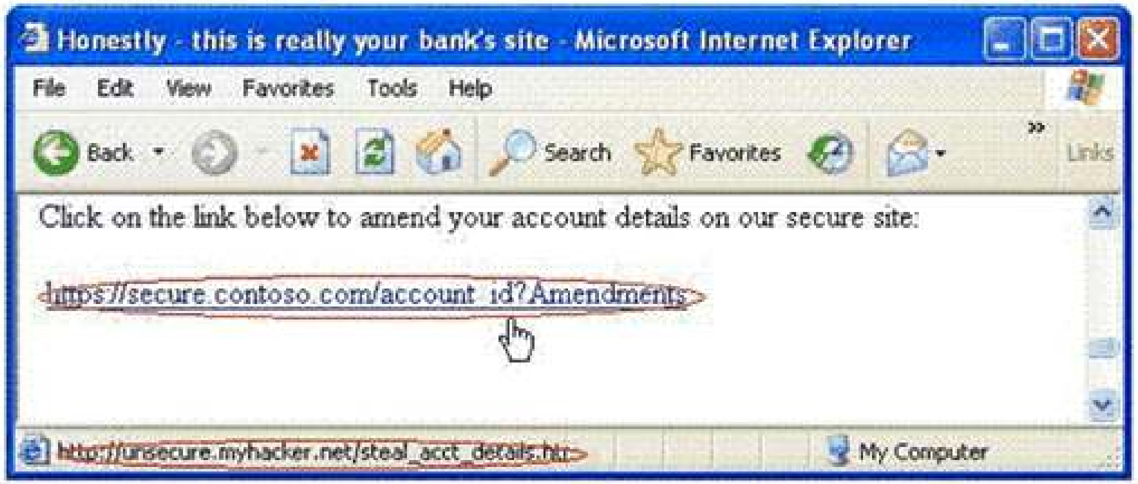
Computer-Based Social Engineering (cont'd)

Pop-up Windows

- Windows that suddenly pops up, while surfing the Internet and asks for users' information to login or sign-in

Hoaxes and chain letters

- Hoax letters are emails that issue warningsto user on new virus, Trojans or worms that may harm the user's system
- Chain letters are emails that offer free gifts such as money, and software on the condition that if the user forwards the mail to said number of persons

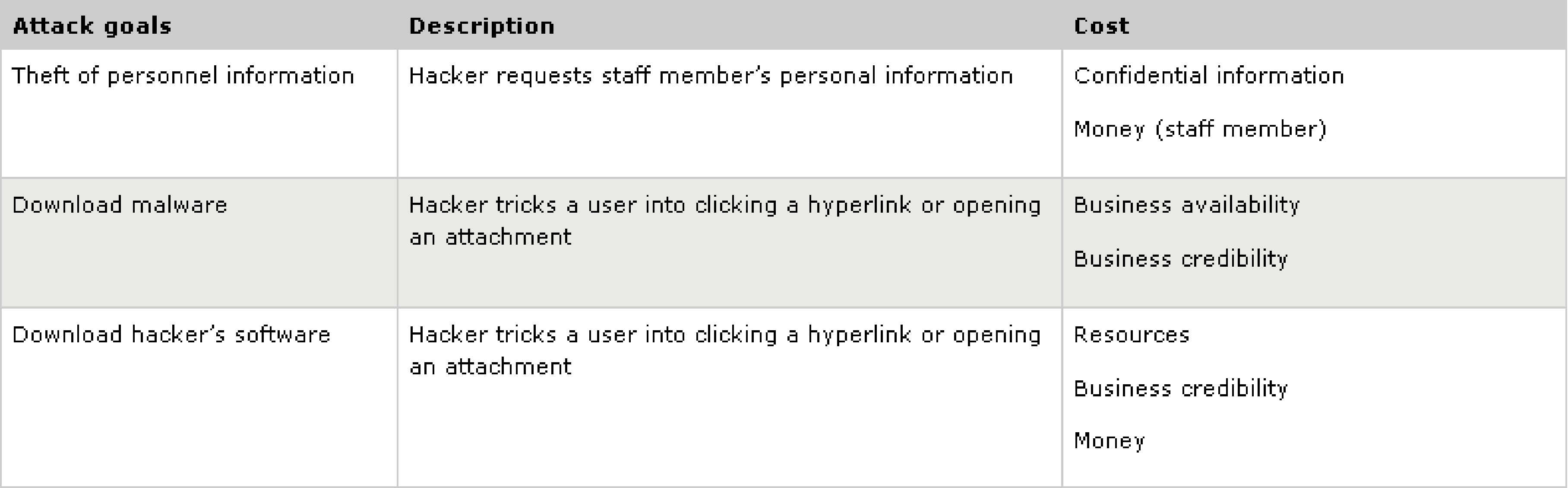

Honestly - this is really your bank's site - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Links
My Computer

Click on the link below to amend your account details on our secure site:

https://secure.contoso.com/account_id?Amendments

http://unsecure.myhacker.net/steal_acct_details.htm

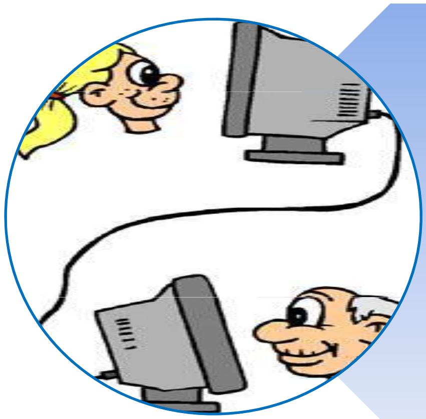
Computer-Based Social Engineering (cont'd)



Attack goals	Description	Cost
Theft of personnel information	Hacker requests staff member's personal information	Confidential information Money (staff member)
Download malware	Hacker tricks a user into clicking a hyperlink or opening an attachment	Business availability Business credibility
Download hacker's software	Hacker tricks a user into clicking a hyperlink or opening an attachment	Resources Business credibility Money

Online Pop-Up Attacks and Costs

Computer-Based Social Engineering (cont'd)



Instant Chat Messenger

- Gathering of personal information by chatting witha selected online user to attempt to get information such as birth dates and maiden names
- Acquired data is later used for cracking the users' accounts

Spam email

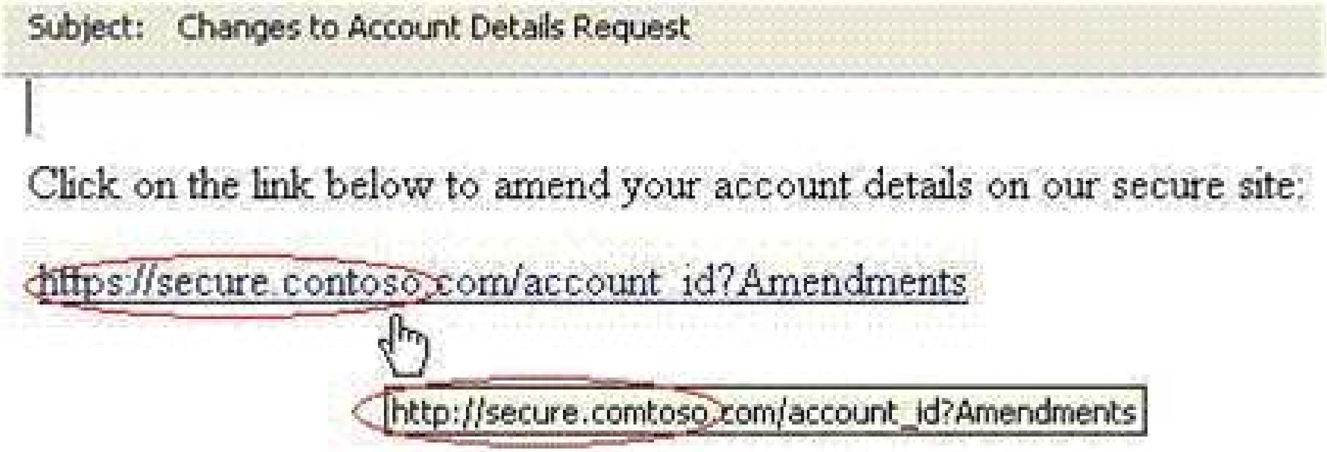
- Email sent to many recipients without prior permission intended for commercial purposes
- Irrelevant, unwanted, and unsolicited email to collect financial information, social security numbers, and network information

Computer-Based Social Engineering (cont'd)

Phishing

- An illegitimate email falsely claiming to be from a legitimate site attempts to acquire user's personal or account information
- Lures online users with statements such as
  - *Verify your account*
  - *Update your information*
  - *Your account will be closed or suspended*
- Spam filters, anti-phishing tools integrated with web browsers can be used to protect from *Phishers*

Computer-Based Social Engineering (cont'd)



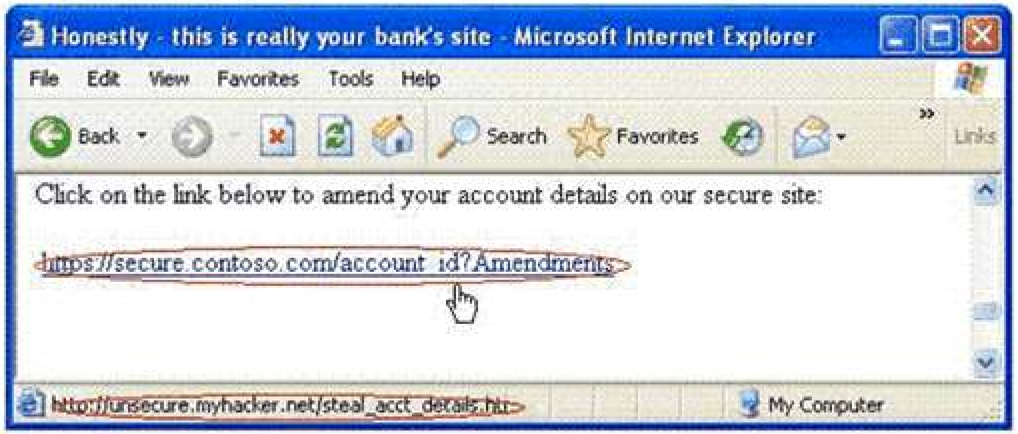
Subject: Changes to Account Details Request

Click on the link below to amend your account details on our secure site:

https://secure.contoso.com/account_id?Amendments

http://secure.comtoso.com/account_id?Amendments

E-mail phishing hyperlink



Honestly - this is really your bank's site - Microsoft Internet Explorer

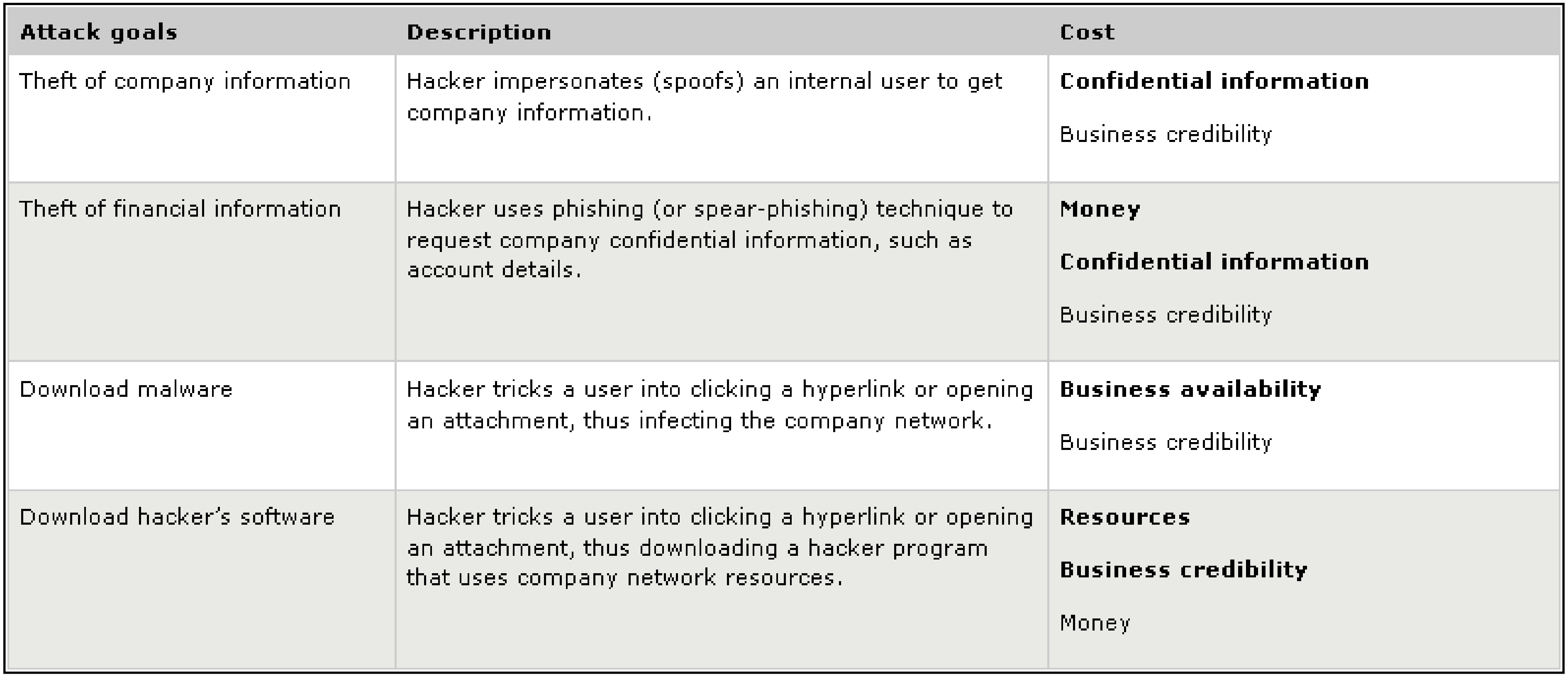
Click on the link below to amend your account details on our secure site:

https://secure.contoso.com/account_id?Amendments

http://unsecure.myhacker.net/steal_acct_details.htr

Web page phishing hyperlink

Computer-Based Social Engineering (cont'd)



Attack goals	Description	Cost
Theft of company information	Hacker impersonates (spoofs) an internal user to get company information.	**Confidential information** Business credibility
Theft of financial information	Hacker uses phishing (or spear-phishing) technique to request company confidential information, such as account details.	**Money** **Confidential information** Business credibility
Download malware	Hacker tricks a user into clicking a hyperlink or opening an attachment, thus infecting the company network.	**Business availability** Business credibility
Download hacker's software	Hacker tricks a user into clicking a hyperlink or opening an attachment, thus downloading a hacker program that uses company network resources.	**Resources** **Business credibility** Money

Online E-mail Attacks and Costs

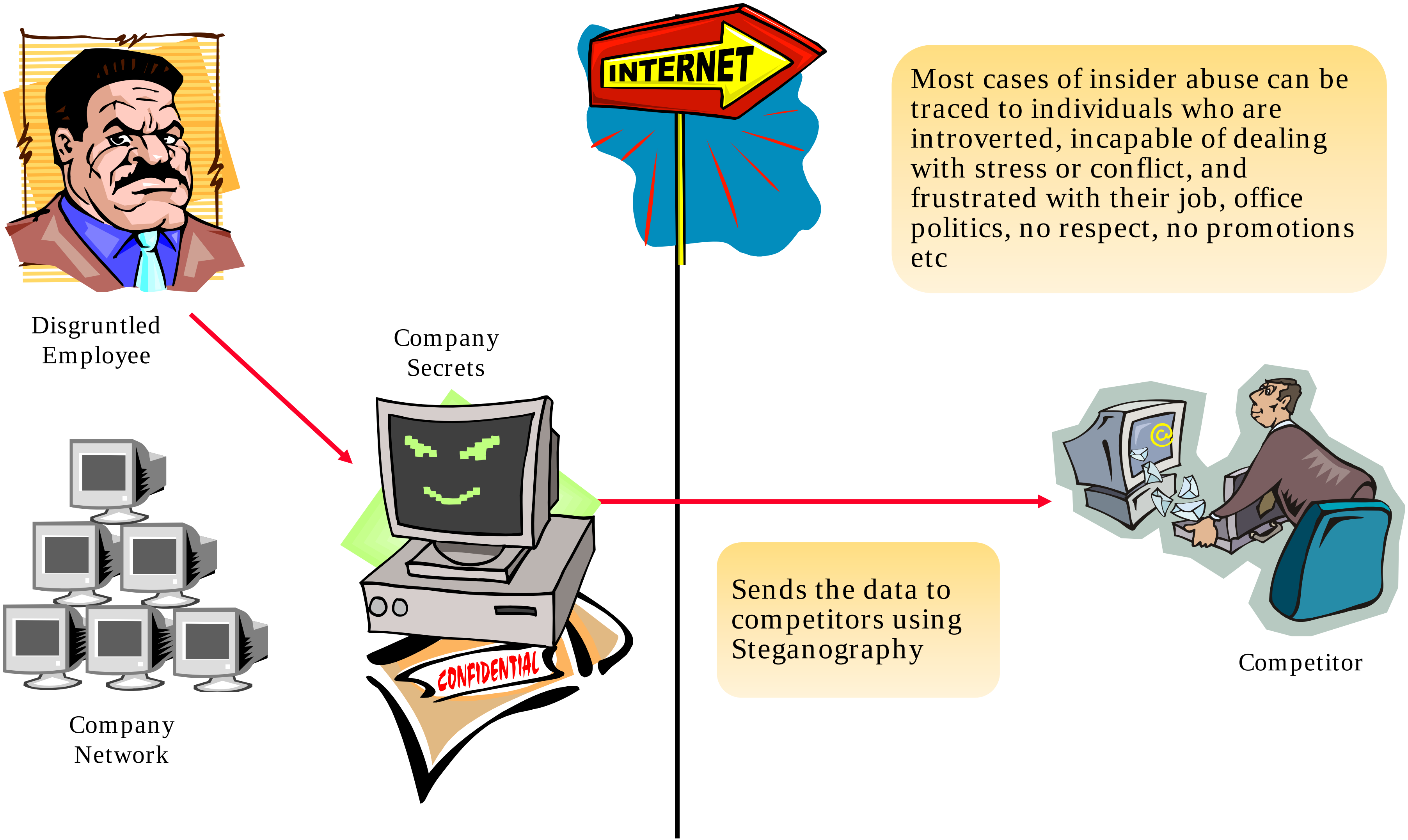
Insider Attack

If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization

It takes only one disgruntled person to take revenge and your company is compromised

- 60% of attacks occur behind the firewall
- An inside attack is easy to launch
- Prevention is difficult
- The inside attacker can easily succeed
- Difficult to catch the perpetrator

Disgruntled Employee



Most cases of insider abuse can be traced to individuals who are introverted, incapable of dealing with stress or conflict, and frustrated with their job, office politics, no respect, no promotions etc

Sends the data to competitors using Steganography

EC-Council

Preventing Insider Threat

There is no single solution to prevent an insider threat

Some recommendations:

- Separation of duties
- Rotation of duties
- Least privilege
- Controlled access
- Logging and auditing
- Legal policies
- Archive critical data

Common Targets of Social Engineering

Receptionists and help desk personnel

Technical support executives

Vendors of target organization

System administrators and users

Social Engineering Threats and Defenses

EC-Council

Social Engineering Threats and Defenses

Major attack vectors that a social engineering hacker uses:

- Online
- Telephone
- Personal approaches
- Reverse social engineering

Online Threats

In a connected business world, staff often use and respond to requests and information that come electronically

This connectivity enables hackers to make approaches to staff from the relative anonymity of Internet

Online attacks, such as e-mail, pop-up application, and instant message attacks; use Trojan horses, worms, or viruses(malware) to damage or subvert computer resources

Social engineering hacker persuades a staff member to provide information through a believable ruse, rather than infecting a computer with malware through a direct attack

An attack may provide information that enables hacker to make a subsequent malware attack

Solution: Advise staff on how to identify and avoid online social engineering attacks

Telephone-Based Threats

Telephone offers a unique attack vector for social engineering hackers

It is a familiar medium, but it is also impersonal, because target cannot see the hacker

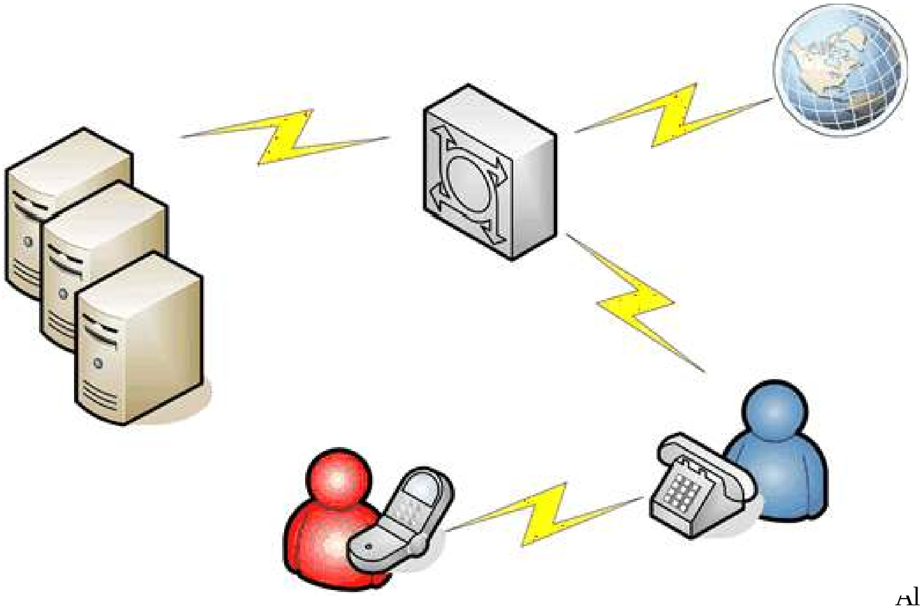
Communication options for most computer systems can also make Private Branch Exchange (PBX) an attractive target

Stealing either credit card or telephone card PINs at telephone booths is another kind of attack

Telephone-Based Threats (cont'd)

There are three major goals for a hacker who attacks a PBX:

- Request information, usually through the imitationof a legitimate user, either to access the telephone system itself or to gain remote access to computer systems
- Gain access to "free" telephone usage
- Gain access to communications network



Telephony PBX attack

Personal Approaches

The simplest and cheapest way for a hacker to get information is to ask for it directly

This approach may seem crude and obvious, but it has been bedrock of confidence tricks since time began

Four main successful approaches for social engineers:

- Intimidation
- Persuasion
- Ingratiation
- Assistance

Defenses Against Social Engineering Threats

After you understand the wide range of threats, 3 steps are necessary to defend against social engineering threats

- Develop a security management framework
- Undertake risk management assessments
- Implement social engineering defenses within your security policy

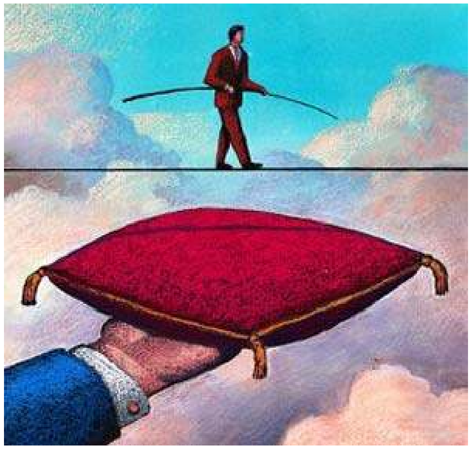
Defenses Against Social Engineering Threats (cont’d)

Risk Assessment:

- You need to assess the level of risk that an attack possesses towards your company for deploying suitable security measures

Risk categories include:

- Confidential information
- Business credibility
- Business availability
- Resources
- Money



Factors that make Companies Vulnerable to Attacks

Insufficient security training and awareness

Several organizational units

Lack of appropriate security policies

Easy access of information e.g. e-mail Ids and phone extension numbers of employees

EC-Council

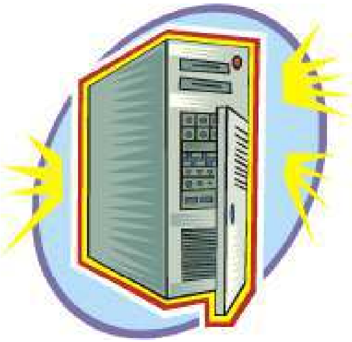
Why is Social Engineering Effective

Security policies are as strong as its weakest link, and humans are the most susceptible factor

Difficult to detect social engineering attempts

There is no method to ensure the complete security from social engineering attacks

No specific software or hardware for defending against a social engineering attack



Warning Signs of an Attack

An attacker may:

- Show inability to give valid callback number
- Make informal requests
- Claim of authority
- Show haste
- Unusually compliment or praise
- Show discomfort when questioned
- Drop the name inadvertently
- Threaten of dire consequences if information is not provided

Tool : Netcraft Anti-Phishing Toolbar

www.netcraft.com

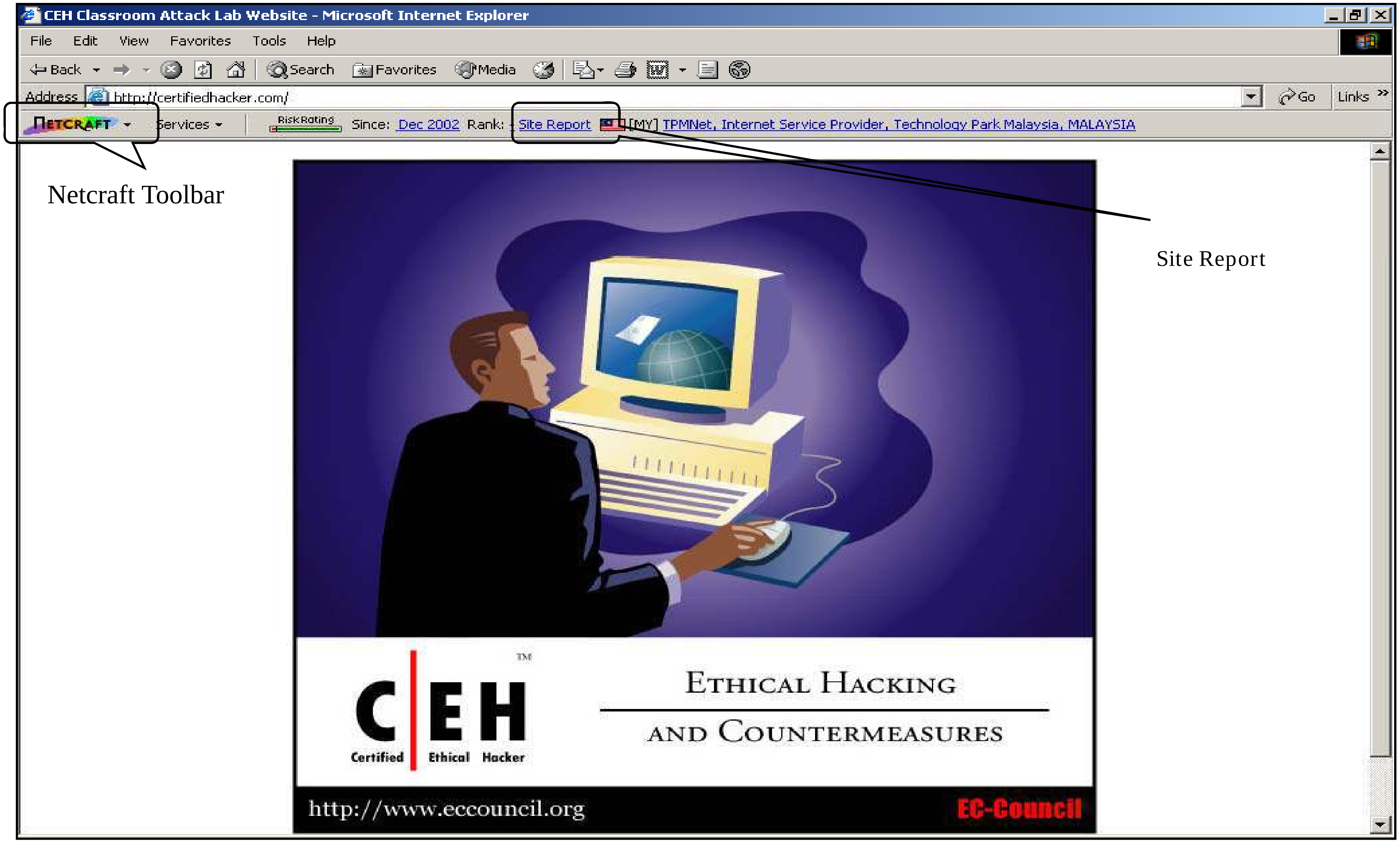
An anti-phishing system consisting of a toolbar and a central server that has information about URLs provided by Toolbar community and Netcraft

Blocks phishing websites that are recorded in Netcraft's central server

Suspicious URLs can be reported to *Netcraft* by clicking *Report a Phishing Site* in the toolbar menu

Shows all the attributes of each site such as host location, country, longevity, and popularity

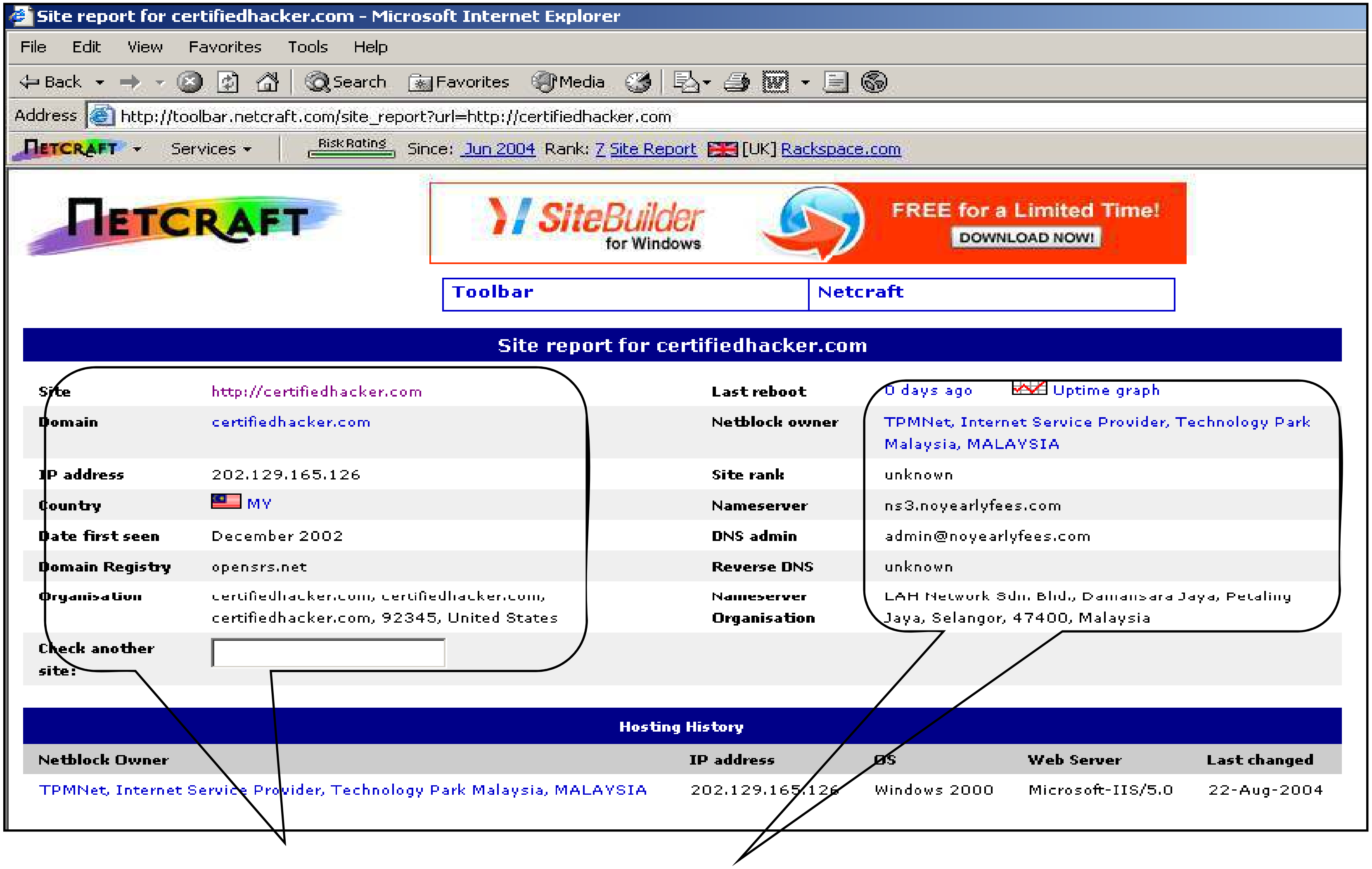
Tool : Netcraft Anti-Phishing Toolbar (cont'd)


CEH Classroom Attack Lab Website - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address http://certifiedhacker.com/
Go
Links
NETCRAFT
Services
Risk Rating
Since: Dec 2002 Rank: Site Report [MY] TPMNet, Internet Service Provider, Technology Park Malaysia, MALAYSIA
CEH Certified Ethical Hacker
ETHICAL HACKING AND COUNTERMEASURES
http://www.eccouncil.org
EC-Council

Netcraft Toolbar

Site Report

Tool : Netcraft Anti-Phishing Toolbar (cont'd)



Site report for certifiedhacker.com - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
NETCRAFT Services Risk Rating
SiteBuilder for Windows FREE for a Limited Time! DOWNLOAD NOW!
Toolbar
Netcraft

http://toolbar.netcraft.com/site_report?url=http://certifiedhacker.com

Since: Jun 2004 Rank: 7 Site Report [UK] Rackspace.com

Site report for certifiedhacker.com

Site	http://certifiedhacker.com	**Last reboot**	0 days ago Uptime graph
Domain	certifiedhacker.com	**Netblock owner**	TPMNet, Internet Service Provider, Technology Park Malaysia, MALAYSIA
IP address	202.129.165.126	**Site rank**	unknown
Country	MY	**Nameserver**	ns3.noyearlyfees.com
Date first seen	December 2002	**DNS admin**	admin@noyearlyfees.com
Domain Registry	opensrs.net	**Reverse DNS**	unknown
Organisation	certifiedhacker.com, certifiedhacker.com, certifiedhacker.com, 92345, United States	**Nameserver Organisation**	LAH Network Sdn. Bhd., Damansara Jaya, Petaling Jaya, Selangor, 47400, Malaysia
Check another site:			

Hosting History

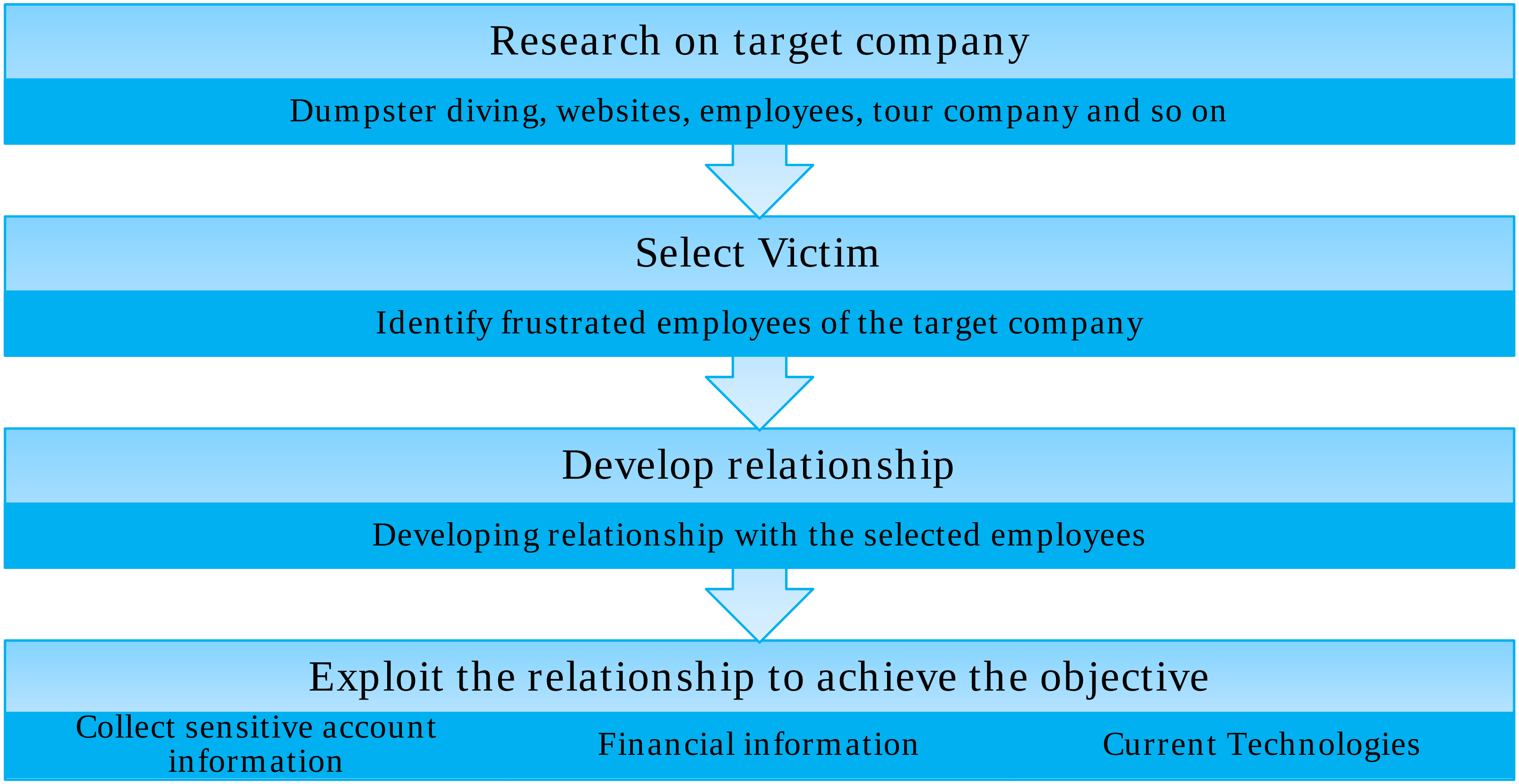
Netblock Owner	IP address	OS	Web Server	Last changed
TPMNet, Internet Service Provider, Technology Park Malaysia, MALAYSIA	202.129.165.126	Windows 2000	Microsoft-IIS/5.0	22-Aug-2004

Location details

Website Network Information

Phases in a Social Engineering Attack

Four phases of a Social Engineering Attack:



Research on target company

Dumpster diving, websites, employees, tour company and so on

Select Victim

Identify frustrated employees of the target company

Develop relationship

Developing relationship with the selected employees

Exploit the relationship to achieve the objective

Collect sensitive account information

Financial information

Current Technologies

Behaviors Vulnerable to Attacks

Trust

- Human nature of trust is the basis of any social engineering attack

Ignorance

- Ignorance about social engineering and its effectsamong the workforce makes the organization an easy target

Fear

- Social engineers might threaten severelosses in case of non- compliance with their request

Greed

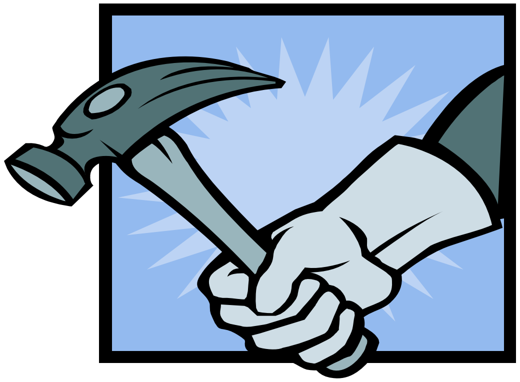
- Social engineers lure the targets to divulge information by promising something for nothing

Moral duty

- Targets are asked for the help, and they comply out of a sense of moral obligation

Impact on the Organization

- Economic losses
- Damage of goodwill
- Loss of privacy
- Dangers of terrorism
- Lawsuits and arbitrations
- Temporary or permanent closure



Countermeasures

Training

- An efficient training program shouldconsist of all security policies and methods to increase awareness on social engineering

Countermeasures (cont'd)

Password policies

- Periodic password change
- Avoiding guessable passwords
- Account blocking after failed attempts
- Length and complexity of passwords
  - Minimum number of characters, use of special characters, and numbers etc. e.g. **ar1f23#$g**
- Secrecy of passwords
  - Do not reveal if asked, or write on anything to remember them

Countermeasures (cont'd)

Operational guidelines

- Ensure security of sensitive information and authorized use of resources

Physical security policies

- Identification of employees e.g. issuing of ID cards, uniforms and so on
- Escorting the visitors
- Accessing area restrictions
- Proper shredding of useless documents
- Employing security personnel

Countermeasures (cont’d)

Classification of Information

- Categorize the information as top secret, proprietary, for internal use only, for public use, and so on

Access privileges

- Administrator, user, and guest accounts with proper authorization

Background check of employees and proper termination process

- Insiders with a criminal background and terminated employees are easy targets for procuring information

Proper incidence response system

- There should be proper guidelines for reacting in case of a social engineering attempt

Policies and Procedures

Policy is the most critical component for any information security program

Good policies and procedures are ineffective if they are not taught and reinforced by the employees

Employees need to emphasize their importance

After receiving training, the employee should sign a statement acknowledging that they understand the policies

Security Policies - Checklist

- Account setup
- Password change policy
- Help desk procedures
- Access privileges
- Violations
- Employee identification
- Privacy policy
- Paper documents
- Modems
- Physical access restrictions
- Virus control

What Happened Next

We were able to convince 35 managers and employees to provide us their username and to change their password.

The 35 managers and employees who were willing to change their password gave several reasons why they were willing to accommodate our request.

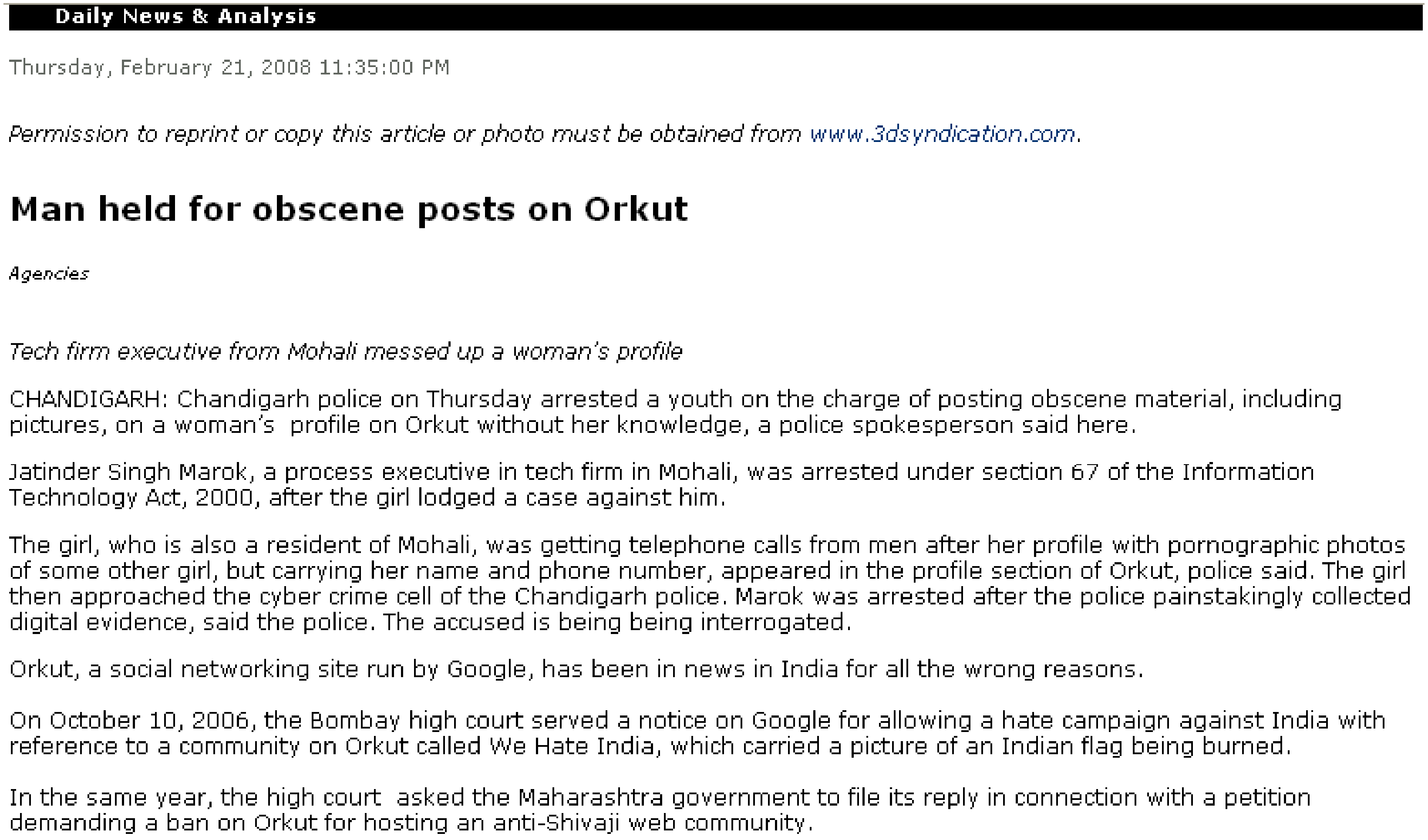
- They were not aware of social engineering tactics as well as the security requirements to protect their passwords.
- They were willing to assist in any way possible once we identified ourselves as the IT helpdesk.
- They were having network problems and the call seemed legitimate.
- Although they questioned the caller's identity and could not locate the caller's name, which was fictitious, on the IRS' global email address book, they changed their password anyway.
- They were hesitant, but their managers gave them approval to assist us.

Source http://www.treasury.gov/

Impersonating Orkut, Facebook, MySpace

EC-Council

News



Daily News & Analysis

Thursday, February 21, 2008 11:35:00 PM

Permission to reprint or copy this article or photo must be obtained from www.3dsyndication.com.

Man held for obscene posts on Orkut

Agencies

Tech firm executive from Mohali messed up a woman's profile

CHANDIGARH: Chandigarh police on Thursday arrested a youth on the charge of posting obscene material, including pictures, on a woman's profile on Orkut without her knowledge, a police spokesperson said here.

Jatinder Singh Marok, a process executive in tech firm in Mohali, was arrested under section 67 of the Information Technology Act, 2000, after the girl lodged a case against him.

The girl, who is also a resident of Mohali, was getting telephone calls from men after her profile with pornographic photos of some other girl, but carrying her name and phone number, appeared in the profile section of Orkut, police said. The girl then approached the cyber crime cell of the Chandigarh police. Marok was arrested after the police painstakingly collected digital evidence, said the police. The accused is being being interrogated.

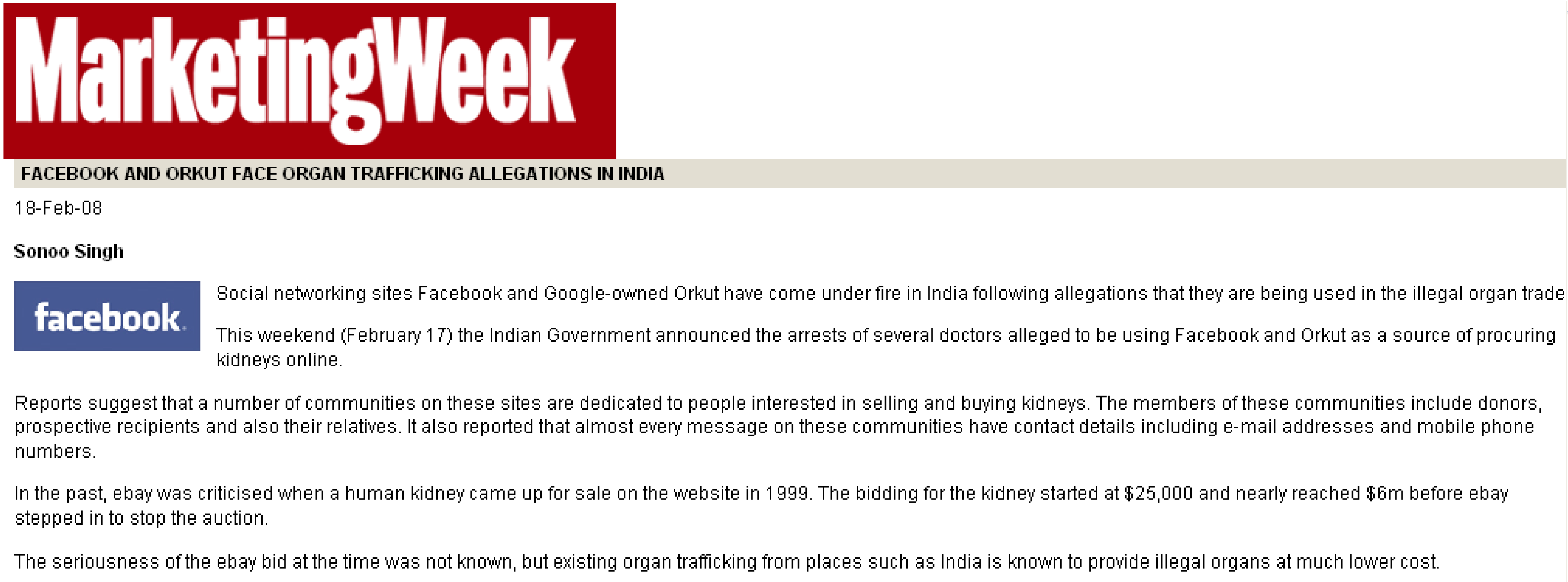
Orkut, a social networking site run by Google, has been in news in India for all the wrong reasons.

On October 10, 2006, the Bombay high court served a notice on Google for allowing a hate campaign against India with reference to a community on Orkut called We Hate India, which carried a picture of an Indian flag being burned.

In the same year, the high court asked the Maharashtra government to file its reply in connection with a petition demanding a ban on Orkut for hosting an anti-Shivaji web community.

Source: *http://www.dnaindia.com/*

News



MarketingWeek

FACEBOOK AND ORKUT FACE ORGAN TRAFFICKING ALLEGATIONS IN INDIA

18-Feb-08

Sonoo Singh

Social networking sites Facebook and Google-owned Orkut have come under fire in India following allegations that they are being used in the illegal organ trade

This weekend (February 17) the Indian Government announced the arrests of several doctors alleged to be using Facebook and Orkut as a source of procuring kidneys online.

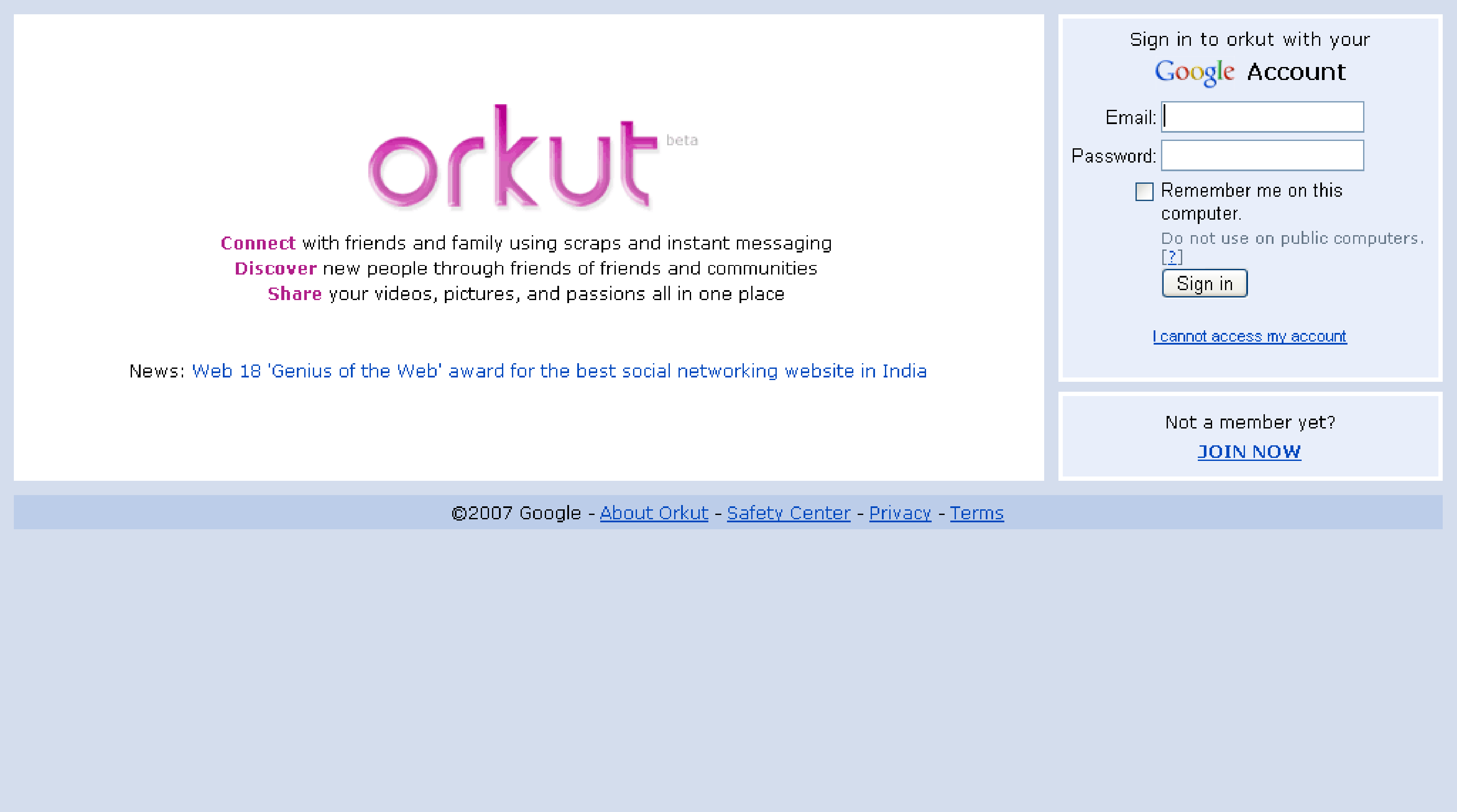
Reports suggest that a number of communities on these sites are dedicated to people interested in selling and buying kidneys. The members of these communities include donors, prospective recipients and also their relatives. It also reported that almost every message on these communities have contact details including e-mail addresses and mobile phone numbers.

In the past, ebay was criticised when a human kidney came up for sale on the website in 1999. The bidding for the kidney started at $25,000 and nearly reached $6m before ebay stepped in to stop the auction.

The seriousness of the ebay bid at the time was not known, but existing organ trafficking from places such as India is known to provide illegal organs at much lower cost.

Source: *http://www.marketingweek.co.uk/*

Orkut



Connect with friends and family using scraps and instant messaging
Discover new people through friends of friends and communities
Share your videos, pictures, and passions all in one place

News: Web 18 'Genius of the Web' award for the best social networking website in India

Sign in to orkut with your Google Account

Email:

Password:

□ Remember me on this computer.

Do not use on public computers. [?]

Not a member yet?

©2007 Google - About Orkut - Safety Center - Privacy - Terms

Impersonating on Orkut

Impersonation means imitates or copies the behavior or actions of others

Orkut is a famous social networking site, and as a open source anyone can steal the personal and corporate information and create the account on others' name

On Orkut, accounts can be hacked by 2 main methods: Cookie Stealing and Phishing (Fake Page)

Cookie Stealing involves a simple JavaScript which is backed up by a powerful PHP script in the back

When this script is run by the victim, his cookie comes to the hacker, using which he can get into the victim's account

Fake pages look like pages of Orkut; when user name and password is put into their respective fields, they are sent to the email ID of the hacker

MW.Orc worm

MW.Orc worm steals users' banking details, usernames, and passwords by propagating through Orkut

This attack is triggered as the user launches an executable file disguised as a JPEG file

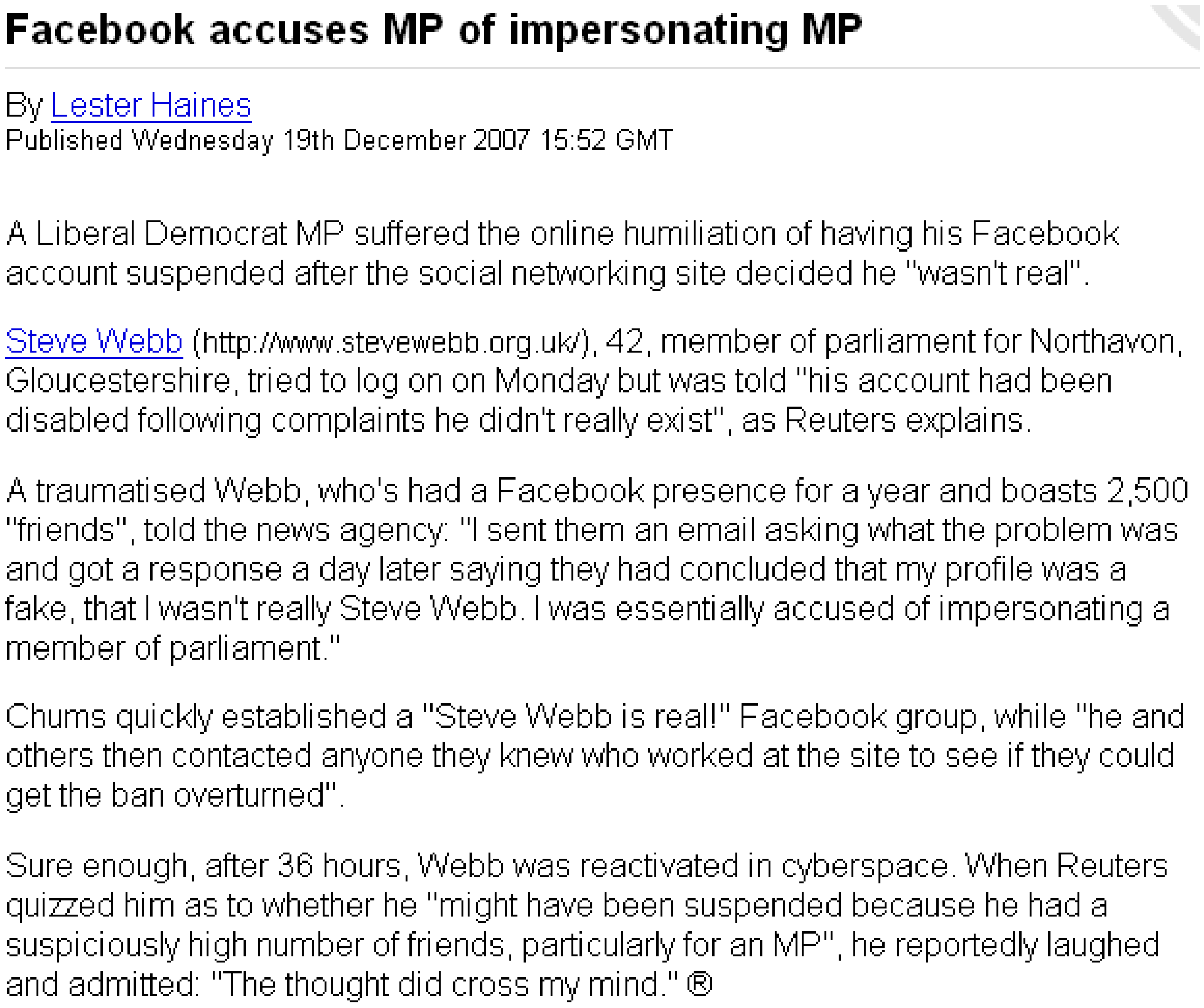
The initial executable file that causes the infection, installs two additional files on the user's computer

These files then pass e-mail banking details and passwords to the worm's anonymous creator when the infected users click on “My Computer” icon

Infection spreads automatically by posting a URL in another user's Orkut Scrapbook; a guestbook where visitors can leave comments visible on user's page

Apart from stealing personal information, this malware also enables a remote user to control PC and make it a part of botnet which is a network of infected PCs

News



Facebook accuses MP of impersonating MP

By Lester Haines
Published Wednesday 19th December 2007 15:52 GMT

A Liberal Democrat MP suffered the online humiliation of having his Facebook account suspended after the social networking site decided he "wasn't real".

Steve Webb (http://www.stevewebb.org.uk/), 42, member of parliament for Northavon, Gloucestershire, tried to log on on Monday but was told "his account had been disabled following complaints he didn't really exist", as Reuters explains.

A traumatised Webb, who's had a Facebook presence for a year and boasts 2,500 "friends", told the news agency: "I sent them an email asking what the problem was and got a response a day later saying they had concluded that my profile was a fake, that I wasn't really Steve Webb. I was essentially accused of impersonating a member of parliament."

Chums quickly established a "Steve Webb is real!" Facebook group, while "he and others then contacted anyone they knew who worked at the site to see if they could get the ban overturned".

Sure enough, after 36 hours, Webb was reactivated in cyberspace. When Reuters quizzed him as to whether he "might have been suspended because he had a suspiciously high number of friends, particularly for an MP", he reportedly laughed and admitted: "The thought did cross my mind." ®

Source: *http://www.theregister.co.uk/*

Techie jailed for playing prince on Facebook

Reuters

FACE THE TROUBLE: Fouad Mortada imitated Prince Moulay Rachid of Morocco without his consent.

Rabat: A Moroccan computer engineer appeared in court on Friday charged with setting up a Facebook account in the name of King Mohammed's brother.

Twenty-six-year-old Fouad Mortada could face jail on the charges of falsifying computer data and imitating Prince Moulay Rachid on the social networking site without his consent. Relatives said he was motivated by admiration for the 37-year-old prince, who is second in line to the throne.

Mortada said he was blindfolded and taken to an unknown building where he was beaten, spat on and insulted, according to a Website set up by his supporters (www.helpfouad.com).

"This is a nightmare," Mortada's uncle Mohamed El Yousfi told Reuters. "Fouad is threatened, as well as his job and his family. He had no evil intent to damage the royal family, which he respects. He has done nothing wrong." Newspapers quoted Mortada as telling the judicial police he had set up the Facebook account to give him a better chance of romantic encounters.

Defence lawyer Ali Ammar said that was untrue. "He said that to stop being tortured," Ammar said. "The police wanted to know if there was any relation between Fouad and terrorist groups seeking to harm the royal family but they found nothing of the kind."

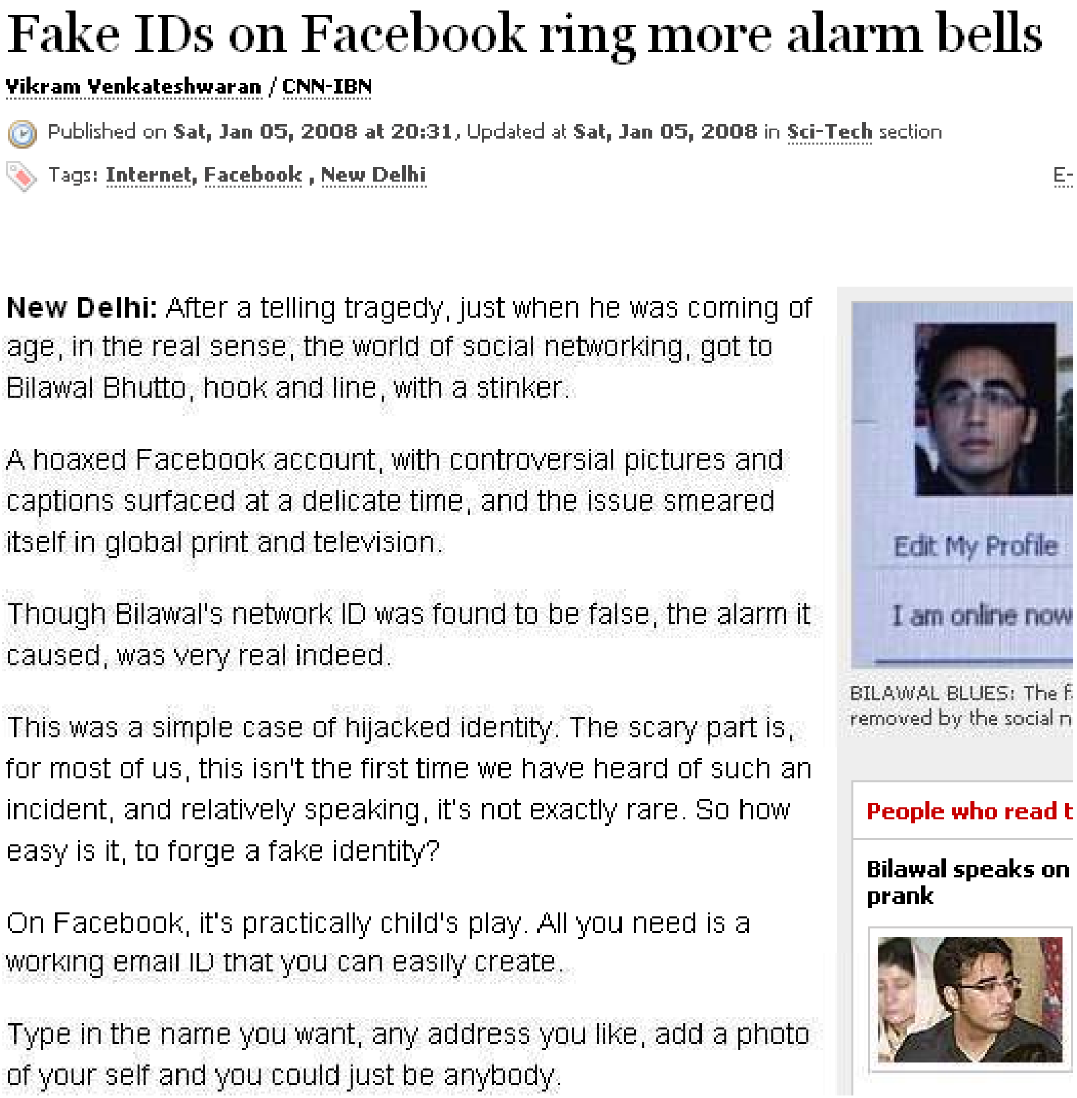
A source close to the security services told Reuters Mortada was arrested at the request of the judicial authorities and under their supervision. "Concerning the accusations of torture, the security services deny this. He was very cooperative," the source said.

Defence lawyer Ammar said he asked the judge to release Mortada during his trial, which is due to resume on Feb. 22. "Fouad is a computer technician," said his brother Ilyas. "If his intentions were bad, why would he use his own computer to set up the account knowing full well that someone could trace him back to his IP address?"

He said thousands of people had set up accounts on Facebook and other sites under the name of famous people they admired.

Source: *http://www.ibnlive.com/news/*

News



Fake IDs on Facebook ring more alarm bells

Vikram Venkateshwaran / CNN-IBN

Published on Sat, Jan 05, 2008 at 20:31, Updated at Sat, Jan 05, 2008 in Sci-Tech section

Tags: Internet, Facebook , New Delhi

E-

New Delhi: After a telling tragedy, just when he was coming of age, in the real sense, the world of social networking, got to Bilawal Bhutto, hook and line, with a stinker.

A hoaxed Facebook account, with controversial pictures and captions surfaced at a delicate time, and the issue smeared itself in global print and television.

Though Bilawal's network ID was found to be false, the alarm it caused, was very real indeed.

This was a simple case of hijacked identity. The scary part is, for most of us, this isn't the first time we have heard of such an incident, and relatively speaking, it's not exactly rare. So how easy is it, to forge a fake identity?

On Facebook, it's practically child's play. All you need is a working email ID that you can easily create.

Type in the name you want, any address you like, add a photo of your self and you could just be anybody.

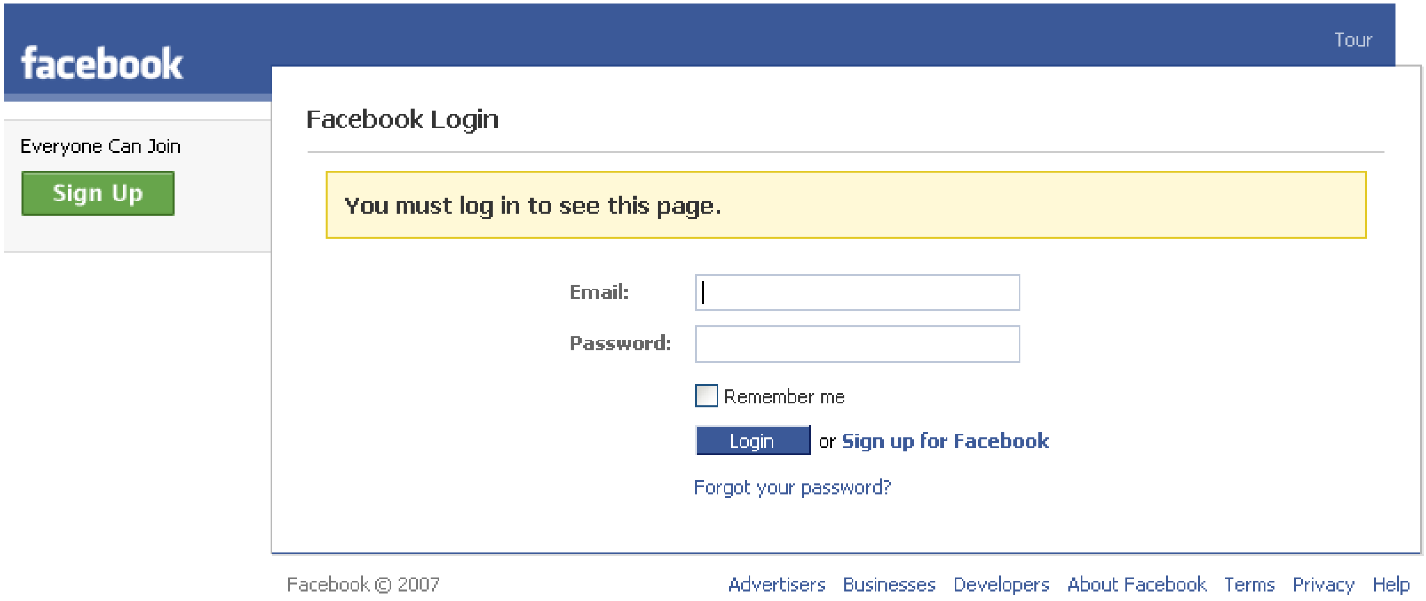
BILAWAL BLUES: The f
removed by the social n

People who read t

Bilawal speaks on prank

Source: *http://www.ibnlive.com/*

Facebook



facebook

Tour

Everyone Can Join

Sign Up

Facebook Login

You must log in to see this page.

Email:

Password:

□ Remember me

Login or **Sign up for Facebook**

Forgot your password?

Facebook © 2007

Advertisers Businesses Developers About Facebook Terms Privacy Help

Impersonating on Facebook

Facebook bloggers use a nickname instead of the real name

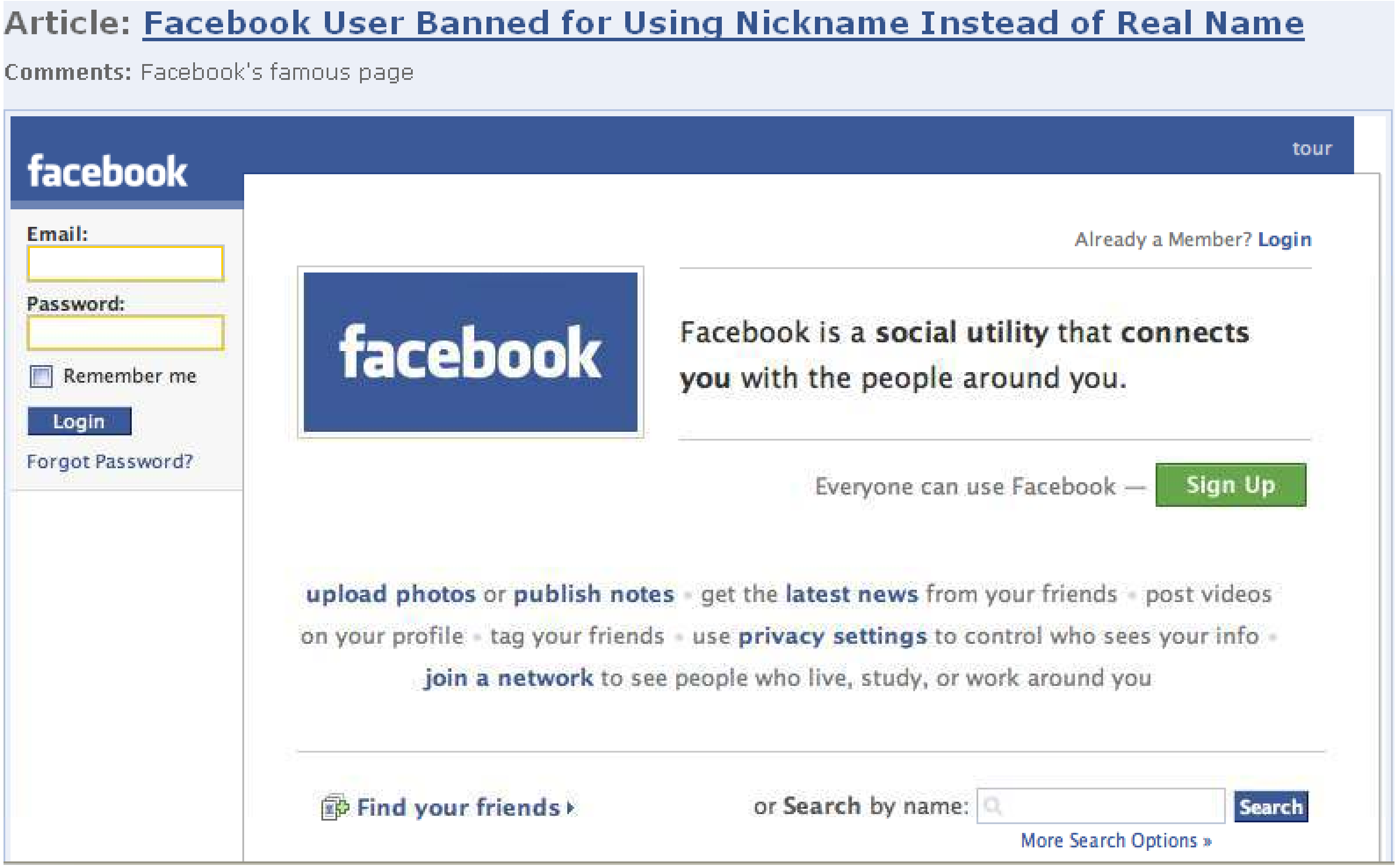
Fake accounts are a violation of Terms of Use

Facebook requires users to provide their real first and last names

The impostor keeps adding up friends

The impostor uses other's profile to get critical and valuable information

Screenshot



Article: Facebook User Banned for Using Nickname Instead of Real Name

Comments: Facebook's famous page

facebook

tour

Email:

Password:

□ Remember me

Login

Forgot Password?

Already a Member? **Login**

facebook

Facebook is a **social utility** that **connects you** with the people around you.

Everyone can use Facebook — **Sign Up**

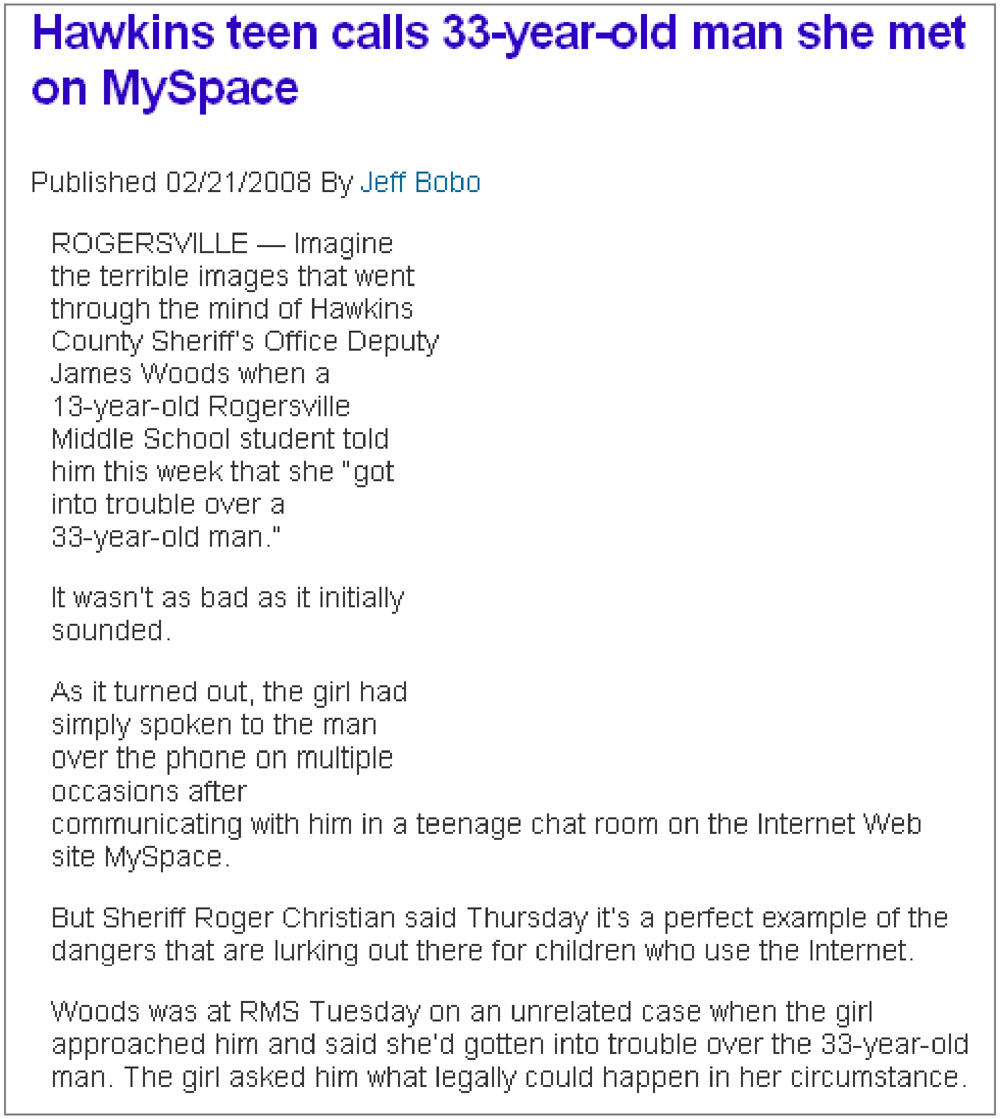
upload photos or **publish notes** · get the **latest news** from your friends · post videos on your profile · tag your friends · use **privacy settings** to control who sees your info · **join a network** to see people who live, study, or work around you

Find your friends ▸

or **Search** by name: **Search**

More Search Options »

News



Hawkins teen calls 33-year-old man she met on MySpace

Published 02/21/2008 By Jeff Bobo

ROGERSVILLE — Imagine the terrible images that went through the mind of Hawkins County Sheriff's Office Deputy James Woods when a 13-year-old Rogersville Middle School student told him this week that she "got into trouble over a 33-year-old man."

It wasn't as bad as it initially sounded.

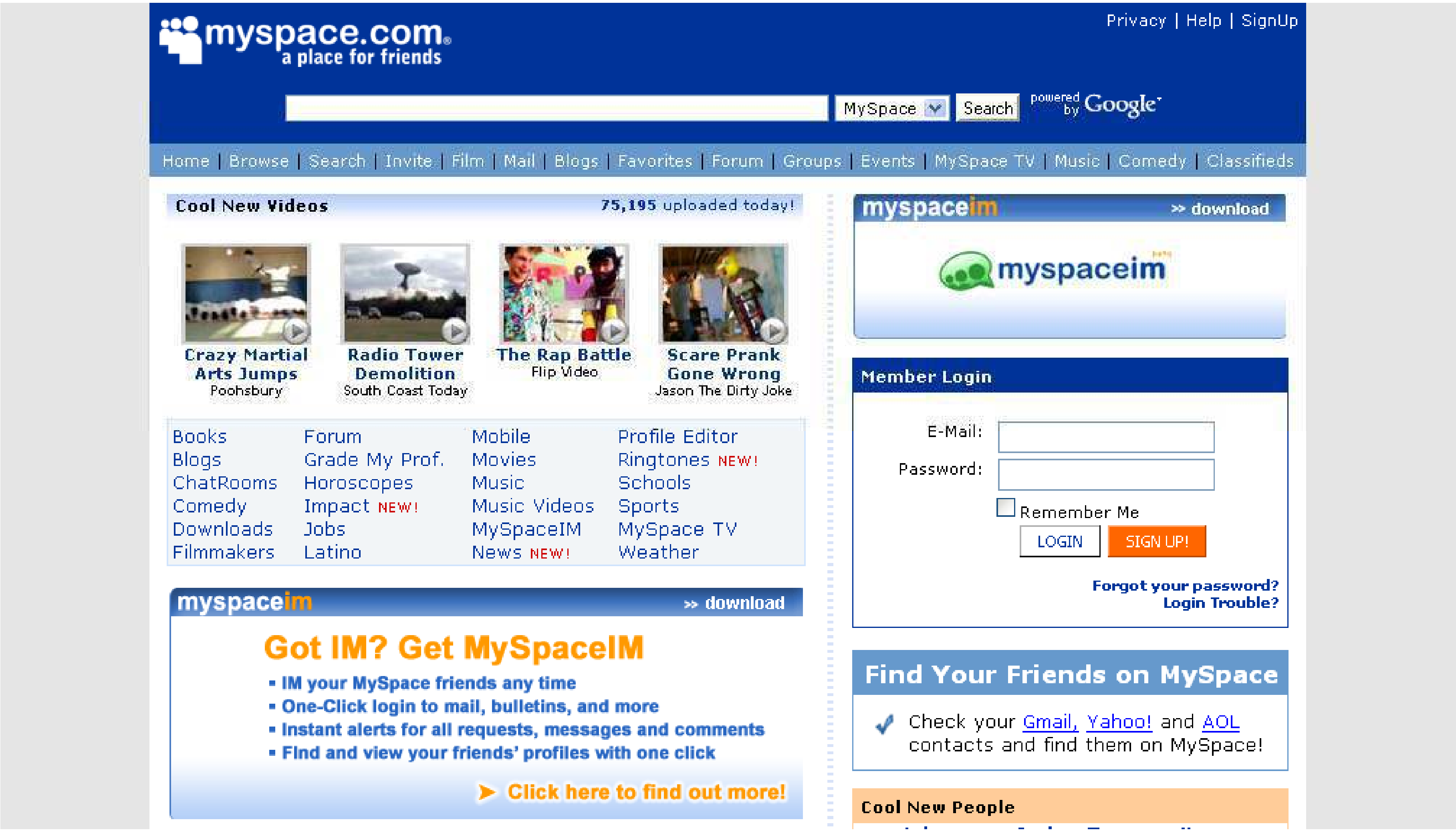
As it turned out, the girl had simply spoken to the man over the phone on multiple occasions after communicating with him in a teenage chat room on the Internet Web site MySpace.

But Sheriff Roger Christian said Thursday it's a perfect example of the dangers that are lurking out there for children who use the Internet.

Woods was at RMS Tuesday on an unrelated case when the girl approached him and said she'd gotten into trouble over the 33-year-old man. The girl asked him what legally could happen in her circumstance.

Source: *http://www.timesnews.net/*

MySpace


myspace.com a place for friends
Privacy | Help | SignUp
MySpace
Search
powered by Google
Home | Browse | Search | Invite | Film | Mail | Blogs | Favorites | Forum | Groups | Events | MySpace TV | Music | Comedy | Classifieds
myspaceim
» download
myspaceim
LOGIN
SIGN UP!

Cool New Videos 75,195 uploaded today!

Crazy Martial Arts Jumps Poohsbury	**Radio Tower Demolition** South Coast Today	**The Rap Battle** Flip Video	**Scare Prank Gone Wrong** Jason The Dirty Joke

Books
Blogs
ChatRooms
Comedy
Downloads
Filmmakers

Forum
Grade My Prof.
Horoscopes
Impact NEW!
Jobs
Latino

Mobile
Movies
Music
Music Videos
MySpaceIM
News NEW!

Profile Editor
Ringtones NEW!
Schools
Sports
MySpace TV
Weather

Got IM? Get MySpaceIM

- IM your MySpace friends any time
- One-Click login to mail, bulletins, and more
- Instant alerts for all requests, messages and comments
- Find and view your friends' profiles with one click

➤ Click here to find out more!

Member Login

E-Mail:

Password:

□ Remember Me

Forgot your password?
Login Trouble?

Find Your Friends on MySpace

✓ Check your Gmail, Yahoo! and AOL contacts and find them on MySpace!

Cool New People

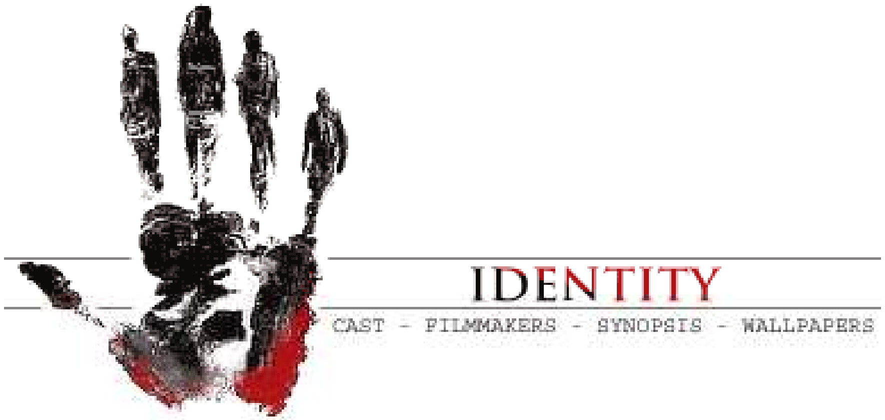
Impersonating on MySpace

MySpace has become an effective marketing tool

Various people have their profiles on MySpace to gain exposure

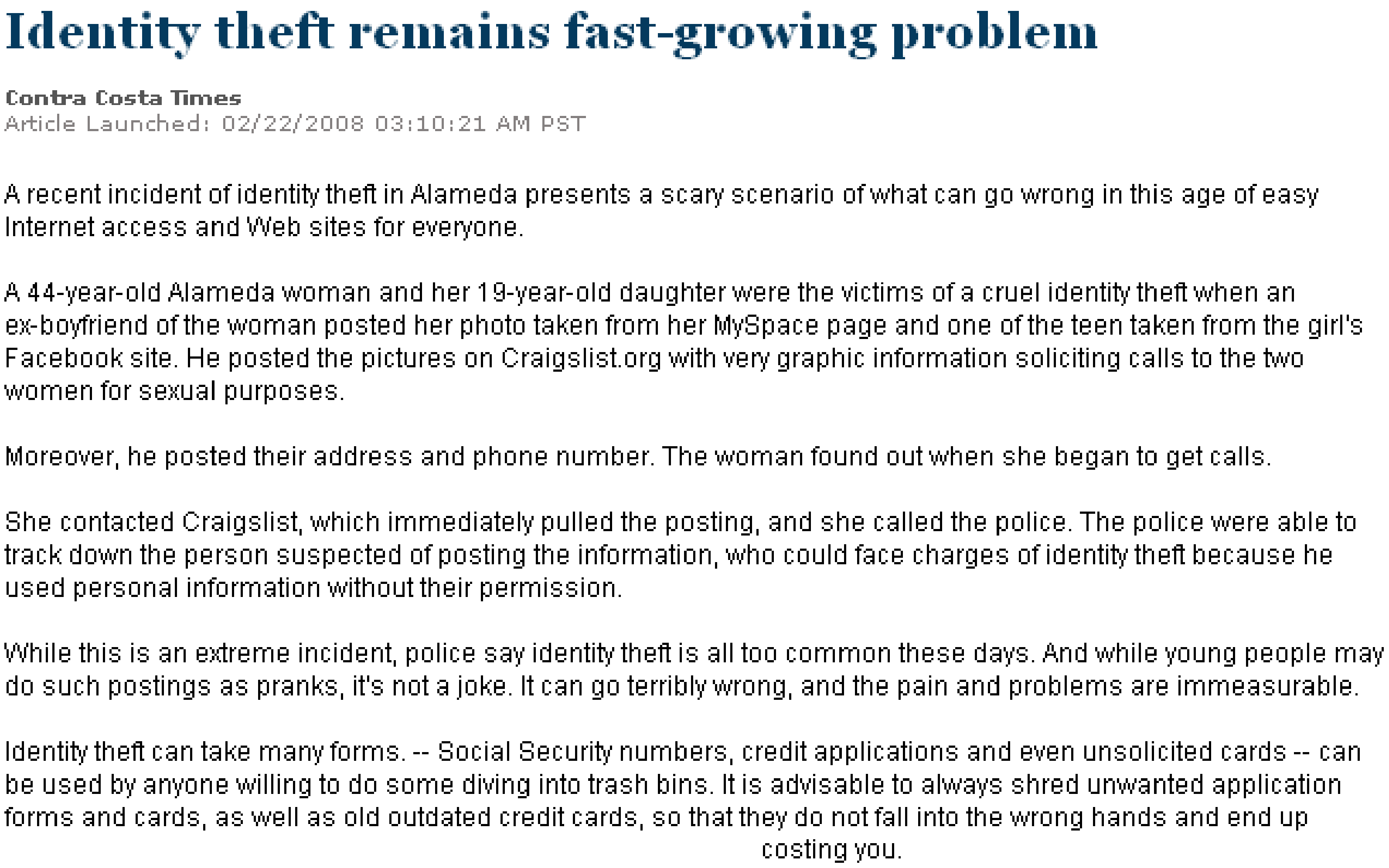
All MySpace profiles are not genuine and real

Adults impersonate as teen on MySpace which leads to tragedy



Identity Theft

News



Identity theft remains fast-growing problem

Contra Costa Times
Article Launched: 02/22/2008 03:10:21 AM PST

A recent incident of identity theft in Alameda presents a scary scenario of what can go wrong in this age of easy Internet access and Web sites for everyone.

A 44-year-old Alameda woman and her 19-year-old daughter were the victims of a cruel identity theft when an ex-boyfriend of the woman posted her photo taken from her MySpace page and one of the teen taken from the girl's Facebook site. He posted the pictures on Craigslist.org with very graphic information soliciting calls to the two women for sexual purposes.

Moreover, he posted their address and phone number. The woman found out when she began to get calls.

She contacted Craigslist, which immediately pulled the posting, and she called the police. The police were able to track down the person suspected of posting the information, who could face charges of identity theft because he used personal information without their permission.

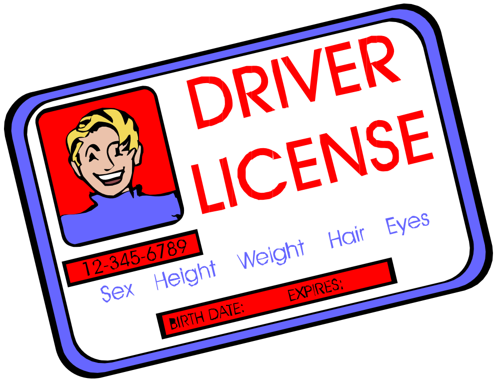
While this is an extreme incident, police say identity theft is all too common these days. And while young people may do such postings as pranks, it's not a joke. It can go terribly wrong, and the pain and problems are immeasurable.

Identity theft can take many forms. -- Social Security numbers, credit applications and even unsolicited cards -- can be used by anyone willing to do some diving into trash bins. It is advisable to always shred unwanted application forms and cards, as well as old outdated credit cards, so that they do not fall into the wrong hands and end up costing you.

Source: *http://www.mercurynews.com/*

What is “Identity Theft”

Identity theft occurs when someone steals your name and other personal information for fraudulent purposes



Identity Theft

© 1999 Randy Glasbergen.
www.glasbergen.com

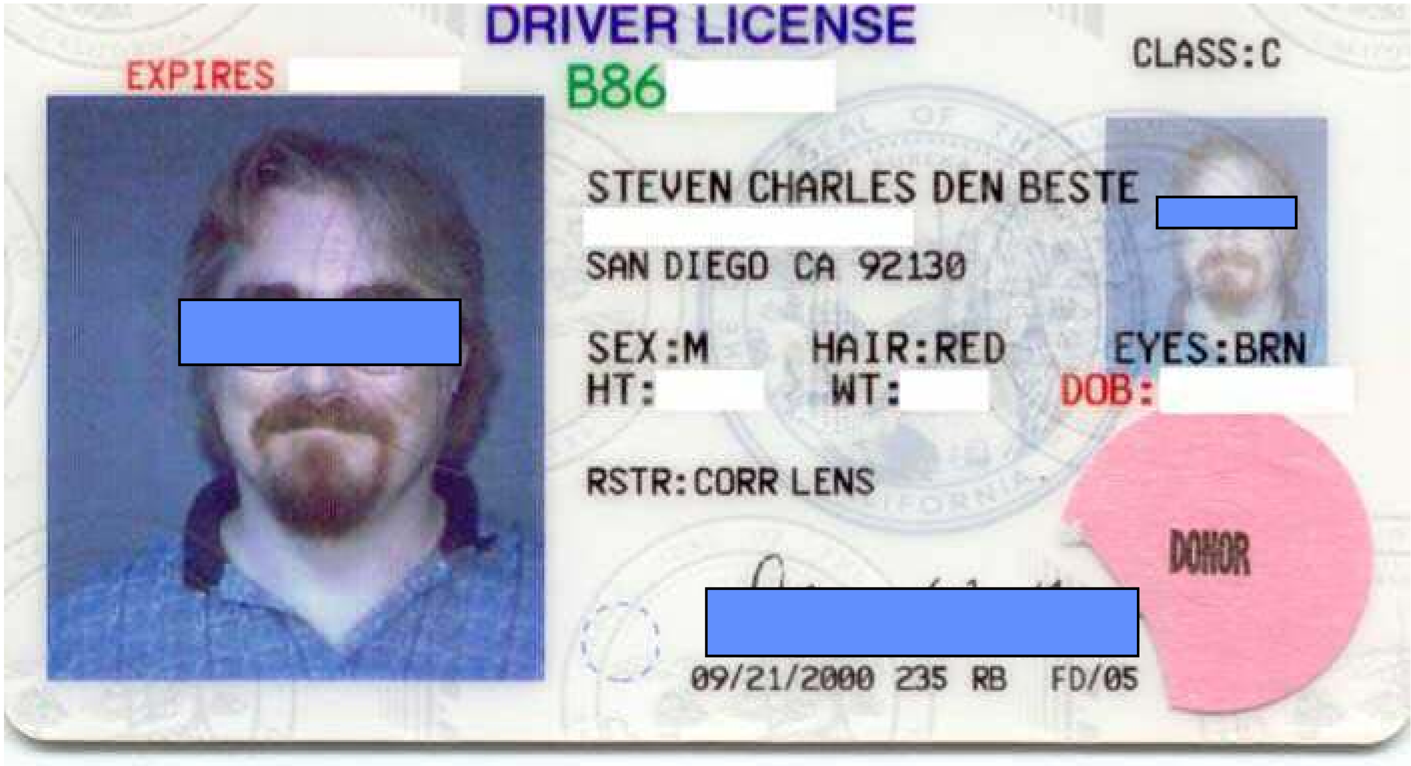
"You'll give your credit card to a waitress with sixteen earrings and an obscene tattoo, but you won't give it to a reputable company with a web site?"

How do you steal Identity?

How to Steal Identity

Original identity – Steven Charles

Address: San Diego CA 92130



DRIVER LICENSE

EXPIRES [redacted]

B86[redacted]

CLASS:C

STEVEN CHARLES DEN BESTE [redacted]

[redacted]

SAN DIEGO CA 92130

SEX:M HAIR:RED EYES:BRN

HT:[redacted] WT:[redacted] DOB:[redacted]

RSTR:CORR LENS

DONOR

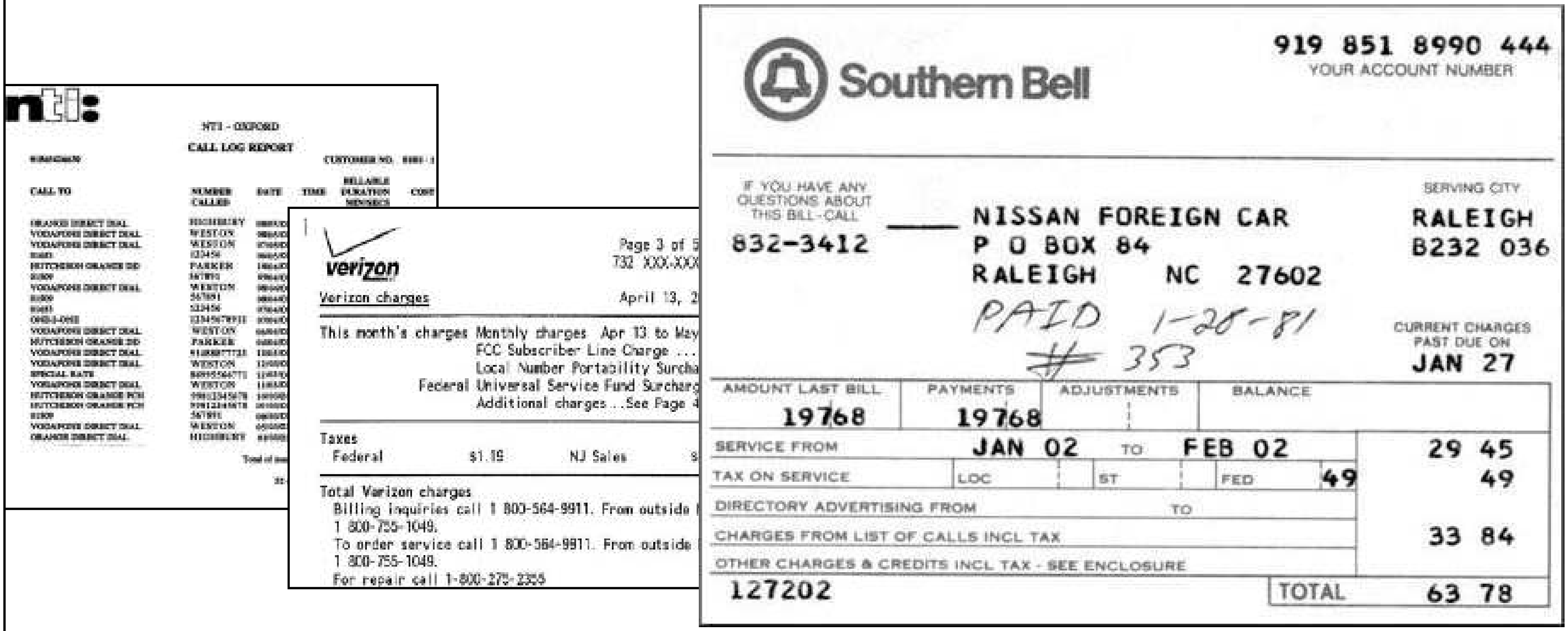
[redacted]

09/21/2000 235 RB FD/05

EC-Council

STEP 1

Get hold of Steven’s telephone bill, water bill, or electricity bill using dumpster diving, stolen email, or onsite stealing



ntl:

NTL - OXFORD

CALL LOG REPORT

[illegible] CUSTOMER NO. [illegible]

CALL TO	NUMBER CALLED	DATE	TIME	BILLABLE DURATION MINUTES	COST
ORANGE DIRECT DIAL	HIGHBURY	[illegible]			
VODAFONE DIRECT DIAL	WESTON	[illegible]			
VODAFONE DIRECT DIAL	WESTON	[illegible]			
01865	123456	[illegible]			
HUTCHISON ORANGE DD	PARKER	[illegible]			
01509	567891	[illegible]			
VODAFONE DIRECT DIAL	WESTON	[illegible]			
01509	567891	[illegible]			
01865	123456	[illegible]			
[illegible]	123456789[illegible]	[illegible]			
VODAFONE DIRECT DIAL	WESTON	[illegible]			
HUTCHISON ORANGE DD	PARKER	[illegible]			
VODAFONE DIRECT DIAL	[illegible]	[illegible]			
VODAFONE DIRECT DIAL	WESTON	[illegible]			
SPECIAL RATE	[illegible]	[illegible]			
VODAFONE DIRECT DIAL	WESTON	[illegible]			
HUTCHISON ORANGE PCH	[illegible]	[illegible]			
HUTCHISON ORANGE PCH	[illegible]	[illegible]			
01509	567891	[illegible]			
VODAFONE DIRECT DIAL	WESTON	[illegible]			
ORANGE DIRECT DIAL	HIGHBURY	[illegible]			

Total of [illegible]

verizon

Page 3 of 5
732 XXX-XXX

Verizon charges

April 13, 2

This month's charges Monthly charges Apr 13 to May
FCC Subscriber Line Charge ....
Local Number Portability Surcha
Federal Universal Service Fund Surcharg
Additional charges ...See Page 4

Taxes
Federal $1.19 NJ Sales $

Total Verizon charges
Billing inquiries call 1 800-564-9911. From outside
1 800-755-1049.
To order service call 1 800-564-9911. From outside
1 800-755-1049.
For repair call 1-800-275-2355

Southern Bell

919 851 8990 444
YOUR ACCOUNT NUMBER

IF YOU HAVE ANY QUESTIONS ABOUT THIS BILL - CALL
832-3412

NISSAN FOREIGN CAR
P O BOX 84
RALEIGH NC 27602

SERVING CITY
RALEIGH
B232 036

PAID 1-28-81
353

CURRENT CHARGES PAST DUE ON
JAN 27

AMOUNT LAST BILL	PAYMENTS	ADJUSTMENTS	BALANCE
19768	19768		

SERVICE FROM	JAN 02	TO FEB 02	29 45
TAX ON SERVICE	LOC ST FED	49	49
DIRECTORY ADVERTISING FROM		TO	
CHARGES FROM LIST OF CALLS INCL TAX			33 84
OTHER CHARGES & CREDITS INCL TAX - SEE ENCLOSURE			
127202		TOTAL	63 78

STEP 2

Go to the Driving License Authority

Tell them you lost your driver's license

They will ask you for proof of identity like a water bill,and electricity bill

Show them the stolen bills

Tell them you have moved from the original address

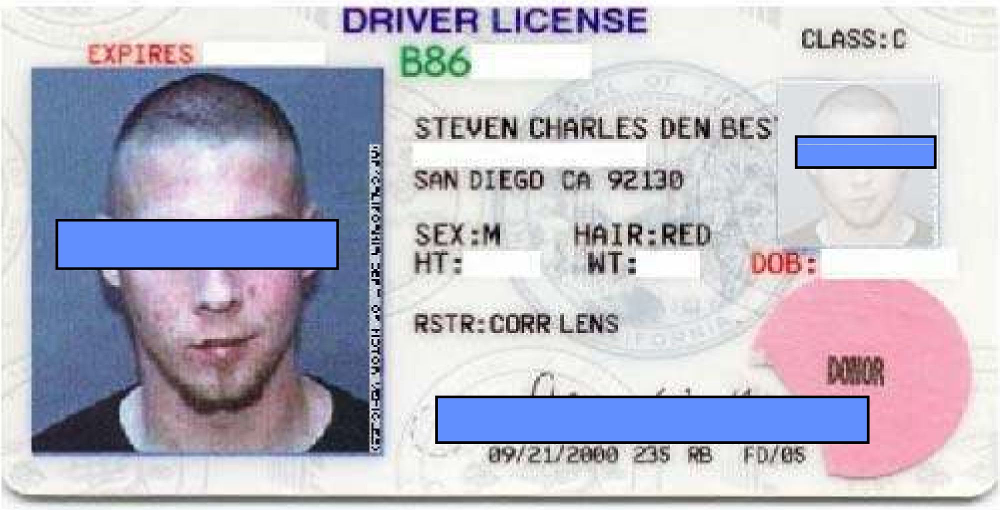
The department employee will ask you to complete 2 forms – 1 for the replacement of the driver's license and the 2nd for a change in address

You will need a photo for the driver's license

STEP 3

Your replacement driver's license will be issued to your new home address

Now you are ready to have some serious fun



DRIVER LICENSE

EXPIRES

B86

CLASS:C

[redacted]

STEVEN CHARLES DEN BES

[redacted]

SAN DIEGO CA 92130

SEX:M HAIR:RED

HT: WT: DOB:

RSTR:CORR LENS

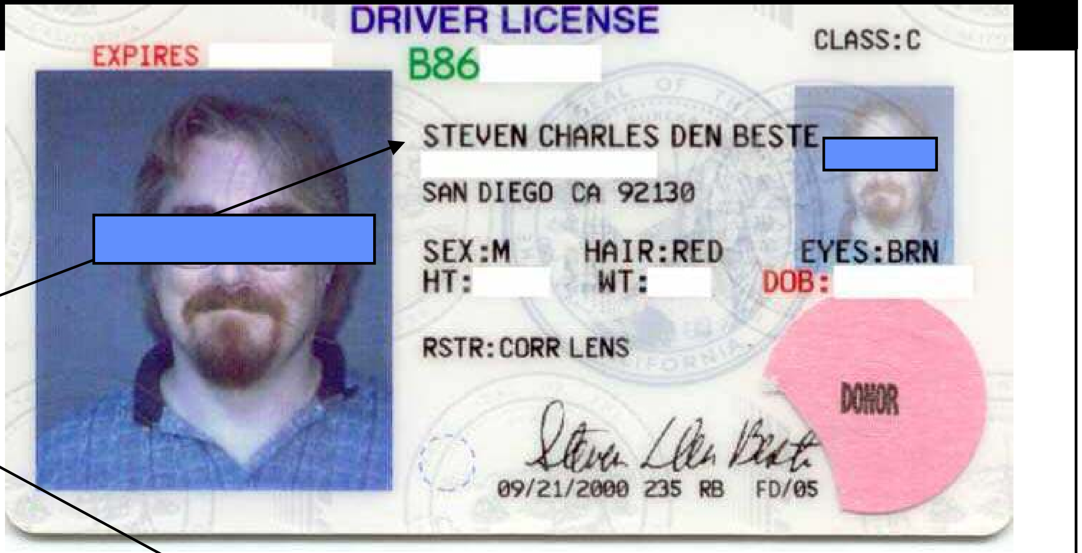
DONOR

[redacted]

09/21/2000 235 RB FD/05

Comparison

- Original



DRIVER LICENSE

EXPIRES

B86

CLASS:C

[redacted]

STEVEN CHARLES DEN BESTE [redacted]

SAN DIEGO CA 92130

SEX:M HAIR:RED EYES:BRN

HT: WT: DOB:

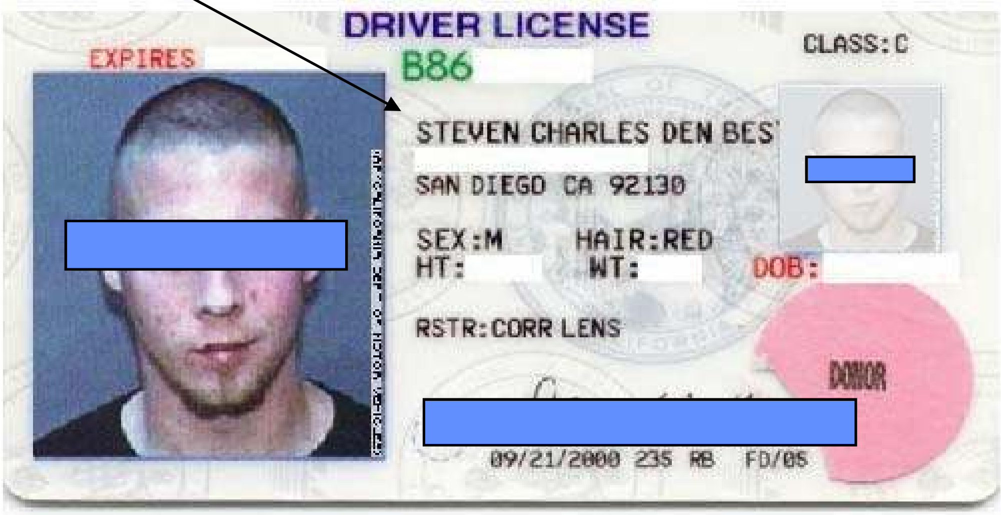
RSTR:CORR LENS

DONOR

09/21/2000 235 RB FD/05

Same name: Steven Charles

- Identity Theft



DRIVER LICENSE

EXPIRES

B86

CLASS:C

[redacted]

STEVEN CHARLES DEN BES

[redacted]

SAN DIEGO CA 92130

SEX:M HAIR:RED

HT: WT: DOB:

RSTR:CORR LENS

DONOR

[redacted]

09/21/2000 235 RB FD/05

STEP 4

Go to a bank in which the original Steven Charles has an account (Example Citibank)

Tell them you would like to apply for a new credit card

Tell them you do not remember the account number and ask them to look it up using Steven's name and address

The bank will ask for your ID: Show them your driver's license as ID

ID is accepted. Your credit card is issued and ready for use

Now you are ready for shopping

Fake Steven has a New Credit Card

The fake Steven visits Wal-Mart and purchases a 42" plasma TV and state-of-the-art Bose speakers

The fake Steven buys a Vertu Gold Phone worth USD 20K

International Citizen
Preffered
2423 5435 4543 56765
02/03 01/06 V
Stevens Charles
MasterCard

C|EH™ Certified Ethical Hacker

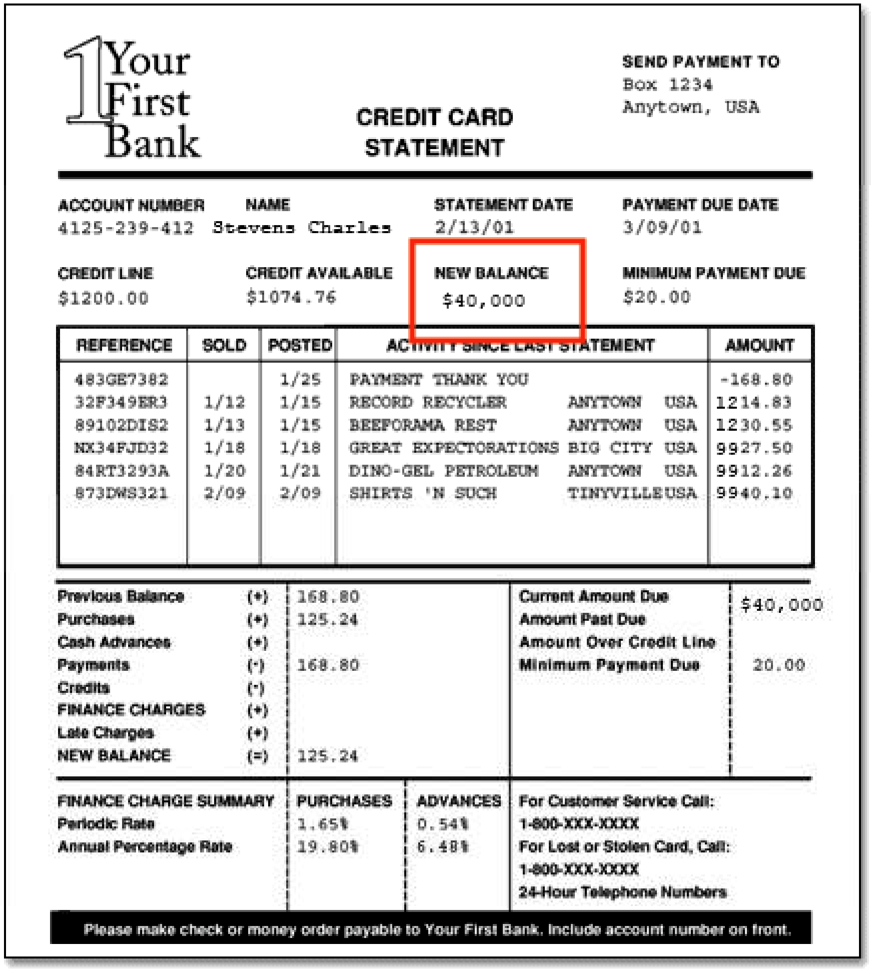
Fake Steven Buys Car

The fake Steven walks into a store and applies for a car loan; minutes later he is driving a new Audi

Present your driver's license as a form of ID

The loan officer does the credit check, and it comes out clean since the original Steven has a clean credit history

Real Steven Gets Huge Credit Card Statement – USD 40k



Your First Bank

CREDIT CARD STATEMENT

SEND PAYMENT TO
Box 1234
Anytown, USA

ACCOUNT NUMBER	NAME	STATEMENT DATE	PAYMENT DUE DATE
4125-239-412	Stevens Charles	2/13/01	3/09/01
CREDIT LINE	CREDIT AVAILABLE	NEW BALANCE	MINIMUM PAYMENT DUE
$1200.00	$1074.76	$40,000	$20.00

REFERENCE	SOLD	POSTED	ACTIVITY SINCE LAST STATEMENT	AMOUNT
483GE7382		1/25	PAYMENT THANK YOU	-168.80
32F349ER3	1/12	1/15	RECORD RECYCLER ANYTOWN USA	1214.83
89102DIS2	1/13	1/15	BEEFORAMA REST ANYTOWN USA	1230.55
NX34FJD32	1/18	1/18	GREAT EXPECTORATIONS BIG CITY USA	9927.50
84RT3293A	1/20	1/21	DINO-GEL PETROLEUM ANYTOWN USA	9912.26
873DWS321	2/09	2/09	SHIRTS 'N SUCH TINYVILLEUSA	9940.10

Previous Balance	(+)	168.80	Current Amount Due	$40,000
Purchases	(+)	125.24	Amount Past Due	
Cash Advances	(+)		Amount Over Credit Line	
Payments	(-)	168.80	Minimum Payment Due	20.00
Credits	(-)			
FINANCE CHARGES	(+)			
Late Charges	(+)			
NEW BALANCE	(=)	125.24		

FINANCE CHARGE SUMMARY	PURCHASES	ADVANCES
Periodic Rate	1.65%	0.54%
Annual Percentage Rate	19.80%	6.48%

For Customer Service Call:
1-800-XXX-XXXX
For Lost or Stolen Card, Call:
1-800-XXX-XXXX
24-Hour Telephone Numbers

Please make check or money order payable to Your First Bank. Include account number on front.

Ahhh!!! Somebody stole my identity!!

What Else…Oh My God!

Fake Steven can apply for a new passport

Fake Steven can apply for a new bank account

Fake Steven can shut down your utility services

FAKE STEVEN CAN MAKE THE LIFE OF REAL STEVEN HELL

Scary eh?

“One bit of personal information is all someone needs to steal your identity”

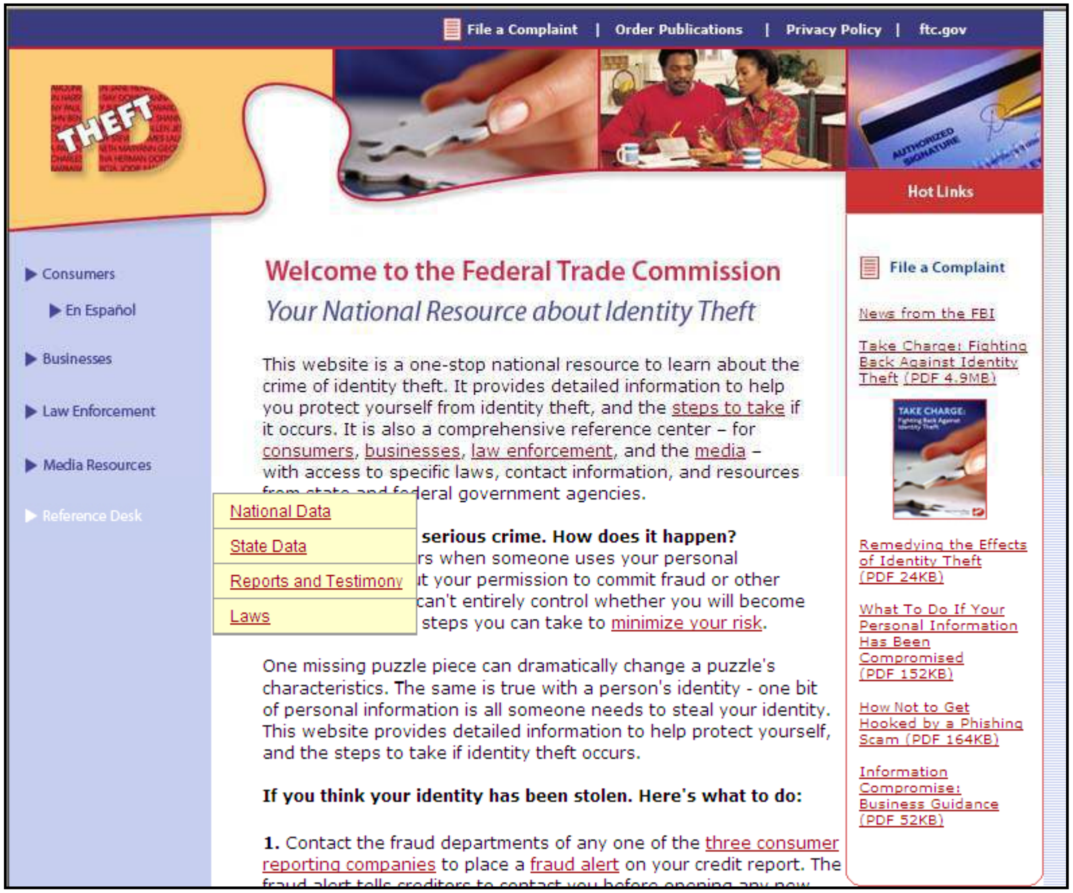
Identity Theft - Serious Problem

Identity theft is a serious problem

The number of violations has continued to increase

Securing personal information in the workplace and at home, and looking over credit card reports are just few of the ways to minimize the risk of the identity theft

http://www.consumer.gov/idtheft/



Welcome to the Federal Trade Commission

Your National Resource about Identity Theft

This website is a one-stop national resource to learn about the crime of identity theft. It provides detailed information to help you protect yourself from identity theft, and the steps to take if it occurs. It is also a comprehensive reference center – for consumers, businesses, law enforcement, and the media – with access to specific laws, contact information, and resources from state and federal government agencies.

serious crime. How does it happen?
rs when someone uses your personal
ut your permission to commit fraud or other
can't entirely control whether you will become
steps you can take to minimize your risk.

One missing puzzle piece can dramatically change a puzzle's characteristics. The same is true with a person's identity - one bit of personal information is all someone needs to steal your identity. This website provides detailed information to help protect yourself, and the steps to take if identity theft occurs.

If you think your identity has been stolen. Here's what to do:

1. Contact the fraud departments of any one of the three consumer reporting companies to place a fraud alert on your credit report. The fraud alert tells creditors to contact you before opening any new

News from the FBI

Take Charge: Fighting Back Against Identity Theft (PDF 4.9MB)

Remedying the Effects of Identity Theft (PDF 24KB)

What To Do If Your Personal Information Has Been Compromised (PDF 152KB)

How Not to Get Hooked by a Phishing Scam (PDF 164KB)

Information Compromise: Business Guidance (PDF 52KB)

Summary

Social Engineering is the human-side of breaking into a corporate network

Social Engineering involves acquiring sensitive information or inappropriate access privileges by an outsider

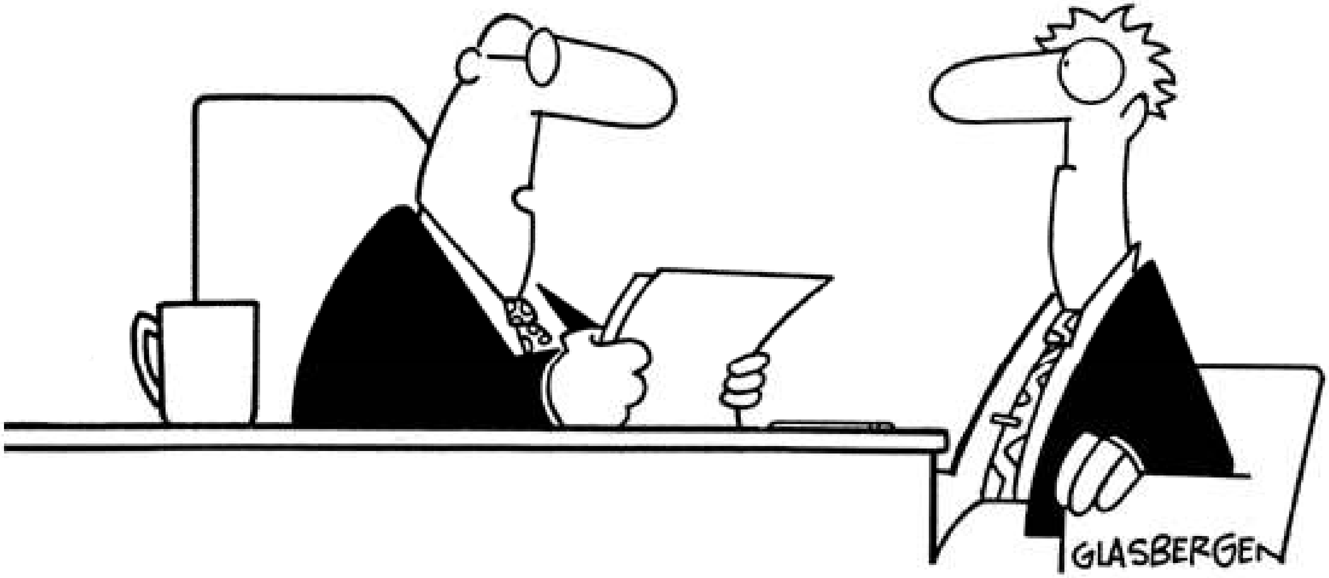
Human-based social engineering refers to person-to-person interaction to retrieve the desired information

Computer-based social engineering refers to having computer software that attempts to retrieve the desired information

A successful defense depends on having good policies and their diligent implementation

“If you were concerned about identity theft, you shouldn’t have left your private information lying around where I could find it!”

Copyright 2003 by Randy Glasbergen.
www.glasbergen.com



"We're looking for someone who can help us crack down on identity theft. Fill out this application and don't forget to include your Social Security number, date of birth, phone number, home address and mother's maiden name."