



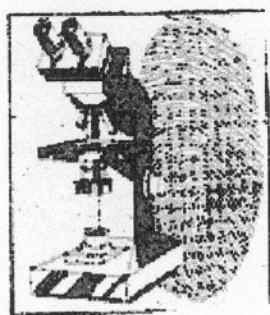
**Audit of Fraud
Fraud Detection Techniques
& Forensic Audit**

**Case Studies
on
Cyber Crimes**

Indian Audit & Accounts Department
Regional Training Institute
26/1, Civil Lines, Nagpur
E-mail : rtiaadnr_ngp@sancharnet.in
Phone : (0712) - 2545420, 2545816, 2545829
Fax : 0712-2562577

CONTENTS

Sr. No	Topic	Page Nos.
1.	How cyber crime operations work – and why they make money	1 - 3
2.	Tricks on evading scams	4
3.	Cyber crimes – some case studies	5 - 24
4.	Cyber crimes – case studies - Presentations by NetWork Security Solutions (I) Ltd.	25 - 40



HOW CYBER CRIME
OPERATIONS WORK

&

WHY THEY MAKE
MONEY

1. How cybercrime operations work – and why they make money

Hackers are no longer motivated by notoriety – it's now all about the money. Guillaume Lovet, Threat Response Team Leader at security firm Fortinet, identifies the players, their roles and the returns they enjoy on their investments.

Cyber crime has become a profession and the demographic of your typical cyber criminal is changing rapidly, from bedroom-bound geek to the type of organised gangster more traditionally associated with drug-trafficking, extortion and money laundering.

It has become possible for people with comparatively low technical skills to steal thousands of pounds a day without leaving their homes. In fact, to make more money than can be made selling heroin (and with far less risk), the only time the criminal need leave his PC is to collect his cash. Sometimes they don't even need to do that. In all industries, efficient business models depend upon horizontal separation of production processes, professional services, sales channels etc. (each requiring specialized skills and resources), as well as a good deal of trade at prices set by the market forces of supply and demand. Cyber crime is no different: it boasts a buoyant international market for skills, tools and finished product. It even has its own currency.

The rise of Cyber crime is inextricably linked to the ubiquity of credit card transactions and online bank accounts. Get hold of this financial data and not only can you steal silently, but also – through a process of virus-driven automation – with ruthlessly efficient and hypothetically infinite frequency.

The question of how to obtain credit card/bank account data can be answered by a selection of methods each involving their own relative combinations of risk, expense and skill.

The most straightforward is to buy the 'finished product'. In this case we'll use the example of an online bank account. The product takes the form of information necessary to gain authorised control over a bank account with a six-figure balance. The cost to obtain this information is \$400 (cyber criminals always deal in dollars). It seems like a small figure, but for the work involved and the risk incurred it's very easy money for the criminal who can provide it. Also remember that this is an international trade; many cyber-criminals of this ilk are from poor countries in Eastern Europe, South America or South-East Asia.

The probable marketplace for this transaction will be a hidden IRC (Internet Relay Chat) chat room. The \$400 fee will most likely be exchanged in some form of virtual currency such as e-gold. Not all cyber-criminals operate at the coalface, and certainly don't work exclusively of one another; different protagonists in the crime community perform a range of important, specialised functions. These broadly encompass: Coders – comparative veterans of the hacking community. With a few years' experience at the art and a list of established contacts, 'coders' produce ready-to-use tools (i.e. Trojans, mailers, custom bots) or services (such as making a binary code undetectable to AV engines) to the cybercrime labour force – the 'kids'. Coders can make a few hundred

dollars for every criminal activity they engage in. Kids – so-called because of their tender age: most are under 18. They buy, trade and resell the elementary building blocks of effective cyber-scams such as spam lists, php mailers, proxies, credit card numbers, hacked hosts, scam pages etc. 'Kids' will make less than \$100 a month, largely because of the frequency of being 'ripped off' by one another. Drops – the individuals who convert the 'virtual money' obtained in cybercrime into real cash. Usually located in countries with lax e-crime laws (Bolivia, Indonesia and Malaysia are currently very popular), they represent 'safe' addresses for goods purchased with stolen financial details to be sent, or else 'safe' legitimate bank accounts for money to be transferred into illegally, and paid out of legitimately. Mobs – professionally operating criminal organisations combining or utilising all of the functions covered by the above. Organised crime makes particularly good use of safe 'drops', as well as recruiting accomplished 'coders' onto their payrolls.

Gaining control of a bank account is increasingly accomplished through phishing. There are other cybercrime techniques, but space does not allow their full explanation.

All of the following phishing tools can be acquired very cheaply: a scam letter and scam page in your chosen language, a fresh spam list, a selection of php mailers to spam-out 100,000 mails for six hours, a hacked website for hosting the scam page for a few days, and finally a stolen but valid credit card with which to register a domain name. With all this taken care of, the total costs for sending out 100,000 phishing emails can be as little as \$60. This kind of 'phishing trip' will uncover at least 20 bank accounts of varying cash balances, giving a 'market value' of \$200 – \$2,000 in e-gold if the details were simply sold to another cybercriminal. The worst-case scenario is a 300% return on the investment, but it could be ten times that. Better returns can be accomplished by using 'drops' to cash the money. The risks are high, though: drops may take as much as 50% of the value of the account as commission, and instances of 'ripping off' or 'grassing up' to the police are not uncommon. Cautious phishers often separate themselves from the physical cashing of their spoils via a series of 'drops' that do not know one another. However, even taking into account the 50% commission, and a 50% 'rip-off' rate, if we assume a single stolen balance of \$10,000 – \$100,000, then the phisher is still looking at a return of between 40 and 400 times the meagre outlay of his/her phishing trip.

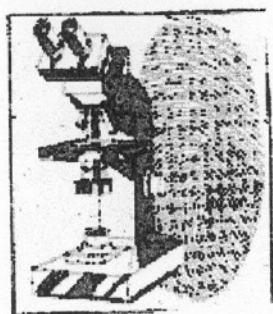
In large operations, offshore accounts are invariably used to accumulate the criminal spoils. This is more complicated and far more expensive, but ultimately safer.

The alarming efficiency of cybercrime can be illustrated starkly by comparing it to the illegal narcotics business. One is faster, less detectable, more profitable (generating a return around 400 times higher than the outlay) and primarily non-violent. The other takes months or years to set-up or realise an investment, is cracked down upon by all almost all governments internationally, fraught with expensive overheads, and extremely dangerous. Add phishing to the other cyber-criminal activities driven by hacking and virus technologies – such as carding, adware/spyware planting, online extortion, industrial spying and mobile phone dialers – and you'll find a healthy community of cottage industries and international organisations working together productively and

trading for impressive profits. Of course these people are threatening businesses and individuals with devastating loss, financial hardship and troubling uncertainty – and must be stopped.

On top of viruses, worms, bots and Trojan attacks, organisations in particular are contending with social engineering deception and traffic masquerading as legitimate applications on the network. In a reactive approach to this onslaught, companies have been layering their networks with stand alone firewalls, intrusion prevention devices, anti-virus and anti-spyware solutions in a desperate attempt to plug holes in the armoury. They're beginning to recognise it's a failed strategy. After all, billions of pounds are being spent on security technology, and yet security breaches continue to rise.

To fight cybercrime there needs to be a tightening of international digital legislation and of cross-border law enforcement co-ordination. But there also needs to be a more creative and inventive response from the organisations under threat. Piecemeal, reactive security solutions are giving way to strategically deployed multi-threat security systems. Instead of having to install, manage and maintain disparate devices, organisations can consolidate their security capabilities into a commonly managed appliance. These measures combined, in addition to greater user education are the best safeguard against the deviousness and pure innovation of cyber-criminal activities.



TRICKS ON EVADING SCAMS

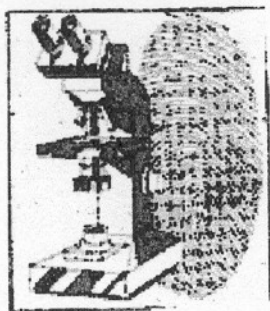
2. Tricks on evading scams

The beginning of the new year is the ideal time to make resolutions which should also include your Internet habits. Listed below are a number of suggestions that can help prevent your email address from becoming a target to spammers.

Never respond to spam. If you reply, even to request removing your e-mail address from the mailing list, you are confirming that your e-mail address is valid and the spam has been successfully delivered to your inbox. Lists of confirmed e-mail addresses are more valuable to spammers than unconfirmed lists, and are frequently bought and sold by spammers.

- Check to see if your e-mail address is visible to spammers by typing it into a Web search engine. If your e-mail address is posted to any Web sites or newsgroups, remove it if possible to help reduce how much spam you receive. · Disable in-line images, or do not open spam messages. Frequently spam messages include "Web beacons" enabling the spammer to determine how many, or which e-mail addresses have received and opened the message. Most current e-mail programs disable in-line images by default to prevent this from occurring.
- Do not click on the links in spam messages, including unsubscribe links. These frequently contain a code that identifies the e-mail address of the recipient, and can confirm the spam has been delivered and that you responded.
- When unsubscribing from e-mail, the main rule to follow is: if you didn't originally opt-in to receive it, or if you don't recognise the sender / company sending the e-mail, then don't unsubscribe. Trying to unsubscribe from one e-mail can start a flood of mail from other sources, so if you are unsure, it is best not to unsubscribe and block the mail another way. When unsubscribing from mail always check that the links in the e-mail go to the correct company Web site and not a Phishing site.
- When filling in Web forms, check the site's privacy policy to ensure it will not be sold or passed on to other companies. There may be a checkbox to opt out of third party mailings.
- Do not respond to e-mail requests to validate or confirm any of your account details. Your bank, credit card company etc. already have your account details, and would not need you to validate them. If you are unsure if a request for personal information from a company is legitimate, contact the company directly or type the Web site URL directly into your browser.
- Do not click on the links in the e-mail, as they may be fake links to phishing Web sites.
- If you have an e-mail address that receives a large amount of spam, consider replacing it with a new address and informing your contacts of the new address. Once you are on lots of spammers' mailing lists, it is likely that the address will receive more and more spam.

Source: securitypark.co.uk



CYBER CRIMES – SOME CASE STUDIES

3. Phishing in people's accounts

Today, 10 times more Indians use the internet for their banking needs than five years ago. And not surprisingly, the number of fraudsters eyeing your account have also multiplied. Globally, \$6 billion is stolen from consumer accounts by attacks called phishing and the scale of such fraud in India is fast catching up.

Sukhwinder Singh can never forget the day he checked his account online in late October last year. His account showed a deduction of Rs 41,000 and he had no clue where the money had gone. Investigation revealed the money had been transferred to one Harpreet Chohan in Delhi. It was later revealed that Sukhwinder had been a victim of a phishing attack on ICICI Bank. He had given his password and name online by replying to an email sent by the hackers. The hackers then logged into Sukhwinder's account and put in their mobile number instead of his. So that, when they did make the transfer, the message alerting Sukhwinder of the transfer would go out to their mobile and not his. This very move proved to be the hacker's nemesis.

The alleged phisher, Harpreet Chohan told CNBC-TV18, "I don't know how the money got into my account. I don't know how to operate a computer, so how can I be a hacker."

Cyber security expert, Vijay Mukhi says, "Phishing normally begins by you getting an innocuous e-mail - let's say from the bank - saying that someone is trying to hack into your account so you need to re-give us your password. So, you click on the link. That website is a fake or the spoofed website. Here you actually key in your personal details - you key in your name, your password when you click on ok, you don't realize that your user name and password has gone to the phisher."

Once the password and user name are with the phisher, it's only a matter of a few minutes before your money is transferred from your account to the phishers. What's even more threatening is that a phishing attack can be launched sitting in any part of the world. Mukhi says, "The problem with the internet is that it doesn't recognize geographical boundaries. So, today most of the phishing attacks to a bank will never occur from the country itself. I would launch a phishing attack on an Indian bank sitting in America and the spoofed page might be in Taiwan."

Finally, when the authorities do catch on, often the money trail leads to empty bank accounts with the cash long vanished. What's more, the attacks have just begun - October has seen over 26,000 phishing attacks worldwide, as compared to 15,000 last year. But industry experts say banks and customers both are catching on at a fast pace.

Head of Operations, ICICI Bank, Madhabi Puri Buch explains, "The interesting trend we are seeing in the case of phishing is that, while the number of attempts being made is increasing, the impact of each of these attempts is sharply declining. And the reason is very simple, just as the fraudsters are trying many things - both the banks and the customers come together to find ways to react to these attempts very rapidly. And in today's environment, in just a matter of four hours, these malicious sites are clamped down and they have no impact whatsoever on the customer."

Banks across the country have put up alerts against phishing e-mails on their websites and many have even launched campaigns to alert investors against it, so is this a sign of the increasing vulnerability of the industry?

Buch says, "When you see the tip of the iceberg is when you have to take action - not when you crash into the iceberg. Since, we believe that customers have such a vital role to play in prevention of fraud - not only in the case of phishing but in all types of financial fraud - we believe that it is part of our duty as a very large player in the financial system to create that awareness amongst a larger and larger set of people." So, just how does a phisher launch an attack? Well, you can't see them or even hear them but sitting behind computer screens, they are plotting their next move to get to your money. Launching a phishing attack often takes just a few hours and just about anyone can do it.

But experts say the sheer ease with which phishing can be executed is threatening as the knowledge on how to launch a phishing attack is often just a click away. Head-S-E Asia & India, Websense Inc, Surinder Singh says, 'It's getting more and more organised by the day. There is a whole set of an organised economy - where there are websites which sell these phishing kits. With these phishing kits, even a layman like me and you without any technical background, can launch these phishing attacks. In one or two days, there are hacking tools which are sold over these websites. It's very well organised and getting bigger by the day.'

Experts say phishers often meet in online secret chat rooms and trade knowledge on different security systems and new ways of launching attacks across countries. Mukhi explains, 'Once I was at a chat show on the internet and there were some phishers who were sharing ideas and they were all very unanimous - that most of the banks in India do not have an emergency response team for phishers and they don't respond as fast as an American or European bank would. So, phishers are now going to target Indian banks because they get more user names and passwords than any other banks.'

Buch says, 'We have created a special place where an alert can be given and we have found that the speed of response is extremely high. Within half an hour or a couple of hours of the mail first reaching us, we get an alert. The authorities have been extremely helpful. Through the authorities, we are able to bring down the site and there is no damage done to our customers. We are available to our customers 24x7 on so many channels. The people who are mapped to that e-mail ID that I mentioned - in addition to the executive director, it goes to a host of people who are on duty and on call 24x7.'

Sounds far fetched? Not really. Just a few days ago, UTI Bank was the victim of a phishing attack. The Delhi police has arrested four Nigerian nationals and an Indian in the case. According to the police, Oxabe and his accomplices allegedly sent e-mails that included a hyper-link within the e-mail itself. A click on that link took the recipients to a web page which was identical to UTI Bank's site. After the customers had logged in with their passwords and names, the information was sent to the alleged fraudsters who then used the information to transfer large sums of money to various accounts, all over the world, using the internet banking facility.

The police believe it's an international racket involving even more people, sitting in various parts of the world. Additional Commissioner of Police, Delhi police, KK Vyas

says, 'They had organised this racket in which they actually sent phishing mails using UTI Bank's details. They had copied the UTI logo etc and on that basis, they prepared letters as if they had originated from the bank.

But phishing attacks are continuing unabated. Last month, UTI Bank filed an FIR with the Delhi police after it received complaints from customers that cash had been debited from their accounts without their knowledge. Customers from Thane, Delhi, Vishakapatnam, Nasik and Ahmedabad - all had one thing in common- they had replied to an e-mail from the bank. The damage: 30 customers who lost Rs 20 lakhs and this amount was reported by the ones who caught on early.

KK Vyas explains, 'We had been receiving more and more complaints and that means this scam could run into a very high proportion. It is quite possible that other branches of UTI Bank in various parts of the country might also be affected. So, the process of verification is going on and we are in the process of identifying where all the money has gone.' Data from the Computer Emergency Response Team India shows phishing attacks are on the rise. The year 2005 saw 86 incidents of phishing reports. In 2006, this number more than doubled to 200 incidents. Not only were attacks being launched in India but 2006 saw the maximum phishing attacks being launched from India on other countries as well.

Security expert, Surinder Singh says, 'As per Websense Security Lab, we find that at any given point in time in 2006, there were 2 to 300 websites being hosted. There was a spurt in October where we identified 790 websites which were hosted in India and being used to carry out attacks.'

Buch adds, 'Over the last six months, we have done three specific initiatives. We introduced true factor verification on the website, which means in addition to the user ID and password, the customer now has a challenge mechanism, where we ask them things only they know and only if the answer is correct, do we allow him to do a transaction.'

But Singh admits, 'No system is perfect because all these criminals also study what protection techniques are being used and they will come up with something new. It's kind of a guerilla war. You can limit the phishing incident, so you can reduce the exposure but there's no way of totally eliminating it.'

Phishing and phishers may be keeping banks on high alert but the law is lagging far behind. Cyber Law expert, Pawan Duggal explains, 'Phishing is not an offence that is specifically defined under the IT Act, 2000. The law enforcement authorities are keen if at all to report and register a case under the typical generic provisions of cheating and criminal breach of trust under the Indian Penal Code, IPC.'

One of the biggest problems when you encounter phishing is that of cyber jurisdiction. Since these attacks are launched from any part of the world with the victim in a separate country, prosecutions of such cases becomes even more difficult.

Duggal says, 'One of the biggest problems in phishing is how do you go ahead and arrest these kind of offenders. If you look at the law book, it gives you an academic answer. The IT Act, 2000 has extra-territorial jurisdiction and it applies to any person of any nationality anywhere in the world - so long as the impacted computer is physically located in India. But having said that, the reality is that the Indian law is still not

applicable to people outside the territorial boundaries. Therefore, the law enforcement agencies reach a dead end.'

With the loopholes in the law, the best way to keep your money safe is to protect yourself from such attacks. Here's how to do that:

- * Be on the alert when a banking e-mail uses dramatic information to get you to react immediately.

- * Beware of e-mails from shopping websites offering free goods. It might be a scam to get your banking details.

- * Phishing e-mails are not personalized. Your bank will generally use your name when they contact you.

- * Finally, clicking on phishing sites may install a spying device on your computer. Downloading an anti-spyware programme will help.

Buch adds, 'We believe that working together with an alert set of customers and with banks who take very rapid action is the perfect antidote. With the authorities coming in and catching and penalizing the offenders, this combination is very rapidly going to make it not worthwhile for a fraudster to even attempt it.'

India is at tenth place when it comes to hosting phishing sites with the US and China biting the phishing bait more often. The United States remains at the top with 28.78% of all phishing sites located out of the United States and 11.96% out of China. Korea, Germany, Australia, Canada, Japan, United Kingdom, Italy and India are the other countries where phishing attacks are prevalent. As of now, 2.11% of the phishing sites are located in India.

Singh says, 'India on the threshold of having more and more people getting into online banking or taking online personal loans. So, it won't be a surprise if someday someone tells me that out of the total size of frauds happening - India would be at 1% or 2% - but even that would be Rs 200 crore.'

Though Buch says, 'If you look internationally at any of the large 3-4 banks in the world, they would be experiencing one phishing attempt a day. We are nowhere near that number.'

But even as banks are gearing up to tackle phishing, there is another kind of threat emerging - phishers are trying to get account details over the phone and this is called wishing. Singh explains, 'Instead of phishing, it's something called 'wishing', where they are using VoIP. Banks are telling people not to click on links. Now e-mails are coming saying that call us on this number for some particular reason and when people dial that number, actually it's not going to the interactive voice response or IVR of the bank, it's going to some other IVR, which mimics the IVR of the bank and you are asked your credit card details or some other details. So, new ways will keep coming up.' Mehak Kasbekar

4. UTI Bank hooked in a phishing attack

Fraudsters of cyberspace have reared its ugly head, the first of its kind this year, by launching a phishing attack on the website of Ahmedabad-based UTI Bank, a leading private bank promoted by India's largest financial institution, Unit Trust of India (UTI).

A URL on Geocities that is almost a facsimile version of the UTI Bank's home page is reported to be circulating amongst email users. The web page not only asks for the account holder's information such as user and transaction login and passwords, it has also beguilingly put up disclaimer and security hazard statements. "

In case you have received any e-mail from an address appearing to be sent by UTIBANK, advising you of any changes made in your personal information, account details or information on your user id and password of your net banking facility, please do not respond. It is UTI Bank's policy not to seek or send such information through email. If you have already disclosed your password please change it immediately, " the warning says. The tricky link is available on <http://br.geocities>

If any unsuspecting account holder enters his login id, password, transaction id and password in order to change his details as 'advised' by the bank, the same info is sent vide mailform.cz (the phisher's database).

After investigation, we found that Mailform is a service of PC Svet, which is a part of the Czech company PES Consulting. The Webmaster of the site is a person named Petr Stastny whose e-mail can be found on the web page.

Top officials at UTI Bank said that they have reported the case to the Economic Office Wing, Delhi Police. The bank has also engaged the services of Melbourne-based FraudWatch International, a leading anti-phishing company that offers phishing monitoring and take-down solutions. "We are now in the process of closing the site. Some of these initiatives take time, but customers have been kept in the loop about these initiatives, " said V K Ramani, President - IT, UTI Bank.

As per the findings of UTI Bank's security department, the phishers have sent more than 1,00,000 emails to account holders of UTI Bank as well as other banks. Though the company has kicked off damage control initiatives, none of the initiatives are cent percent foolproof. "

Now there is no way for banks to know if the person logging-in with accurate user information is a fraud," said Ramani. However, reliable sources within the bank and security agencies confirmed that the losses due to this particular attack were zilch.

The bank has sent alerts to all its customers informing about such malicious websites, besides beefing up their alert and fraud response system. "Engaging professional companies like FraudWatch help in reducing time to respond to attacks," said Sanjay Haswar, Assistant Vice President, Network and Security, UTI Bank.

5. Mumbai Police can now nail web offenders

Landmark deal signed with Orkut to share IP addresses and help arrest those posting objectionable content

Mumbai, March 10: Anti-Shivaji forums or anti-Ambedkar postings or “hate India” campaigns on Google’s social networking site, Orkut, have been confounding our authorities for quite sometime now. Other than blocking the objectionable forums, the Mumbai Police could do little—except wait for the next one to pop up on the web, say, a “fan club” of wanted underworld dons like Dawood Ibrahim or Chhota Shakeel.

But not any more. The Mumbai Police is finally equipped to track down such offenders and bring them to book. A single e-mail between the DCP in charge of the Enforcement Branch and the California-based company will now nail such persons.

Following a meeting between representatives of the site and the Enforcement Directorate last month, the Mumbai Police and Orkut have entered into an agreement to seal such cooperation in matters of objectionable material on the web.

“Early February, I met three representatives from Orkut.com, including a top official from the US. The other two were from Bangalore. We reached a working agreement whereby Orkut has agreed to provide us details of the ip address from which an objectionable message or blog has been posted on the site and the Internet service provider involved,” said DCP Enforcement, Sanjay Mohite.

That the measure is fool-proof is evident from the fact that an encrypted code has also been agreed upon for such communication to prevent people from posing as the Mumbai Police and laying their hands on such information from Orkut.

“I am also going to hold a meeting with all Internet service providers to stress the need to share information. We are also hoping to rope in U Tube in the future,” said Mohite.

Earlier, if a complaint regarding objectionable content was received, the police would contact the computer emergency response team, a government body based in New Delhi, and ask it to block the concerned web page. They did not have any way to track down the culprits.

“It was almost out of the question to track down the person who posted the material as we would have to go through the CBI to get basic information from Orkut as they are based in the US. The entire process of letter derogatory would come into play. But now we can take action on any content posted on the site from India,” he explained.

Mohite talks of a citizen who had complained to the police in November regarding a photograph of her posted on Orkut, along with derogatory text.

“She provided us the name of a suspected, but we did not have any proof. After the new

agreement was reached, we asked Orkut for the details of the concerned IP address. They replied instantly and we nailed the culprit, who turned out to be the suspect," said Mohite.

6. Three people held guilty in on line credit card scam

Customers credit card details were misused through online means for booking air-tickets. These culprits were caught by the city Cyber Crime Investigation Cell in Pune. It is found that details misused were belonging to 100 people.

Mr. Parvesh Chauhan, ICICI Prudential Life Insurance officer had complained on behalf of one of his customer. In this regard Mr. Sanjeet Mahavir Singh Lukkad, Dharmendra Bhika Kale and Ahmead Sikandar Shaikh were arrested. Lukkad being employeeed at a private institution, Kale was his friend. Shaiklh was employed in one of the branches of State Bank of India

According to the information provided by the police, one of the customer received a SMS based alert for purchasing of the ticket even when the credit card was being held by him. Customer was alert and came to know something was fishy; he enquired and came to know about the misuse. He contacted the Bank in this regards. Police observed involvement of many Bank s in this reference.

The tickets were book through online means. Police requested for the log details and got the information of the Private Institution. Investigation revealed that the details were obtained from State Bank of India . Shaikh was working in the credit card department; due to this he had access to credit card details of some customers. He gave that information to Kale. Kale in return passed this information to his friend Lukkad. Using the information obtained from Kale Lukkad booked tickets. He used to sell these tickets to customers and get money for the same. He had given few tickets to various other institutions.

Cyber Cell head DCP Sunil Pulhari and PI Mohan Mohadikar A.P.I Kate were involved in eight days of investigation and finally caught the culprits.

In this regards various Banks have been contacted; also four air-line industries were contacted.DCP Sunil Pulhari has requested customers who have fallen in to this trap to inform police authorities on 2612-4452 or 2612-3346 if they have any problems.

7. Conmen in Rs 400m SMS scam arrested in Mumbai

The alleged mastermind behind a Rs 400 million SMS fraud that duped at least 50,000 people has been arrested along with an associate more than two months after the scam was unearthed.

Jayanand Nadar, 30, and Ramesh Gala, 26, were arrested late on Monday from a hotel in Mira Road in the western suburbs. Nadar, a first year college dropout, along with his brother Jayaraj had allegedly duped at least 50,000 people of Rs.400 million, said officials in the city police's Economic Offences Wing (EOW).

The two brothers along with Gala allegedly took help of SMS technology and launched the first-of-its-kind SMS fraud in India.

According to EOW sources, in August 2006 the duo launched an aggressive and catchy advertisement campaign in the print media that read: "Nothing is impossible. The word itself is: I M Possible."

As part of the attractive scheme, the Nadar brothers messaged random numbers, asking people interested in 'earning Rs.10,000 per month' to contact them.

"The modus operandi adopted by the brothers was alluring," an EOW official said Tuesday. "Interested 'subscribers' were asked to deposit Rs.500 each. The conmen duo claimed to be working with a US-based company named Aropis Advertising Company, which wanted to market its client's products through SMS," senior inspector A Thakur said. "The brothers even put up a website (www.getpaid4sms.com) to promote their scheme. Subscribers who registered with them received about 10 SMS' every day about various products and were promised handsome commissions if they managed to rope in more subscribers by forwarding the messages," Thakur said.

In return, the Nadars promised to pay Rs.10,000 over 16 months to the investors. The amount was to be paid in instalments of Rs.1,000 every few months.

The brothers are said to have told the subscribers that their American clients wanted to conduct a study about local response to their advertisement and were using SMS as it was the latest medium of communication.

The duo invited people to become agents and get more members for the scheme. Gala reportedly looked after the accounts.

Initially, the brothers paid up small amounts. But when cheques and pay orders of larger sums issued by the duo were not honoured, the agents got worried. The SMSes too suddenly stopped.

On November 30, one of the duped agents approached the DN Road police station and lodged a complaint after a bank failed to honour a pay order amounting Rs.2.17 million issued by the Nadar brothers.

Then suddenly, the Nadars and Gala disappeared, leaving their agents and investors in the lurch. By December, the police were flooded with similar complaints. The DN Road police station registered a case against the brothers and Gala and later transferred it to the EOW.

"By December 2006 the scheme had an over 50,000 membership in Mumbai alone. And we suspect that hundreds of thousands from across the country were also hooked to the scheme, thanks to a massive agent network and a door-to-door campaign carried out by the firm's now duped agents," Thakur said. "We suspect that the fraud amount may be over Rs.1 billion. With the extent of the scam spread across the country, we are still trying to get the details." During investigations, the EOW came to know that the Nadars, residents of the upmarket Juhu-Tara Road, owned a fleet of imported sport utility vehicles and sedans. "The brothers led an extravagant life. They would stay in top five star hotels, throw massive parties for investors and were also known faces in the city's Page-3 circuit," Thakur revealed. "We are now looking for Jayaraj, who has eluded arrest. Gala, who is believed to have looked after the accounts, and Jayanand have been remanded to police custody till March 5."

8. Man arrested in a cyber fraud case

TRIVANDRUM — 4 March 2007 : The city police arrested a 27-year-old man for allegedly cheating a Mumbai based software engineer through the Internet by posing as a woman and stealing money from his bank account.

Rajesh, a resident of Ambalamukku, runs an Internet cafe at Chenthitta. After befriending the engineer through chat, Rajesh posed as 'Renuka' and used a voice converter to disguise his voice, Sub-Inspector, Thampanoor police station Sheen Tharayil said. He later forwarded a photo from a marriage bureau to the engineer, who provided a credit card and code to 'Renuka' to withdraw Rs2,500 for purchasing a flight ticket to Mumbai. The engineer even booked a room for 'Renuka' who failed to turn up. Enquiries revealed that Rs22,000 was withdrawn using the credit card.

9. Juhu police arrest 5 Nigerians

Mumbai: Juhu police arrested five Nigerian nationals for their alleged involvement in an inter-state job racket. The arrested have been identified as Vinset Mezek (26), Ogobol Tony (25), Kovhni Okosav (35), Charles Niogo (21) and Odirom Babatude (26). One person named Terri, who is a wanted in the case, is at large, say police.

According to the police, the accused used to send mails to people about vacancies in hotels outside India. If anyone responded, they would ask him to deposit money in their bank accounts in Mumbai. However, once they received the money, they would never contact the person. Although the accused have admitted to have duped only one person of Rs 1.2 lakh, the police say that they may have cheated many more in Mumbai and in other cities.

The whole matter came to light after Prabhat Singh, a resident of Orrisa, lodged a complaint with the Juhu police. Singh had paid Rs 1.2 lakh to an unidentified person for a job in the UK. He was never contacted after that.

“During our course of investigation, we tracked the account numbers where the money was deposited. We also tracked down the e-mail ID and the mobile numbers from which the mails and messages were sent,” said PD Shinde, senior police inspector at Juhu police station.

10. City principals seek police help to check cyber crime

Principals across the city seem to be taking a cue from principal of Bombay Scottish School, Mahim. After students began posting insults against him on Orkut, instead of punishing them he decided to call in cyber cell cops to talk to students. Now, other school principals have decided to bring in the cyber cell police to speak at their schools. They feel students and parents need to be educated against the legal and moral consequences of cyber crime.

Admitting to the existence of some mischievous students who misuse the internet and also stray into restricted sites due to lack of supervision, principals feel the cyber cell can play a huge role in educating students and warning them. Principal Rekha Vijaykar, GHK School, Santacruz, said that with more and more exposure to the internet, students had started misusing the freedom and hence needed to be monitored. "Monitoring and educating students against the pitfalls of visiting restricted sites is the responsibility of parents. However, the school too has to play an active role," she said.

Principal Alka Lokre of J M Bajaj School, Nagothane concurred. "Students need to be oriented with soul searching and conscience questioning which will help restrain them from misusing modern amenities," she said. As a solution, Principal Fr Dr Francis Swamy of Holy Family School, Andheri, said that apart from educating students, parents and teachers also needed to be roped in for the success of any initiative against internet abuse. "Without the support of parents, no awareness programme can succeed. Parents need to be sensitised to the problem on hand and should be active in stopping their children from maligning anyone," he said.

Principal Paul Machado of Champion School went a step further, highlighting the longterm effect of such uncontrolled freedom to students. "Parents must understand that today their children are misusing the internet to abuse others. Tomorrow, they may become victims of it too. Hence, parents need to be taken into confidence too to stem this rot." Apart from the above, all principals lauded the move by Dr D P N Prasad, Bombay Scottish principal, to invite the cyber cell to speak on cyber crime and said that they would also be inviting the cell officials to speak on the subject in their schools.

ADVICE TO PRINCIPALS

Pyschiatrist Dr Harish Shetty advises principals faced with students writing foul things about them and the school on internet sites Ignore it largely and it slowly dies When provoked and make critical observations or issue threats directly or indirectly the kids enjoy it. The aim is also to rattle teachers. The net is a free world and makes all in authority or influence and others vulnerable. Kids too share a love-hate relation with teachers At one level the net is a safe space to vent frustrations. Here feelings, not necessarily facts, are expressed. This is not cyber crime as all kids are under 18 and empty threats do not work. Amidst the junk, look for hidden messages. Such sites are popular for a short time and the fad passes away soon Educating kids about the negatives of the net and providing enough safe spaces within school walls will bring down such postings.

Principals should educate teachers not to be rattled by it. Do not humiliate children following such an event and also lower the 'humiliatory index' in your schools Almost 60 Bombay Scottish students had contributed freely to a forum on Orkut, alleging in their postings that the Principal and his deputy have ruined the image of the school

11. Tamil Tiger credit card racket spreads to Chennai, India

The Sri Ramachandra Medical College police at Porur, Chennai, arrested G. Elango, a Tamil Tiger agent carrying a British passport, on Friday and seized 28 ATM cards in his possession. The police said Elango illegally withdrew over Rs. 30 lakh from the ATM centres of a few nationalized banks and a private bank. The amount was then sent to the United Kingdom through unauthorized channels.

It is learnt that the Chennai Police was alerted by a civilian who had seen Elango using several ATM cards to withdraw money from an ATM centre of a private bank on Mount-Poonamallee Road, Porur.

A police team led by the Assistant Commissioner Police Balasubramaniam caught Elango red-handed while he was withdrawing money from the ATM machine.

G. Elango (38) of Middlesex, United Kingdom, is a shareholder in 'Thamilini' -- a cash and carry grocery shops operated by the Tamil Tigers in UK.

Elango is from Valvetiturai, a notorious port for smugglers in the north of Sri Lanka. He is the partner of the LTTE's cash and carry centres of Thamilini in London suburbs - one in Croydon and another in Southall.

After the arrest Police has found, besides the ATM cards, registration certificate books of two cars, a cellular phone and a passport. Tamil Nadu Police is now seeking the assistance of the Scotland Yard to obtain more information about Elango. The Tamil Tigers are also under investigation in UK for operating credit card rackets in Europe.

<http://www.asiantribune.com/index.php?q=node/4236>

12. Net con duo in net, associates missing

Bhubaneswar: Rourkela police busted a racket involving an online fraud worth Rs 12.5 lakh. The modus operandi of the accused was to hack into the eBay India website and make purchases in the names of credit cardholders.

Two persons, including alleged mastermind Debasis Pandit, a BCA student, were arrested and forwarded to the court of the subdivisional judicial magistrate, Rourkela. The other arrested person is Rabi Narayan Sahu.

Superintendent of police D.S. Kutty said the duo was later remanded in judicial custody but four other persons allegedly involved in the racket were untraceable.

A case has been registered against the accused under Sections 420 and 34 of the Indian Penal Code and Section 66 of the IT Act and further investigation is on, he said.

While Pandit, son of a retired employee of Rourkela Steel Plant, was arrested from his Sector VII residence last night, Sahu, his associate and a constable, was nabbed at his house in Uditnagar.

Pandit allegedly hacked into the eBay India site and gathered the details of around 700 credit cardholders. He then made purchases by using their passwords.

The fraud came to the notice of eBay officials when it was detected that several purchases were made from Rourkela while the customers were based in cities such as Bangalore, Baroda and Jaipur and even London, said V. Naini, deputy manager of eBay.

The company brought the matter to the notice of Rourkela police after some customers lodged complaints.

Pandit used the address of Sahu for delivery of the purchased goods, said police. The gang was involved in train, flight and hotel reservations.

The hand of one Satya Samal, recently arrested in Bangalore, is suspected in the crime. Samal had booked a room in a Bangalore hotel for three months. The hotel and transport bills rose to Rs 5 lakh, which he did not pay.

Samal was arrested for non-payment of bills, following which Pandit rushed to Bangalore and stood guarantor for his release on bail, police sources said.

13.Orkut: The new danger

Orkut, the online portal, owned by Google finds itself at the centre of debate. A nineteen-year-old student has been accused of making a fake account of a girl. Can we prevent the misuse of this technology by not posting our numbers and pictures?

ABHISHEK NEVER IMAGINED that the prank he played on his classmate would land him in jail. Abhishek, a management student and still in his teens, was arrested by the Thane police following a girl's complaint about tarnishing her image in the public forum - Orkut. The report after being published in Mumbai Mirror has created a stir among the Orkutians and opened up a whole new box of debate.

The incident

Abhishek had created a fake account in the name of the girl with her mobile number posted on the profile. The profile has been sketched in such a way that it draws lewd comments from many who visit her profile. The Thane Cyber Cell tracked down Abhishek from the false e-mail id that he made to open up the account.

The question

In this case, the girl has not posted her picture or mobile number in the fake profile. A brief search in the Orkut profile will reveal many such profiles with pictures of beautiful girls. My guess is that many of these girls are not even aware of the fact that their profile exists. These are created by some other people. I will term this as "rape of the image". Now the question is "Can we really prevent this rape?"

The debate

The Mumbai Mirror's report on the issue came with tips to the Orkut users. Police Sub-Inspector Ravindra Chauhan has been quoted as saying, "Orkut users should not put up their photographs on the site. They should not reveal personal information in their profile. Also no cellphone numbers or identity should be mentioned in the scrap book, as it is open to all." But whether this really can be a way out, is debatable. "What about the hundreds of CVs I send to the unknown agencies everyday? They even contain my mobile number", says Aditi, a DU student and a hardcore Orkut addict. She does have a point.

The truth is that in today's world mobile numbers are far from being personal information. The proof lies in the numerous sales calls that we receive from credit card agents. On the issue of the photograph, Aditi says, "When Orkut gives an opportunity to show your face to the whole world, then why not?" When asked about the risks involved, she replied, "Who cares?" But everyone is not as carefree as Aditi. A brief search in Orkut once more will reveal profiles that have pictures of film stars, flowers, animals, sceneries and not the face of the owner. "I will never put my picture on Orkut profile," says Mansi, whose profile in Orkut carries the picture of Aishwarya Rai. "It's not safe, anybody and everybody can save it on their computer and can misuse it." But here again the question lies - can we really prevent it? What happens to the hundreds of passport photographs we send with the application forms all our life? Any of them can be scanned and put up without our notice. Are we sure that all copies of the digital pictures taken at

our local photography shop are deleted after we leave? "I don't know, but there is no harm in being careful," says Mansi.

So perhaps even in this age of globalisation and technical advancements we will hold ourselves from showing our face to the entire world for we never know who is misusing it in what way. And as the lawmakers say "We cannot do anything, until a complaint is lodged".

14. Offensive SMS can lead to 2 years in jail

With mobile phones virtually taking over the role of a personal computer, the proposed amendments to the Information Technology Act, 2006, have made it clear that transmission of any text, audio or video that is offensive or has a menacing character can land a cellphone user in jail for two years. The punishment will also be attracted if the content is false and has been transmitted for the purpose of causing annoyance, inconvenience, danger or insult.

And if the cellphone is used to cheat someone through personation, the miscreant can be punished with an imprisonment for five years.

The need to define communication device under the proposed amendments became imperative as the current law is quiet on what kind of devices can be included under this category. The amended IT Act has clarified that a cellphone or a personal digital assistance can be termed as a communication device and action can be initiated accordingly. Accentuated by various scandals that hit the country during the past two years, including the arrest of the CEO of a well-known portal, the government has also introduced new cyber crimes under the proposed law. The amended Act, which was placed before the Lok Sabha during the recently concluded winter session, has excluded the liability of a network service provider with regard to a third party's action. However, it has made cyber stalking, cyber defamation and cyber nuisance an offence. Anybody found indulging in all these offences can be imprisoned for two years.

The proposed changes have also sought amendments in the form of insertions in the Indian Penal Code, thereby declaring identity theft an offence. If a person cheats by using electronic signature, password or any other unique identification feature of any other person, he shall be punished with imprisonment for two years and also liable to fine.

Asking for an insertion in the Indian Penal Code as Section 502A of the law, the proposed amendments have said that whoever intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, shall be punished with two years of imprisonment and fine of Rs 2 lakh. The private parts can be either naked or undergarment clad public areas.

Making the law more technologically neutral, the amended provisions have included authentication of electronic record by any electronic technique. At the moment, electronic records can be authenticated by just digital signatures, the public key infrastructure technology (PKI).

With the new provisions, however, biometric factors like thumb impression or retina of an eye shall be included as techniques for authentication.

Even as the law makers have tried to cover up for the lapses of the current IT Act, they seem to have made it liberal by way of reducing the punishment from three years to two years. With these changes, a cyber criminal will now be entitled to bail as a matter of right, as and when he gets arrested.

15. NIGERIAN HELD IN E-CRIME

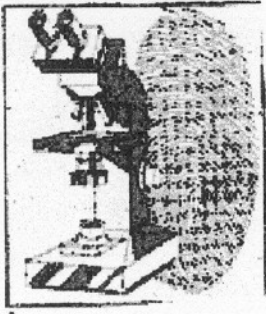
The Cyber Crime Branch of the Mumbai Police arrested a 30-year old Nigerian on Monday for allegedly duping 26 customers of the ICICI Bank to the tune of Rs 6. 93 lakh.

Abdul Rehman Azocz would send fake e-mail to the bank's customers with the intention to cheat, mislead and defraud the bank customers and illegally collecting the information from the bank customers and infringe the website of ICICI Bank and carrying out illegal transactions causing loss to the customers.

Sources said the accused identified as Abdul Rehman Azocz, resident of house no 23, Ofim street, Lagos Island. Lagos. In Mumbai, he was put up at a lodge at Pydhonie from where he was arrested on Monday. The additional chief metropolitan magistrate's court at Esplanade remanded Azocz to custody till January 23 after Sections 419, 420, 468, 469 and 471 of IPC were pressed against him.

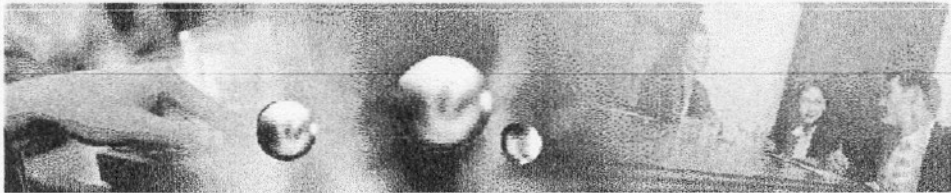
A Cyber Crime Branch officer told DNA that Azocz was arrested after he contacted Ms Basra alias Shanu, an account holder with ICICI Bank, through email and fraudulently transferred money from her account last week. Basra then informed the bank authority, which in turn turned the matter to Cyber Crime Cell. The police officials traced Azocz with the help of IT experts.

Complainant Samir Dabral, 30, assistant manager of Risk Containment Unit in ICICI Bank told DNA, " There are 26 customers in Mumbai and other cities in India, who have been duped to the tune of Rs 6.93 lakh. Moreover, the bank has not warned its customers, through email or otherwise, about providing user information via fake e-mails or fake webpages."



CYBER CRIMES – CASE STUDIES (PRESENTATIONS)

Digital Forensic



Network Security solutions (I) Ltd © 2005-2006



Digital Forensics

"Like a detective, the archaeologist searches for clues in order to discover and reconstruct something that happened. Like the detective, the archaeologist finds no clues too small or insignificant. And like the detective, the archaeologist must usually work with fragmentary and often confusing information. Finally, the detective and the archaeologist have as their goal the completion of a report, based on a study of their clues, that not only tells what happened but proves it."



Network Security solutions (I) Ltd © 2005-2006





Phishing

- Phishing is a tactic used to get credit card information from consumers who believe they are visiting legitimate bank and credit card sites. Usually accomplished through use of pop-up windows that piggyback on real sites, phishing has been on the scene for some time, but recent attacks have underscored how easily attackers can get hold of personal information .



Phishing and Pharming

- Phishing attacks use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc.
- Pharming uses the same kind of spoofed sites, but uses malware/spyware to redirect users from real websites to the fraudulent sites (typically DNS hijacking).
- By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince recipients to respond to them.





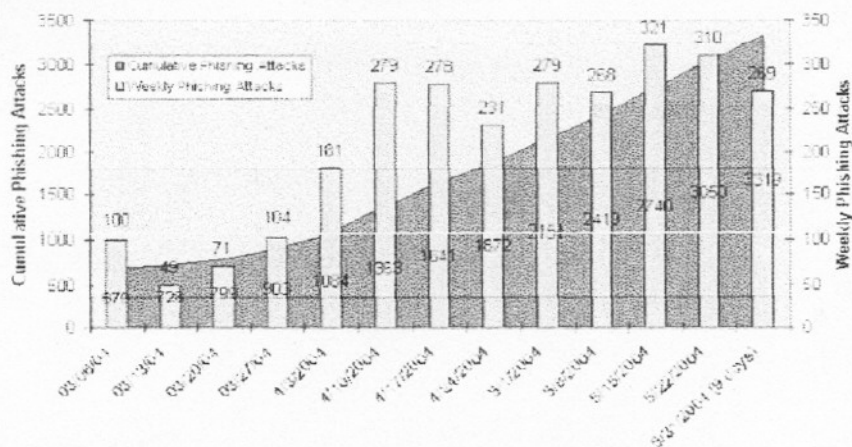
Phishing Attack Statistic

Number of unique phishing attacks reported in recent months	1197
Peak number of unique phishing attacks per week reported in recent months	321
Organization most targeted by phishing attacks in recent months	Citibank (370)
Business sector most targeted by phishing attacks in recent months	Financial Services
Percentage of phishing attacks using spoofed email addresses	95%

REST ASSURED



Unique Phishing Attack Trends
Mar 2004 - May 2004



REST ASSURED





What to do to feel protected?

• Internet Auction Fraud

- Understand as much as possible about how the auction works, what your obligations are as a buyer, and what the seller's obligations are before you bid.
- Find out what actions the web site/company takes if a problem occurs and consider insuring the transaction and shipment.
- Learn as much as possible about the seller, especially if the only information you have is an e-mail address. Examine the feedback on the seller.
- Determine what method of payment the seller is asking from the buyer and where he/she is asking to send payment.



Example of Phishing

From: Customer Support [mailto:support@citibank.com]

Sent: Thursday, October 07, 2004 7:53 PM

To: Eilts

Subject: NOTE! Citibank account suspend in process

Dear Customer:

Recently there have been a large number of cyber attacks pointing our database servers. In order

to safeguard your account, we require you to sign on immediately. This personal check is requested of you as a precautionary measure and to ensure yourselves that everything is normal with your balance and personal information. This process is mandatory, and if you did not sign on within the nearest time your account may be subject to temporary suspension. Please make sure you have your **Citibank(R) debit card number and your User ID and Password at hand**. Please use our secure counter server to indicate that you have signed on, please click the link below: <http://211.158.34.249/citifi/>. Note that we have no particular indications that your details have been compromised in any way. Thank you for your prompt attention to this matter and thank you for using Citibank(R)

Regards,

Citibank(R) Card Department

(C)2004 Citibank. Citibank, N.A., Citibank, F.S.B.,

Citibank (West), FSB. Member FDIC. Citibank and Arc





How to Detect Deception

- Publish your mail server addresses (to thwart spoofing)
- Educate customers (and employees)
- Establish online communication protocols
- Create a response plan now
- Proactively monitor for phishers and fraud
- Make yourself a difficult target

<http://www.cio.com/archive/090104/phish.html>



REST ASSURED



IN YOUR INTEREST



Prevent Phishing

- Never click on hyperlinks
- Use Anti-SPAM filters
- Use Anti-Virus Software
- Use personal firewalls
- Keep all software updated
- Always look for https and sites that ask for "personal information"
- Keep computer clean from Spyware
- Know Fraudulent activity on the Internet
- Check your credit report immediately for free!
- If unsure, ask!



REST ASSURED



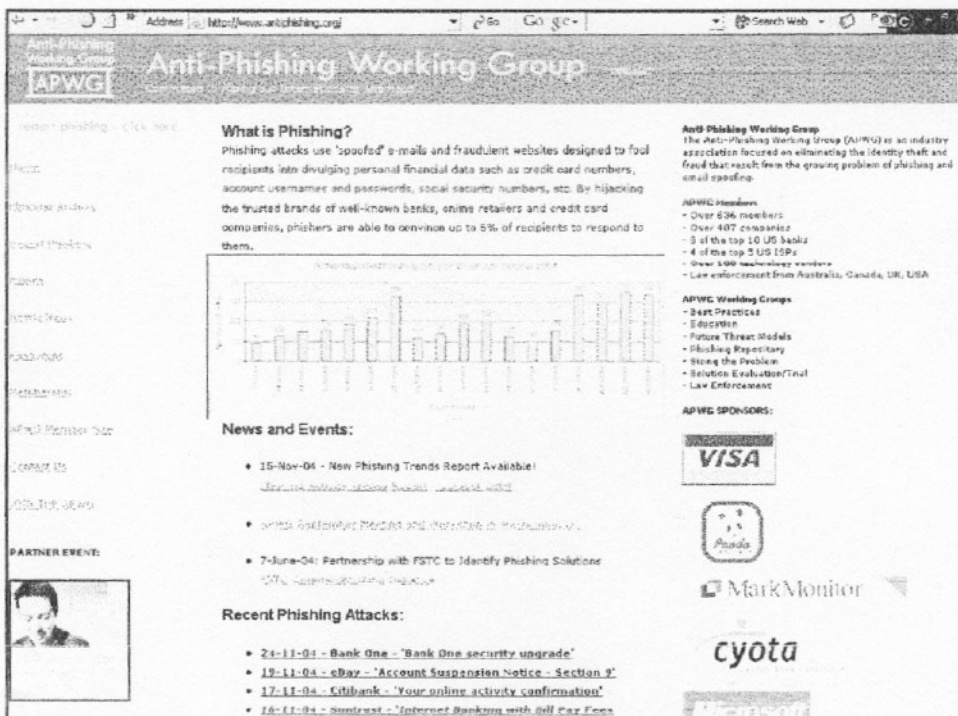
IN YOUR INTEREST



Industry Sponsored Anti-Phishing Efforts

- **"The Anti-Phishing Working Group (APWG) is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing."** <http://www.antiphishing.org/>
 - An updated chart of examples of phishing attacks submitted to [antiphishing.org](http://www.antiphishing.org) are available here: http://www.antiphishing.org/phishing_archive.htm
- White Paper, **Anti-Spam Technical Alliance**, 22 June 2004, <http://tinyurl.com/2qaje>
- **Microsoft Anti-Spam Virtual Press Room**, <http://www.microsoft.com/presspass/events/antispam/material.a.sp>
- **TECF – Trusted Electronic Communications Forum** <http://www.tecf.org/>
 - "The Trusted Electronic Communications Forum (TECF) is a global, cross-industry consortium of industry leaders focused on efforts to eliminate the phishing and spoofing attacks that lead to identity theft and brand distrust."



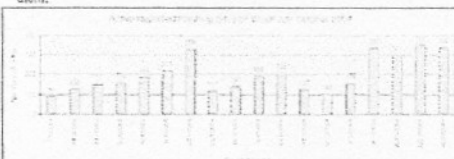


The screenshot shows the APWG website with the following content:

Anti-Phishing Working Group

What is Phishing?

Phishing attacks use "spoofed" e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince up to 5% of recipients to respond to them.



News and Events:

- 15-Nov-04 - New Phishing Trends Report Available
- 17-Nov-04 - Partnership with FSTC to Identify Phishing Solutions

Recent Phishing Attacks:

- 24-11-04 - Bank One - "Bank One security upgrade"
- 19-11-04 - eBay - "Account Suspension Notice - Section 9"
- 17-11-04 - Citibank - "Your online activity confirmation"
- 16-11-04 - SunTrust - "Internet Bankers with Tell Fax Fees"

APWG Members:

- Over 636 members
- Over 407 companies
- 3 of the top 10 US banks
- 4 of the top 5 US ISPs
- Over 500 technology vendors
- Law enforcement from Australia, Canada, UK, USA

APWG Working Groups:

- Best Practices
- Education
- Future Threat Models
- Phishing Repository
- Stopping the Problem
- Solution Evaluation/Trust
- Law Enforcement

APWG SPONSORS:





The best protection

- The best protection against these phishing scams is to assume the worst
 - An e-mail asking for your credit-card number or similar information isn't real.
 - If you think the message may be authentic, pick up a telephone and call the real phone number for the company that's supposedly seeking information from you.
- Additional assistance can be found online at www.antiphishing.org.
 - The site lists recent phishing scams and offers tips on how to avoid being defrauded.



REST ASSURED



REST ASSURED



Credit Card Fraud

- Don't give out your credit card number(s) online unless the site is a secure and reputable site.
- Sometimes a tiny icon of a padlock appears to symbolize a higher level of security to transmit data. This icon is not a guarantee of a secure site, but might provide you some assurance.
- Don't trust a site just because it claims to be secure.
- Before using the site, check out the security/encryption software it uses.



REST ASSURED



REST ASSURED



Phishing Basics (1)

- Pronounced "fishing"
- Scam to steal valuable information such as credit cards, social security numbers, user IDs and passwords.
- Also known as "brand spoofing"
- Official-looking e-mail sent to potential victims
 - Pretends to be from their ISP, retail store, etc.,
 - Due to internal accounting errors or some other pretext, certain information must be updated to continue the service.



Credit Card Fraud

- Make sure you are purchasing merchandise from a reputable source.
- Do your homework on the individual or company to ensure that they are legitimate.
- Try to obtain a physical address rather than merely a post office box and a phone number, call the seller to see if the number is correct and working.
- Send them e-mail to see if they have an active e-mail address and be wary of sellers who use free e-mail services where a credit card wasn't required to open the account





Frauds

- Investment Fraud

- Don't invest in anything based on appearances. Just because an individual or company has a flashy web site doesn't mean it is legitimate.

Web sites can be created in just a few days. After a short period of taking money, a site can vanish without a trace.

- Nigerian Letter Scam

- Be skeptical of individuals representing themselves as Nigerian or foreign government officials asking for your help in placing large sums of money in overseas bank accounts.

Do not believe the promise of large sums of money for your cooperation.

Guard your account information carefully.



REST ASSURED



REST ASSURED



Statistics

- Based on the representative sample in its April survey,
- Gartner believes nearly 11 million people, or 19 percent of the 57 million who received a phishing attack e-mail, clicked on a link in that e-mail.
- Of those, 1.78 million, or 3 percent, remember giving phishers sensitive financial or personal information, such as credit card numbers or billing addresses.



REST ASSURED



REST ASSURED



Phishing Basics (2)

- Link in e-mail message directs the user to a Web page
 - Asks for financial information
 - Page looks genuine
 - Easy to fake valid Web site
 - Any HTML page on the real Web can be copied and modified
- E-mails sent to people on selected lists or to any list
 - Some % will actually have account
- "Phishing kit"
 - Set of software tools
 - Help novice phisher imitate target Web site
 - Make mass mailings
 - May include lists of e-mail addresses



REST ASSURED



Serious Problem

"Illegal access to checking accounts, often gained via phishing scams, has become the fastest-growing form of consumer theft in the United States, accounting for a staggering \$2.4 billion in fraud in the previous 12 months."

-- Gartner Group



REST ASSURED





Citibank

Dear Citibank Customer

We were unable to process the recent transactions on your account. To ensure that your account is not suspended, please update your information by clicking [here](#).

If you have recently updated your information, please disregard this message as we are processing the changes you have made.

Links to
<http://82.90.165.65/citi>

Citibank Customer Service
Citibank Alerting Service
Citibank [alert@citibank.com]

REST ASSURED



PayPal (1)

PayPal

Security Center



Military Grade Encryption is Only the Start

At PayPal, we want to increase your security and comfort level with every transaction. From our Buyer and Seller Protection Policies to our Verification and Reputation systems, we'll help to keep you safe.

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to believe that your account was hijacked by a third party without your authorization.

If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you. However, if you are the rightful holder of the account, click on the link below to log into your account and follow the instructions.



Actually links to
<http://212.45.13.185/paypal/index.php>

<https://www.paypal.com/cgi-bin/webscr?cmd=login-run>

If you choose to ignore our request, you leave us no choice but to temporarily suspend your account.

We ask that you allow at least 72 hours for the case to be investigated and we strongly recommend to verify your account in that time.

If you received this notice and you are not the authorized account holder, please be aware that it is in violation of PayPal policy to represent oneself as another PayPal user. Such action may also be in violation of local, national, and/or international law. PayPal is committed to assist law enforcement with any inquiries related to attempts to misappropriate personal information with the intent to commit fraud or theft. Information will be provided at the request of law enforcement agencies to ensure that perpetrators are prosecuted to the fullest extent of the law.

Thanks for your patience as we work together to protect your account.

Sincerely,
 PayPal Account Review Department
 PayPal, an eBay Company






Dear Citibank Customer,

At Citibank, we take security very seriously. As many customers already know, Microsoft Internet Explorer has significant 'holes' or vulnerabilities that virus creators can easily take advantage of.

At Citibank, we maintain your personal information and data according to strict standards of security and confidentiality as described in the Terms and Conditions that govern your use of this site. Online access to your account portfolio is only possible through a secure web browser.

In order to further protect your account, we have introduced some new important security standards and browser requirements. Citibank security systems require that your computer system is compatible with our new standards.

This security update will be effective immediately. Please sign on to Citibank Online in order to verify security update installation. Failure to do so may result in your account being compromised.

Citibank Online

Copyright © 2004 Citicorp

Links to
<http://200.189.70.90/citi/>






eBay



Dear eBay customer,

During our regularly scheduled account maintenance and verification procedures, we have detected a slight error in your billing information.

This might be due to either of the following reasons:

1. A recent change in your personal information (i.e. change of address).
2. Submitting invalid information during the initial sign up process.
3. An inability to accurately verify your selected option of payment due to an internal error within our processors.

<http://signin-ebay.com/cgi-bin.tk/eBayd11.php>

Please update and verify your information by clicking the link below:

<http://cgi.ebay.com/saw-cgi/eBayISAPI.dll?RegisterEnterInfo>

If your account information is not updated within 48 hours then your ability to sell or bid on eBay will become restricted.



REST ASSURED



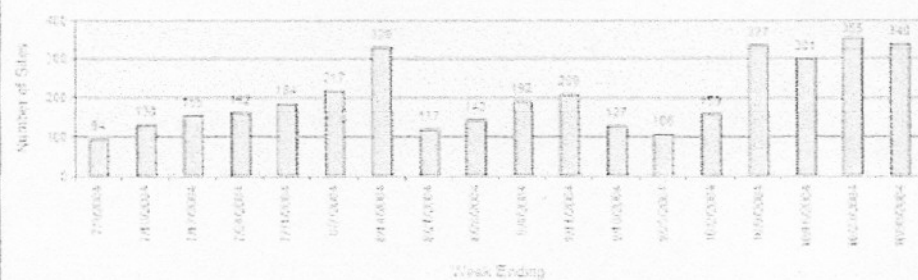
www.ebay.com



APWG (antiphishing.org)

• Anti-Phishing Working Group

Active Reported Phishing Sites by Week July-October 2004



REST ASSURED



www.antiphishing.org

Spoofed Page and Address Bar

Not the real address bar

See http://www.antiphishing.org/news/03-31-04_Alert-FakeAddressBar.html

ATM/Debit Card (CIN) / Card #

Expiration Date /

PIN

REST ASSURED

Based on a slide copyright © 2004 Don Holden, CISSP
Used with permission (and thanks).

Spoofed Address Bar

- Problem
 - JavaScript device replaces address bar
 - Allows complete control
 - Can show one URL while going to another
 - Viewing source code for page does NOT show Java source code
- Implications
 - With address bar installed, could track other sites visited
 - Could do a man-in-the-middle attack to see everything entered

REST ASSURED



Public Education

- Use digitally-signed documents ONLY
 - Don't release unsigned documents
 - Get consumers used to idea that an unsigned document is an untrustworthy document
- Use public education campaigns
 - "No one will ever ask you to confirm your password"
 - "Don't believe alerts that address you as 'Dear Customer.'"
 - Link to APWG documents; e.g.,
http://www.antiphishing.org/consumer_rec.html

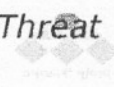


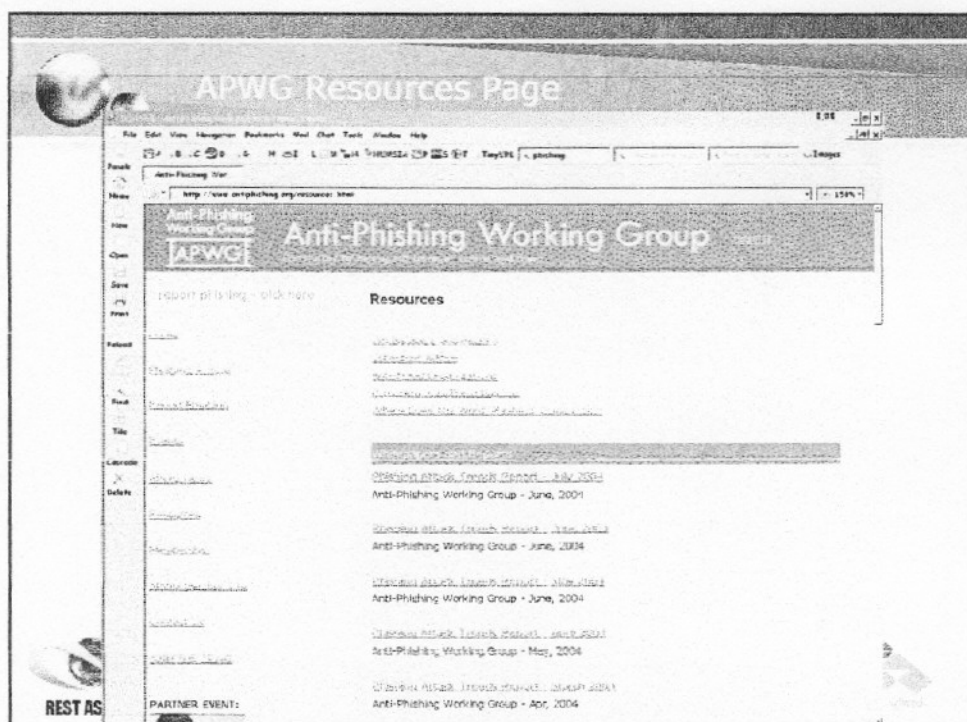
Possible Solutions

- Strong Website authentication
- Mail server authentication
- Digitally-signed e-mail with desktop verification
- Digitally-signed e-mail with gateway verification



APWG: *Proposed Solutions to Address the Threat of Email Spoofing Scams*





CloudMark's Community Approach

- Cloudmark SafetyBar
 - <http://www.cloudmark.com/>
 - Works for Outlook and Outlook Express
- Community members report new spam or fraud at push of button
 - Information sent worldwide to improve blocking
- Anti-fraudster measures
 - Reliability of reports affects credibility of reporter
 - Spammers and fraudsters would lose credibility fast

REST ASSURED

