Cyber Law Cases in India and World

**MYSPACE CATCHES A MURDERER**   
  
MySpace has played an important role in helping Oakland police apprehend a 19-year old man accused of shooting a San Leandro High School football player Greg "Doody" Ballard, Jr.

Oakland police had a street name of a suspect and were able to identify Dwayne Stancill, 19 of Oakland from a picture they found on a gang's MySpace page. Police brought the suspect to their headquarters where detectives say he confessed. What was most troubling to investigators was the lack of motive for the killing.

**OFFICIAL WEBSITE OF MAHARASTRA GOVERNMENT HACKED**  
  
MUMBAI, 20 September 2007 — IT experts were trying yesterday to restore the official website of the government of Maharashtra, which was hacked in the early hours of Tuesday.

Rakesh Maria, joint commissioner of police, said that the state’s IT officials lodged a formal complaint with the Cyber Crime Branch police on Tuesday. He added that the hackers would be tracked down. Yesterday the website, http://www.maharashtragovernment.in, remained blocked.

Deputy Chief Minister and Home Minister R.R. Patil confirmed that the Maharashtra government website had been hacked. He added that the state government would seek the help of IT and the Cyber Crime Branch to investigate the hacking.

“We have taken a serious view of this hacking, and if need be the government would even go further and seek the help of private IT experts. Discussions are in progress between the officials of the IT Department and experts,” Patil added.

The state government website contains detailed information about government departments, circulars, reports, and several other topics. IT experts working on restoring the website told Arab News that they fear that the hackers may have destroyed all of the website’s contents.

According to sources, the hackers may be from Washington. IT experts said that the hackers had identified themselves as “Hackers Cool Al-Jazeera” and claimed they were based in Saudi Arabia. They added that this might be a red herring to throw investigators off their trail.

According to a senior official from the state government’s IT department, the official website has been affected by viruses on several occasions in the past, but was never hacked. The official added that the website had no firewall.

**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 employeed 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.  
 **How cyber crime 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.  
Cybercrime which is regulated by Internet Law  (Cyber Law) or IT Act has become a profession and the demographic of your typical cybercriminal 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 specialised skills and resources), as well as a good deal of trade at prices set by the market forces of supply and demand. Cybercrime is no different: it boasts a buoyant international market for skills, tools and finished product. It even has its own currency.  
The rise of cybercrime 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 (cybercriminals 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) chatroom. 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.