



International Institute of Security & Safety Management



Let's professionalize the professionals...



Newsletter of NCR Chapter : August 2007

Internet Crimes & Security Professionals



Readers may recall that our July Newsletter had editorial on the subject of misuse of mobile phones by the terrorists as switching devices for exploding IEDs. Our July Newsletter was circulated on 28th June and as such details of Glasgow and London attempts by the “Doctors of Terror” were no available in details. However we at IISSM had attempted to analyze the latest trends for use or rather ‘misuse’ of mobile phones by the terrorist and thought it appropriate to warn our readers so that they are better prepared little knowing that somewhere some one was already planning the ghastly details for misuse.

Among the security measures that need to be taken to make it difficult for the terrorists to use cell phones are strict pre-sale checks, control over pre-paid SIM cards or even a ban on them etc. Despite such measures, terrorists manage to circumvent the security measures. The only way out is not to let the guard down and not to permit complacency in the security personnel.

In past many issues we have attempted to put some light on the crimes of new world - internet crimes. We have given some elementary information on types of the crimes, criminals and their modus-operandi. We have also given some common solutions to the common problems. But, now is the time that security professional have to come of age! Time to grow-up! For we can not avoid but have to deal the subject head long, for we can not but start understanding the technologies and techniques of the internet crimes! For want of efforts we shall perish - as security professionals. We must professionalize the profession by understanding the subject how-so-ever technical it might appear, and then only we can offer solution to our Management. Otherwise we security professionals will be liabilities on management and who wants liabilities?

**Capt S B Tyagi, FISM, CSC
For NCR Chapter, IISSM**



What are Internet Crimes?

Internet crime is crime committed on the Internet, using the Internet and by means of the Internet.

Computer crime is a general term that embraces such crimes as –

- phishing,
- credit card frauds,
- bank robbery,
- illegal downloading,
- industrial espionage,
- child pornography,
- kidnapping children via chat rooms,
- scams,
- cyber terrorism,
- creation and/or distribution of viruses spam and so on.

All such crimes are computer related and facilitated crimes.

With the evolution of the Internet, along came another revolution of crime where the perpetrators commit acts of crime and wrongdoing on the World Wide Web. Internet crime takes many faces and is committed in diverse fashions. The number of users and their diversity in their makeup has exposed the Internet to everyone. Some criminals in the Internet have grown up understanding this superhighway of information, unlike the older generation of users. This is why Internet crime has now become a growing problem in the world.

The different types of Internet crime vary in their design and how easily they are able to be committed. Internet crimes can be separated into two different categories. There are crimes that are only committed while being on the Internet and are created exclusively because of the World Wide Web. The typical crimes in criminal history are now being brought to a whole different level of innovation and ingenuity. Such new crimes devoted to the Internet are email “phishing”, hijacking domain names, virus immistion, and cyber vandalism.

People have been trying to solve virus problems by installing virus protection software and other software that can protect their computers. Other crimes such as email “phishing” are not as known to the public until an individual receives one of these fraudulent emails. These emails are cover faced by the illusion that the email is from your bank or another bank. When a person reads the email he/she is informed of a problem with his/her personal account or that some another individual wants to send the person some of their money and deposit it directly into their account. The email asks for your personal account information and when a person gives this information away, they are financing the work of a criminal.

The question about how to police these crimes have always confounded the security professionals as this task is turning out to be an uphill battle. The reality is that Internet criminals are rarely caught. One reason is that hackers will use one computer in one country to



hack another computer in another country. Another eluding technique used is the changing of the emails, which are involved in virus attacks and “phishing” emails so that a pattern cannot be recognized. An individual can do their best to protect themselves simply by being cautious and careful. Internet users need to watch suspicious emails, use unique passwords, and run anti-virus and anti-spyware software. Do not open any email or run programs from unknown sources.

How internet scams are perpetrated?

Popular products

Fraudsters seem to prefer small and valuable products, such as: watches, jewelry, laptops, digital cameras, and camcorders. These items are usually commodities that are easily sellable and have a broad range of appeal. However, fraud in hosted marketplaces such as EBay covers a broad range of products from cellular phones to desktop computers. The craft has continually evolved in sophistication. In some instances, a picture of the product is sent in place of the actual product. Other times, products are out rightly never sent after the bill is charged to credit card accounts. Victims are left to deal with credit card companies for chargebacks.

Identity Theft Schemes

Stolen credit cards

Most Internet fraud is done through the use of stolen credit card information which is obtained in many ways, the simplest being copying information from retailers, either online or offline. There have been many cases of hackers obtaining huge quantities of credit card information from companies' databases. There have been cases of employees of companies that deal with millions of customers in which they were selling the credit card information to criminals.

Despite the claims of the credit card industry and various merchants, using credit cards for online purchases can be insecure and carry a certain risk. Even so called "secure transactions" are not fully secure, since the information needs to be decrypted to plain text in order to process it. This is one of the points where credit card information is typically stolen.

Get wire transfer information

Some fraudsters approach merchants asking them for large quotes. After they quickly accept the merchant's quote, they ask for wire transfer information to send payment. Immediately, they use online check issuing systems as Qchex that require nothing but a working email, to produce checks that they use to pay other merchants or simply send associates to cash them.

Purchase scams

Direct solicitations

The most straightforward type of purchase scam is a buyer in another country approaching many merchants through spamming them and directly asking them if they can ship to them using credit cards to pay.

An example of such email is as follows:

From: John Bungling [bungling@hotmail.com]
Sent: Saturday, October 01, 2005 11:35 AM



Subject: International order enquiry

This is John Bungling, International Fraudster and I will like to place an order for some products in your store, But before I proceed with listing my requirements, I will like to know if you accept credit card and can ship internationally to Lagos, Nigeria. Could you get back to me with your website so as to forward you the list of my requirements as soon as possible. Regards,

Bungling Inc. 9999 street,
Muslin, Lagos 23401, Nigeria
Telephone: 234-1-99999999, Fax: 234-1-99999999, Email: XXXXXXXXXX@hotmail.com

Most likely, a few weeks or months after the merchant ships and charges the Nigerian credit card, he/she will be hit with a chargeback from the credit card processor and lose all the money.

Cash the check system

In some cases, fraudsters approach merchants and ask for large orders: \$50,000 to \$200,000, and agree to pay via wire transfer in advance. After brief negotiation, the buyers gives an excuse about the impossibility of sending a bank wire transfer. The buyer then offers to send a check, stating that the merchant can wait for the check to clear before shipping any goods. The check received, however, is a counterfeit of a check from a medium to large U.S. company. If asked, the buyer will claim that the check is money owed from the large company. The merchant deposits the check and it clears, so the goods are sent. Only later, when the larger company notices the check, will the merchant's account be debited.

Re-shippers

Re-shipping scams trick individuals or small businesses into shipping goods to countries with weak legal systems. The goods are generally paid for with stolen or fake credit cards.

Nigerian version

In the Nigerian version, the fraudsters have armies of people actively recruiting single women from western countries through chat & matchmaking sites. At some point, the criminal promises to marry the lady and come to their home country in the near future. Using some excuse the criminal asks permission of his "future wife" to ship some goods he is going to buy before he comes. As soon as the woman accepts the fraudster uses several credit cards to buy at different Internet sites simultaneously. In many cases the correct billing address of the cardholder is used, but the shipping address is the home of the unsuspecting "future wife". Around the time when the packages arrive, the criminal invents an excuse for not coming and tells his "bride" that he urgently needs to pick up most or all the packages. Since the woman has not spent any money, she sees nothing wrong and agrees. Soon after, she receives a package delivery company package with pre-printed labels that she has agreed to apply to the boxes that she already has at home. The next day, all boxes are picked up by the package delivery company and shipped to the criminal's real address (in Nigeria or elsewhere). After that day the unsuspecting victim stops receiving communications from the "future husband" because her usefulness is over. To make matters worse, in most cases the criminals were able to create accounts with the package deliverer, based on the woman's name and address. So, a week or two later, the woman receives a huge freight bill from the shipping company which she is supposed to pay because the goods were shipped from



her home. Unwittingly, the woman became the criminal re-shipper and helped him with his criminal actions.

East European version

This is a variant of the Nigerian Version, in which criminals recruit people through classified advertising. The criminals present themselves as a growing European company trying to establish a presence in the U.S. and agree to pay whatever the job applicant is looking to make, and more. The fraudsters explain to the unsuspecting victim that they will buy certain goods in the U.S. which need to be re-shipped to a final destination in Europe. When everything is agreed they start shipping goods to the re-shipper's house. The rest is similar to the Nigerian Version. Sometimes, when the criminals send the labels to be applied to the boxes, they also include a fake cheque, as payment for the re-shipper's services. By the time the cheque bounces unpaid, the boxes have been picked up already and all communication between fraudster and re-shipper has stopped.

Call tag scam

The Merchant Risk Council reported that the "call tag" scam re-emerged over the 2005 holidays and several large merchants suffered losses. Under the scheme, criminals use stolen credit card information to purchase goods online for shipment to the legitimate cardholder. When the item is shipped and the criminal receives tracking information via email, he/she calls the cardholder and falsely identifies himself as the merchant that shipped the goods, saying that the product was mistakenly shipped and asking permission to pick it up upon receipt. The criminal then arranges the pickup issuing a "call tag" with a shipping company different from the one the original merchant used. The cardholder normally doesn't notice that there is a second shipping company picking up the product, which in turn has no knowledge it is participating in a fraud scheme. The cardholder then notices a charge in his card and generates a chargeback to the unsuspecting merchant.

Business opportunity/"Work-at-Home" schemes

Fraudulent schemes often use the Internet to advertise purported business opportunities that will allow individuals to earn thousands of dollars a month in "work-at-home" ventures. These schemes typically require the individuals to pay anywhere from \$35 to several hundred dollars or more, but fail to deliver the materials or information that would be needed to make the work-at-home opportunity a potentially viable business. Often, after paying a registration fee, the applicant will be sent advice on how to place ads similar to the one that recruited him in order to recruit others, which is effectively a pyramid scheme.

Other types of work at home scams include home assembly kits. The applicant pays a fee for the kit, but after assembling and returning the item, it's rejected as sub-standard, meaning the applicant is out of pocket for the materials. Similar scams include home-working directories, medical billing, data entry at home or reading books for money.



Website scams

Click fraud

The latest scam to hit the headlines is the multi-million dollar Clickfraud which occurs when advertising network affiliates force paid views or clicks to ads on their own websites via Spyware, the affiliate is then paid a commission on the cost-per-click that was artificially generated. Affiliate programs such as Google's AdSense capability pay high commissions that drive the generation of bogus clicks. With paid clicks costing as much as \$100 and an online advertising industry worth more than \$10 Billion, this form of Internet fraud is on the increase.

International modem dialing

Many consumers connect to the Internet using a modem calling a local telephone number. Some web sites, normally containing adult content, use international dialing to trick consumers into paying to view content on their web site. Often these sites purport to be free and advertise that no credit card is needed. They then prompt the user to download a "viewer" or "dialer" to allow them to view the content. Once the program is downloaded it disconnects the computer from the Internet and proceeds to dial an international long distance or premium rate number, charging anything up to US\$7-8 per minute. An international block is recommended to prevent this, but in the U.S. and Canada, calls to the Caribbean (except Haiti) can be dialed with a "1" and a three-digit area code, so such numbers, as well as "10-10 dial-round" phone company prefixes, can circumvent an international block.

Phishing

"Phishing" is the act of attempting to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business with a real need for such information in a seemingly official electronic notification or message (most often an email, or an instant message). It is a form of social engineering attack.

The term was coined in the mid 1990s by crackers attempting to steal AOL accounts. An attacker would pose as an AOL staff member and send an instant message to a potential victim. The message would ask the victim to reveal his or her password, for instance to "verify your account" or to "confirm billing information". Once the victim gave over the password, the attacker could access the victim's account and use it for criminal purposes, such as spamming. Phishing has been widely used by fraudsters using spam messages masquerading as large banks (Citibank, Bank of America) or PayPal. These fraudsters can copy the code and graphics from legitimate websites and use them on their own sites to create legitimate-looking scam web pages. They can also link to the graphics on the legitimate sites to use on their own scam site. These pages are so well done that most people cannot tell that they have navigated to a scam site. Fraudsters will also put the text of a link to a legitimate site in an e-mail but use the source code to links to own fake site. This can be revealed by using the "view source" feature in the e-mail application to look at the destination of the link or putting the cursor over the link and looking at the code in the status bar of the browser. Although many people don't fall for it, the small percentage of people that do fall for it, multiplied by the sheer numbers of spam messages sent, presents the fraudster with a substantial incentive to keep doing it.



Pharming

Pharming is the exploitation of vulnerability in the DNS server software that allows a hacker to acquire the domain name for a site, and to redirect that website's traffic to another web site. DNS servers are the machines responsible for resolving internet names into their real addresses - the "signposts" of the internet.

If the web site receiving the traffic is a fake web site, such as a copy of a bank's website, it can be used to "phish" or steal a computer user's passwords, PIN or account number. Note that this is only possible when the original site was not SSL protected, or when the user is ignoring warnings about invalid server certificates.

For example, in January 2005, the domain name for a large New York ISP, Panix, was hijacked to a site in Australia. In 2004 a German teenager hijacked the eBay.de domain name. Secure e-mail provider Hushmail was also caught by this attack on 24th of April 2005 when the attacker rang up the domain registrar and gained enough information to redirect users to a defaced webpage.

Auction and retail schemes online

Fraudsters launch auctions on eBay or TradeMe with very low prices and no reservations especially for high priced items like watches, computers or high value collectibles. They received payment but never deliver, or deliver an item that is less valuable than the one offered, such as counterfeit, refurbished or used. Some fraudsters also create complete 'web stores' that appear to be legitimate, but they never deliver the goods. In some cases, some stores or auctioneers are legitimate but eventually they stopped shipping after cashing the customers' payments.

Sometimes fraudsters will combine phishing to hijacking legitimate member accounts on eBay, typically with very high numbers of positive feedback, and then set up a phony online store. They received payment usually via check, money-order, cash or wire transfer but never deliver the goods; then they leave the poor, unknowing eBay member to sort out the mess. In this case the fraudster collects the money while ruining the reputation of the conned eBay member and leaving a large number of people without the goods they thought they purchased.

Stock market manipulation schemes

These are also called investment schemes online. Criminals use these to try to manipulate securities prices on the market, for their personal profit. According to enforcement officials of the Securities and Exchange Commission, the 2 main methods used by these criminals are:

Avoiding Internet investment scams

The Internet allows individuals or companies to communicate with a large audience without spending a lot of time, effort, or money. Anyone can reach tens of thousands of people by building an Internet web site, posting a message on an online bulletin board, entering a discussion in a live "chat" room, or sending mass e-mails. If you want to invest wisely and steer clear of frauds, you must get the facts. The types of investment fraud seen online mirror the frauds perpetrated over the phone or through the mail. Consider all offers with skepticism.



Internet Crimes: Stealing band-width

There are many "don't steal my bandwidth" pages on the web. They are often long winded and hard for the novice or even the experienced web designer to understand. "Don't Even Think About It" is short and to the point. You will know what stealing bandwidth is in the 3 short minutes it takes you to read this page that is written without any sugar-coating at all.

What is Stealing Bandwidth?

There are many forms of bandwidth stealing on the web today. However, the bandwidth theft focusing on here is image/graphic stealing, and is the bandwidth theft that occurs most. That is when you find an image you like and you are:

1. Too cheap to have server space of your own to use -and/or-
2. Too lazy to upload the image to your own server -and/or-
3. Uneducated about the crime you are committing -or all of the above-

Crime? Yes, it is a crime. The person whose site the image is on that you are linking to for the source of the image is paying to display their image on your site.

First of all, the image belongs to them, not you. What right do you have to say; "Oh, wouldn't this look great on my site?" and just copy the image URL and use it on your site. You have no right at all. It is not your graphic. Even if it is a very common graphic, for example a bullet or an arrow, and you have seen it on many sites. The operative word here is "on." Get it? It is on a site. That site owner is paying one way or another to have that graphic displayed on the web. Perhaps they pay a monthly fee. Perhaps, they use a 'free' web service, however, they have limits on the amount of bandwidth they are allowed to use. By linking to the graphic, YOU have STOLEN from them one way or another.

Secondly, if it is an original graphic that the site owner designed them self, and you link to the source of the graphic to be displayed on your site, you are not only stealing the bandwidth, you are now plagiarizing their work too.

It seems a big culprit these days are the "community" type websites (MSN Groups & Yahoo groups are a fine examples). A person can easily set up a little web site lickety-split - and it's even faster when you link to the source of the graphics you have seen on the web & like rather than uploading them in YOUR space. Not to mention writing to the owner of the graphic and asking their permission first. People do this because it is a fast and cheap way to put something up quickly. In doing this, you are stealing!

One other area that is festering boil for bandwidth stealing are the Bulletin Boards that offer the members an ability to have a cutesy little icon next to their name. People remember that cute little picture of a dancing potato they saw on a web site and link to the image source for their member icon. Now, the site owner who's dancing potato graphic you are linking to is looking through their server logs and see 15,048 hits to this one little graphic. "What the heck," they say in disbelief! Or, they get a notice from their 'free' web site host telling them that they have



exceeded their allowable bandwidth for the month and their site will be shut off OR they have to pay extra money to keep it up.

Bottom line, if you want to use a graphic on your site, you must do these things: write to the site owner of the graphic that you would like to use on your site. •>ASK<•, repeat ASK them if you can use that graphic on your site. If they say yes, then thank them and be certain to thank them in the credits of your site. If they say no, swear a bit under your breath but under no circumstances do you link to the graphic thinking that "I'm not really using it on my site, since it is not on my server. Leave it alone and go find something else instead.

Does this text make you angry or are you grinning ear to ear? If you are feeling angry, you are one of those snatch and grab people who take what they want and say the heck with the rules. If you are smiling ear to ear, you are a site owner who is glad to see the text you have just read. It is in plain English and not sugar coated in any way. PhenomenalWomen.com understands this because so many images on this site are linked to and bandwidth stolen daily.

A warning: many site owners can track down and pinpoint exactly where their images are being used on other sites. When that happens, you will be in trouble. If you are new to the web, take the advice of this page as your first lesson and don't forget it.

Courtesy: nidokidos Moderator [nidokidos-owner@yahoogroups.com]

Humor in Uniform

A number of new Air-Force recruits were being taken on their first training flight. The plane had just leveled out after taking off when one of the engines seized up, and another began smoking badly.

Adjusting his parachute, the instructor strove for nonchalance as he made his way to the hatch door. "Now I want you men to keep perfectly calm," he said, "while I go for help."

Courtesy: Satish Kumar Poonia (skpooniam@gail.co.in)

Captain Dare Devil was known in all the seven seas for his bravery and gallant acts. Once encountering the sea pirates he shouted his Helper to prepare the 'Red Uniform' since he was keeping many colored uniforms. When battle was over and his wounds were being attended by medical staff, his Helper asked softly, "Why did you ask for red uniform my Captain?"

Replied Capt DD, "I didn't want to demoralize my troops seeing me bleeding, that's why I asked for red uniform!"

After some time there was large fleet of sea pirates swarming the ship of Capt DD. Looking at it he shouted to his Helper, "Prepare my brown uniform!"

Courtesy: Kul Bhushan Tyagi (kbtyagi@iocl.co.in)



Dates to Remember!

Certification Courses

It is for the information of security professionals that a two-day long Professional Certification Programme (Certified Facility Security Manager - CFSM) is slated on August 30-31, 2007, in New Delhi.

- Mr. D C Nath, Executive President & CEO, IISSM at nathdc@iissm.com,
Mobile: 9811995693
- Lt. Gen. Prem Sagar, Executive President (C&F), IISSM at premsagar@iissm.com
Mobile: 9899078687

Details of these courses and fees can be obtained from <http://www.iissm.com/>

Suggestions & feedback may be sent to us on e-mail: captsbtyaqi@yahoo.co.in
