INTRODUCTION

Benedine Ofomah has hit a home run! "THE SCAM GAME" is a must read for corporate aspiring executives and individuals who wants to take part in any Internet activity. In this book, Benedine combines personal encounters with fraudsters and years of experience using the Internet, and put it in an easy-to-get-it style. In fact, this is one of the best books on Internet fraud ever to be written by a man who really went through it all. It is a book I urge would be Internet user to read.

This book "THE SCAM GAME" contains eminently practical advice that will affirm, guide and direct those that are using the Internet at present and also those that are yet to use it. This book is wonderful and is a meaningful help to everyone at every rung of Internet activities.

Simply put "THE SCAM GAME" may very be the best book you will ever see on the subject of scam and Internet fraud. This book gives you in-depth information on lots of illegal activities that take place on the Internet. Benedine exposes all frauds that take place on the global community called the "INTERNET" with no exception and he left no corner unexposed.

This is a master piece of art put together by a man that have almost explore almost every nook and cranny of the internet, and this book is a result, a culmination of what he experienced during his tour of the global village called the Internet.

I highly recommend this book to every Internet user out there…….

Nkolika Mmako,
Medical Lab. Scientist,
FEDERAL MEDICAL CENTER
Abakiliki Nigeria.

BRIEF FACTS

For those who are novice to computing and Internet, they will be surprised to find out that almost any site has one or two things to say about scam and hacking. There are lots of Internet crime that include scam, hacking and lots more. Everyday, every newspaper has one of two things to say about scam and other forms of Internet fraud. Those who are now netizen (people that are regular users of the internet and know what goes on the internet) are very much aware of some of the dangers users of the Internet are exposed to, while novice Internet users assumes that there are no safe grounds like the internet. Some who have once been hit by these fraudsters now adopt to look very carefully before they leap. But they forget that you might be hit plan A and you feel you already know it, what about plan B, do you know it? These fraudsters like to sum up it up by saying the "The more you look, the less you see" meaning the more you think you know the ways they you to operate the more like it is that you will be hit. Everyday we hear stories of how people were being ripped off their life savings by Internet fraudsters. In fact, the rate at which Internet crime increases everyday calls for immediate attention and even a solution to it at least if not to eradicate it but curb it. Billion of dollars are at stake due to poor or lack of security.

With the sun rising each day, the numbers of people who are using the Internet multiple in large folds, hence a corresponding increase in the number of scammers, hackers and other type of Internet fraudsters. Due to the increase in the number of those using the internet it present a perfect ground for activities like online banking (pay pal, E-gold, Barclays), E-mail services like Yahoo, Hotmail, online stores like E-bay, Amazon and Overstock. In fact, the Internet is a global village or world; to me personally the Internet is another world within the boundaries of the Earth. That's actually one of the reasons why it is a Gold mining ground for Internet fraudsters. These issue of scam is everywhere in websites, chat rooms and forums.

Another important issue is that the Internet community believes that 50% of Internet crime is being committed by Nigerians. The Internet community has devise lots of ideas to abate and curb scam yet it all proved abortive. It is nothing new that you enter chat room today, to be precise yahoo chat room and once they find out that you are from Nigeria they call you a scammer. Search Google, Ask, and Yahoo search engines for scam and 419 or internet fraud and you will see that Nigeria ranks number one. It is common today to see people who want business partners, but will reject anyone from Nigeria from being part of their business. Personally, I have lost lots of chances of making genuine money on the Internet just because I am from the much-dreaded country Nigeria. I used to work as a freelance web designer and simple java application program, but because I am from Nigeria I hardly have any job to do. I never won any contract just because people believe that I am out there just to scam them. Nobody wants to give you a chance to prove yourself because nobody wants to be scammed, nobody believed me when I said I am not a scammer. I can remember the encounter I had with an Indian man called "TAHN." He owns a very big store in India and he needed an online store where people can place order from his website. Everything went on fine, until he asked me, "where are you from?" Once I said Nigeria that ends it all. I didn't blame the man because is only fools that hear snakes can bite and still wants to pick one with his or her bare hands. This was his reply when I said I am a Nigerian. "Oh, I am sorry this won't work once bitten twice shy." In nearly a year I have lost too many contract just because I am from Nigeria. This make me to search for the truth. That is one of the reasons why I spend time search for details that will lead me to the truth and this book contains in details all that I have found out. Before I continue I will like to say that it was shocking that Nigerians are really as bad as their counterparts from other countries said, but at the same time I want the whole Internet community to know that Nigerians can't alone be responsible for all the crimes on the Internet. One of my local proverb goes like this, "It is the home mouse that told the wild mouse that fish is in the fish basket." They must also know that their countrymen are also part of these daily Internet crime as well as Nigerians. During the course of writing this book I found out that Nigerians are not causing all these damage and havoc alone. I also found out that some Internet groups or companies don't accept Nigerians as their members. Like Paypal don't

accept Nigerian members and also lots of other websites. But the funny thing about it all is that Nigerians have verified paypal address. There are various ways by which one can be conned. In this book I will focus mainly on the various types practiced by Nigerians. Nigerians normal undertake a type of scam called e-mail scam, that's they will send you mails that you have won a lottery, gift, or about a profitable business venture and lots more. More details about their modus operandi are coming up in the upcoming chapters. Another type of e-mail scam they indulge in is the one called "NEXT OF KIN." In such mail they will tell you that they are government officials and that they want to transfer some money out of their country but need your help because the security agents are tracking their moves.

They also engage in a little bit of advance scam know as hacking of credit cards and online bank account details. People that are more likely to be attacked this kind of scam are those that own an online store and those that buy thing from online stores. Sometime ago on 2nd NOVEMBER 2004, I entered yahoo hacking chat room as part of my research for this book. I asked the member that were online then how I can get credit card details, because I needed one. Then one man by name "Abdul" who claimed to be from Egypt send me a private message that contains a forum where hackers paste people credit cards details for members to use. They also have people bank login details especially people from UK and USA. For some reasons I will not list the website here. When I visited the website, to my greatest surprise. There is more than 600 credit card details and information pasted for members to share and use. Nigerians are not really responsible for this kind of scam; I found out that people from Iran, India, and Vietnam are really responsible for all this. In fact, the web I was referred to was own by some Vietnamese. Nigerians don't normally participate in this kind of scam, because their knowledge of the Internet is limited. These kinds of scam that include hacking of credit card information and bank login details require advance and in-depth knowledge of the Internet.

So far so good, I have tried to expose to you some of the activities that take on the Internet. What I have exposed so far is just a preamble to the various forms of crime that happen on the Internet everyday. I will discuss it all in full at the due time and in the due section. My main aim of writing this book is to expose the mode of operation of these new generations of fraudsters to you the reader of this book. These fraudsters are ready to explore any loophole available to them in fact they are always applying new methods and tactics. So all I will give you here is confirm methods that will help you know when you are about to be hit and also teach you how to draw your last line of defense.

In a nutshell, I will like to say that this issue of scam is understood by only a few out of billions of people that are using the Internet everyday. There are various forms of scam and fraud ranging from hacking, bank database, shopping site database hacking, fake login page, scam mails, dos-attack, defacing of websites, hacking of e-mail password and lots more. In the next chapter I will focus on explaining and exposing various scam mail method and the type of scam that are carried out through e-mails and chat rooms. Stay tuned and don't stop reading, because you might be about to be hit or you might be the next victim.

E-mail Scam

This type of scam is the most popular type here in Nigeria. This type of scam is also one of the most popular types. It is practiced by almost 50% of Internet users in Nigeria. Almost all Internet users and non-internet users in Nigeria knows about it. But, I found out that only about 50% of Internet users here practice it, while about 30% of non-Nigerian outside are knowingly or unknowingly helping them to carry out their act. First, I will like to explain what scam mail means to those of you, who don't know what it is. Scam mails are mails sent to e-mail user by Internet fraudsters about lots of mouth watering offers. The content of such mails normally ranges from that they need a business partner in a deal that will yield lots of money, or that you have won a lottery draw, so also send mails to their prey that they run a non-governmental organization that cares for the poor and orphans. They will say that they need some money to continue their work of mercy. Some group of these scam mailers will send mails saying that they are mobile phone, laptop computers and electronic dealers in Nigeria. That they are in need of someone or company that will be supplying goods to them. Another method they use is that you have won a gift, but you need to verify it either with your credit card or by paying them some money through your bank account so they will be sure that you are the winner. They also send you a mail that you are next of kin of unclaimed money or that they want you to help them to claim assets of their client. Below are samples of such mails, that I received in my mail:

From: "BARRISTER OLA MARTINS" <abcd1@globo.com> add to Address Book Add Mobile Alert
Subject: YOUR URGENT ASSISTANCES NEEDEDE!!!*!*
Date: Sat, 10 Jun 2000 18:33:49 -0700

Pardon me for not contacting you early before sending this message. Your identity happen to match the name i have been looking for since 1996.My name is Barrister Ola Martins of the OLA MARTINS CHAMBERS.I am a Lawyer by profession. I am the principal attorney of one Mr.Heppner Michellnow deceased.

Heppner Michell was a contractor with the Federal Government of Nigeria. He executed contracts through the petroleum ministry. He executed a contract worth eighty-six million united states dollars US$16,000,000 in 1995.

He had heart ailment, which eventually lead to his death in 1996. When the payment of the contract he executed was due the Federal Government of Nigeria issued a letter to my law chamber to present His next-of-kin, this was in 1996.I wrote to the Federal Government that I am still searching for the beneficiary.

On 20th March 2006,the Federal Government sent a new message to my Law chamber that i should forward the name of the beneficiary; I did a thorough search for the next of kin but to no avail.

I have every legal documents with me that put you in place as the Next of kin. I believe you stand a better chance as the beneficiary I urge you to contact me. I have every document that will back you up as the beneficiary of US$16,000,000.
Please you can reach me with this number 234-802-0393370. I will be very glad to hear from you.
Regards,

Barrister Ola Martins.

The one below comes from someone claiming to be an agent of Economic and Financial Crime Commission. The fraudster did so, because he believe that we lessen the doubts in my mind that the deal is a scam or fraud.

"Economic and Financial Crime Commission" <scamalert@myway.com> Add to Address Book Add Mobile Alert
To: benjocyb2k@yahoo.com
Subject: OPERATION FIGHT SCAM/STOP FRAUD
Date: Fri, 28 Mar 2003 04:21:38 -0800

From: Economic and Financial Crime Commission (EFCC)
Abuja office
1 Ibrahim Taiwo road
Aso Rock Villa
FCT Abuja,
Nigeria.
Email Contact: scamalert@myway.com
TEL: 234- 1-471-3279
FAX: 234- 9-272-1973

Date: 03/07/2006.

ATTENTION: SIR/MADAM,

It has come to the knowledge of this commission (Economic and Financial Crime Commission) that some scam artists especially from Africa has been contacting you for mutual assistance that would be of benefits to both party, please ensure that if the letter sent to you includes the below features note that it is a false offer:

1). Asking you to act as the next of kin to a late deceased funds to make claim of his/her funds deposited with a security company/bank.
2). Asking you to provide your bank details to enable them transfer funds to you for safe keeping.
3). Contacting you to make claim of your lottery winnings.
4). Contacting you as the Governor of the Central Bank of Nigeria (Prof.Charles Soludo) to make claim of your inheritance funds and providing authorization if you were the one that sent someone to make claim of your funds on your behalf.
5). Contacting you as Nigeria National Petroleum Corporation (NNPC) officials or impersonating themselves as members of this commission(EFCC) contacting you to come and redeemed your funds confisticated either NDLEA or the UNMOVIC organizations and many more.

This commission (Economic and Financial Crime Commission) has been set up by the Federal Government of Nigeria to combat fraud perpetrations and stop this scam perpetrators who through one way or the other tarnishing the image of this country through fraudulents act. Our Major function is to fight and stop scams and also compensate all foreigner's who one way or the other has been retrieve from there hard earn money through illegal transactions.

The below websites can be more reference:

http://news.bbc.co.uk/2/hi/africa/4320984.stm

We wish to inform you that we are ready to work with you to ensure that these scam perpetrators are track down and prosecute to jail. Please be informed that we wish to seek for your services and we want to let you know that any service rendered to this commission, you will be duly be rewarded with the sum of US$150,000.00 but this has to be done when we receive proofs from you.
Forward to this commission all the mails you have been receiving from scam perpetrators including their email contacts and telephone/fax numbers so that we can track and prevent them from causing more damages to this nation.

Peradventure you have been a victim in this cause, kindly inform us as we are ready to refund your funds back to you.

Thanks for your understanding and we are deeply sorry for the inconveniences this has caused you all this while. You can contact us via the above email contact.

We apologies on behalf of the President and the good citizens of Nigeria for any delay and lost this most have coursed you and promise that such thing will not happen again. And if you are dealing with any one of them we urge you to STOP because you are taking a big risk.

Your co-operation will be highly appreciated in regards to this cause.

Best Regards

Donald Ekanem

Secretary
For: Economic and Financial Crime Commission (EFCC)

Note: If you think that this is genuine and you have received any scam mail, you will send the mails to them as proof, so that you will be rewarded. In the process of getting your reward they will scam you.

Below, is a mail I got from a man that claims he is looking for someone that will help him distribute his money to charity funds.

From: "Abdul Razak Kaseem" <abdul_kaseem@katamail.com> Add to Address Book Add Mobile Alert
Subject: Could you kindly assist me
Date: Tue, 02 May 2006 14:01:13 +0000

Greetings to you,

As you read this, I don't want you to feel sorry for me, because, I believe everyone will pass on someday everyone eventually has appointment with death. My name is Abdul Razak Kaseem a merchant in Dubai, in the United Arab Emirate (U.A.E).

I have been diagnosed with esophageal cancer. It has defiled all forms of medical treatment, and right now I have only about a few months to live, according to medical experts (I am in a private ward in a private hospital here in the United Kingdom). I have not particularly lived my life so well, as I never really cared for anyone (not even myself) but my business.Though I am very rich, I was never generous, I was always hostile to people and only focused on my business as that was the only thing I cared for.

But now I regret all this as I now know that there is more to life than just wanting to have or make all the money in the world. I believe when God gives me a second chance to come to this world I would live my life a different way from how I have lived it. I have willed and given most of my property and assets to my immediate and extended family members as well as a few close friends. I want God to be merciful to me and accept my soul so, I have decided to give also to charity organizations,as I want this to be one of the last good deeds I do on earth. So far, I have distributed money to some charity organizations in the U.A.E, Algeria and Malaysia. Now that my health has deteriorated so badly, I cannot do this myself anymore.

I once asked members of my family to close one of my accounts and distribute the money which I have there to charity organization in Bulgaria and Pakistan; they refused and kept the money to themselves. Hence, I do not trust them anymore, as they seem not to be contented with what I have left for them. The last of my money which no one knows of is the huge cash deposit of $18 Million Dollars that I have with a Security Company abroad. I will want you to help me collect/receive this deposit and dispatched it to charity organizations.

I'll be awaiting your quick response.

For your time and honesty, I have set aside 10% for you.

Wassallam.
Abdul Razak Kaseem.

Also, I will show you a copy of mails that I received from fake companies claiming that they are interested in a partner in USA or Canada that will be collecting payments for them and they will be paying the representative 10% of each transaction.

This message is not flagged. [Flag Message - Mark as Unread]

Date: Sun, 2 Jul 2006 00:47:40 +0100 (GMT+01:00)
From: "cheung_companyd@myway.com" <dangwung@virgilio.it> Add to Address Book Add Mobile Alert
Subject: COMPANY AGENT NEEDED

Dear friend,
It is my pleasure to write you in respect of our Company
Wujiang Wanlida Textile Co., Ltd.
No.6 The Third District Nanshan
Road,
Shengze, Wujiang City, Jiangsu
Province. China.
We are experts
in the sale of Textile materials; we export into the United States and
Canada.
We are searching for representatives who can help us establish
a medium of easily getting to our
customers in these areas as well as
making payments through you to us as our representative.
Please if you
are interested in representing us you will be entitled to ten percent
(10%)
of any payment made to you for your agent fee.
If you are
interested please send the following information below:

1.FULL NAMES:
2.RESIDENTIAL ADDRESS:
3.PHONE NUMBERS:

On our receipt of the above
contact information we shall commence our verification and your
endorsement
as our company representative in your province.
Kindly get
back to me so that i can furnish you with more details.

Kindest
Regards,
Mr.Cheung Lee
Company Director.
Wujiang Wanlida Textile Co.,
Ltd.

Printable View This message is not flagged. [Flag Message - Mark as Unread]

From: "eizo kobayashi" <info_eizo2@lycos.co.uk> Add to Address Book Add Mobile Alert
To: gtryu@yahoo.co.uk
Subject: Company Rep Needed!!!
Date: Tue, 11 Jul 2006 01:38:40 -0700

Good day,

USA/CANADA Assistant on Financial Matter

Permit an introduction. My name is Uichiro Niwa, staff of ITOCHU CORPORATION based here in Japan. Our company exports cement, sugar and textile materials for world trade. We are searching for a representatives who can help us establish a medium of getting to our customers America and Canada as well as making payments through you as our payment officer. Most of our customers pay out in check and we do not have an account in your country that will clear this money. Again, there is the problem of language. This has posed a lot of problems as we have engaged the services of interpreters which have proved not so encouraging as we have lost a lot of money to some bad characters in our employ. It is upon this note that we seek your assistance to stand in as our representative inyour country.
Note that, as our representative, you will receive 10% of whatever amount you clear for the company and the balance to be paid to us. If you are interested in this business transaction, forward to us the information below:

1)Full names :
2)Phone:
3)Cell:
4)Fax:
5)Mailing/residential address:
6)Company name:
These information should be forwarded to the President and ChiefExecutive Officer;

Mr. Eizo Kobayashi
President and Chief Executive Officer.
Thank you for your time.
ITOCHU Corporation.
Email:e.kobayshi@laposte.net

Printable View This message is not flagged. [Flag Message - Mark as Unread]

From: "Mr. Dong Bin" <godier@godier.com.cn> Add to Address Book Add Mobile Alert
Subject: INTERNATIONAL REPRESENTATIVE NEEDED
Date: Wed, 5 Jul 2006 22:42:58 +0100
To:

Dear Prospective Representative,

INTERNATIONAL REPRESENTATIVE NEEDED

We are a dynamic company specialized in providing top grade service and products to our customers. Established in 1987, Shanghai Godier Electronics Co. Ltd. Is a multi-national firm dedicated to its customers and their needs. Small size of our firm allows us to give special attention to our customers special needs. We are providing top quality LED display, electronic goods, consumer products, and speciality items into America, Canada and Europe Industrial market. The product can be applied to: Banks, Stock exchange corporation, station, billboard, etc. It is concolorous, bichrome, trichrome. And we can also develope new product according to the demand of the customer. Together with the wholeset of soft in english.

Presently, we are faced with some problems most especially with our Payment methods as most clients we have in the United States/Canada and Europe prefer to pay us with cheque rather than cash. We find it very cumbersome in accepting such payments due to the new monetary policy in our banking systems here in China and this is crippling our business. We have numerous customers in the United States/Canada and Europe, we cannot afford to loose them due to this problem.

We hereby request for your hand in partnership to act as our payment Representatives (Shanghai Godier Electronics Co. Ltd), to act as our clients who shall receive payment on our behalf from our customers in the United States and Canada and Europe. You shall be entitled to 10% of each payment you receive on our behalf and this shall be a continuous process.

Upon receipt of this requested information, we shall provide you with the necessary details of how to become our representative. For official purpose, please send your email address and acceptance via same email for further procedure.

Yours Sincerely,

Mr. Dong Bin
General Manager
Shanghai Godier Electronics Co. Ltd

Below are samples of scam mails that are looking for people they will scam through next of kin method or by asking you to help them divert some money.

This message is not flagged. [Flag Message - Mark as Unread]

From: "Mr. Peter Harrison" <peterharriston124@afs.co.uk> Add to Address Book Add Mobile Alert
Subject: JOINT FINANCIAL MANGEMENT PARTNERSHIP
Date: Sat, 8 Jul 2006 02:55:16 +0100
To:

JOINT FINANCIAL MANGEMENT PARTNERSHIP

Attention: Sir/Madam,

We are a private finance and investment firm based in London England. Our primary aim is to secure our clients funds and to ensure that it is wisely invested in safe and non-speculative projects that would yield maximum returns and less tax. In all instances, most of our clients may request some confidentially especially if they are serving or retired public servants as is the case with this client of ours. Mr. Hatem Kamil Abdul Fatah who was assassinated in Baghdad. He died without any WILL and till date nobody has valued twenty-six million, five hundred thousand ($26.5m) United State Dollars approximately 14,910.302.77 GBP

The website below is a verification of the news about his death, unfortunately this man has no WILL as to his inheritance in London, United Kingdom. I have made every effort to trace his relatives over the internet and locate any member of his family but no avail.

http://news.bbc.co.uk/go/pr/fr/-/1/hi/world/middle_east/3970619.stm
http://www.uslaboragainstwar.org/article.phd?id=6979

The security/financial company have issued a notice of claim for the next of kin to come forward or the deposit is reverted to the state. I have been unsuccessful in locating the relatives for over two years thus seek your consent to present you as next of kin, so that the proceed of this account can be paid to you, for us to share. All necessary documents to back up the claims as next of kin on your behalf will be processed by an attorney through the probate office here in London, I guarantee that this will be executed under a legitimate arrangement that will protect you.

Please do get back to me via same email to enable us discuss further on how to process the claim. I wait to hear from you urgently.

Regards
Mr. Peter Harrison

This message is not flagged. [Flag Message - Mark as Unread]

Date: Thu, 6 Jul 2006 01:38:31 +0100 (GMT+01:00)
From: "Francis Eze" <franciseze001cbn@virgilio.it> Add to Address Book Add Mobile Alert
Subject: re:

DEAR FRIEND,

I KNOW THIS WILL COME TO YOU AS A SURPRISE BECAUSE YOU
DO NOT KNOW ME. I AM MR. FRANCIS EZE, I WORK IN THE CENTRAL BANK OF
NIGERIA, PACKAGING AND COURIER DEPT.

DURING THE AIR-LIFT OF SOME
PRESIDENTIAL LUGAGES TO EUROPE, I AND MY COLLEAGUES IN THE ABOVE
DEPARTMENT UNANIMOUSLY DECIDED TO INCLUDE ADDITIONAL LUGAGE CONTAINING
$15M (FIFTEEN MILLION USD) ONLY FOR OUR OWN BENEFIT THOUGH IT WAS
LABELED "PHOTOGRAPHIC EQUIPMENT" FOR SECURITY REASONS.

I AM OBLIGED
TO CONTACT YOU TO ASSIST US IN GETTING THIS LUGAGE CLEARED AND
DELIVERED TO YOU FROM THE AGENT AS WE HAVE AGREED ON THE FOLLOWING
TERMS.
(1) ALL RELEVANT DOCUMENTS TO CLAIM THIS LUGAGE WILL BE PROCURED
IN YOUR NAME TO ENABLE THE AGENT CLEAR AND DELIVER SAME TO YOUR MAILING
ADDRESS.
(2) THAT YOU WILL BE ENTITLED TO A SHARE OF 25% OF THE TOTAL
MONEY.
(3) THAT 5% OF THE TOTAL MONEY WILL BE SET ASIDE FOR SUNDRY
EXPENSES.
(4) THAT 70% OF THE TOTAL MONEY WILL BE FOR I AND MY
COLLEAGUES.

IF THIS BUSINESS TRANSACTION / TERMS IS OK BY YOU, YOU
CAN CALL ME ON MY PRIVATE TELEPHONE NUMBER: 234-1-7901564 OR E-MAIL ME
AT THE ABOVE EMAIL ADDRESS OR, franeze006_cbn@yahoo.co.in ALSO, FURNISH
ME WITH YOUR FULL NAMES, MAILING ADDRESS, YOUR PERSONAL TELEPHONE / FAX
NUMBERS FOR EASIER COMMUNICATION AND ONWARD TRANSFER TO THE AGENT IN
EUROPE.

NOTE THAT THIS BUSINESS TRANSACTION IS 100% RISK FREE AS ALL
RELEVANT DOCUMENTS TO BACK UP THE CLAIM OF THE LUGAGE WILL BE PROVIDED
FOR YOU HENCE WE ADVICE YOU TO KEEP THE ENTIRE TRANSACTION CLOSE TO
YOURSELF UNTIL YOU MUST HAVE RECEIVED THE LUGAGE. FOR SECURITY REASONS
OTHER MODALITIES WILL BE DISCUSSED AS SOON AS YOU GET BACK TO ME.

YOURS FAITHFULLY,

MR. FRANCIS EZE
COURIER DEPARTMENT (CBN)

Another scam mail I will show you are that of lottery scam mail and what it looks like.

message is not flagged. [Flag Message - Mark as Unread]

Date: Fri, 14 Jul 2006 19:16:59 -0600
Subject: !!Congratulation From MicroSoft Word 2006!!
From: "mswpromotion_07" <mswpromotion_07@terra.com.mx> Add to Address Book Add Mobile Alert
To:

MICROSOFT MEGA JACKPOT LOTTERY
UNITED KINGDOM. LONDON.
BANK OF ENGLAND/MICROSOFT HOUSE, LONDON.
Director: MR. Andrew Gregry III

REF NO: M154S/WL04.
MICRO (LOTTERY) CHIP NO: 9465021

ELECTRONIC MAIL AWARD PROMOTION. MICROSOFT MEGA JACKPOT LOTTERY UNITED KINGDOM.

Finally today, we announce the winners of the MICROSOFT MEGA JACKPOT LOTTO WINNINGS PROGRAMS held on 12th, JULY 2006. Your company or your personal e-mail address, won in the second lottery category 002.

You are therefore been approved for lump sums pay out of £5,500,000.00 FIVE MILLION, FIVE HUNDRED THOUSAND POUNDS. Equivalent to ($10,064,000 USD) Ten Million, sixty four thousand US Dollars. In cash Credited to file REF NO: M154S/WL04. and MICRO (LOTTERY) CHIP NO: 9465021, You are the second lucky winner of the total winners of 10. You all won £5.5, million Pounds each.

All the 10 participants were selected through our Microsoft computer ballot system (MCBS) drawn from each continent, as part of International "E-MAIL" Promotions Program, to promote the use of emails all over the World, and to promote the use of Microsoft Office. Your funds (certified Cashiers cheque) have been insured with your REF NO: M154S/WL04. To claim your winning prize (£5.5, million pounds), you must first, contact the claims department by email for Processing and remittance of your prize money to you. The claims processor is:

Name: Mr. HARRY PETERSON.
E-mail: claimsdepartment_007@yahoo.co.uk

Do email the above email address at once with all the claims requirements below. In order to avoid unnecessary delays and complications. Also you will fine below the Microsoft Delivery Option's to choose only one preferable to you for proper delivery or transfer of your winning cheque.

Claims Requirements:

1.full Name:.....
2.Address:.....
3.Nationality:.....

4.Age:.....Date of Birth:.....
5.Occupation:.....
6.Phone:.....Phone 2:.....Fax:.....
7.State of Origin:.....Country:.....

DELIVERY OPTION'S:

(A) BANK ACTIVATION OPTION: This option requires you to activate an account with our official paying Bank where your funds will be deposited and then transferred to your local account, the minimum of their activation fee is GB 1, 500 pounds,

(B) COURIER OPTION: They will deliver your parcel to you at your requested destination after taking care of their delivery charges, and the minimum of their delivery charges is GB 450,00 pounds, depense on how fast you may like them to deliver your parcel to you.

NOTE: you are responsible for any charges required in any of the options, you may like to use, as your winning cheque has been insured to it's real value and no body has the ordersity to touch neither to deduct from your winnings. All documents covering your winnings are very much available for you if required.

Sincerely,

Secretary
Mr. Lesley Kenneth Jr.

NOTE: Do not reply this mail. You are to contact your claims processor immediately by email. If you have any difficulties call the promotion director Mr. Andrew Gregry on PHONE # :+44-7040101161.
This promo is all about emails, be aware.

WARNING!!!
ANY MAIL RECIEVED OF THIS SUCH WITH ANY OTHER TRADE MARK OR ADDRESS SHOULD BE FOWARDED TO YOUR CLAIMS AGENT IMMEDIATELY; THIS WILL HELP US TO FIGHT SCAM AND LOTTERY IMPOSTERS. THANK YOU FOR YOUR ANTICIPATED CO-OPERATION.

Those who think that they can't be hit will be wondering how they eventually they got hit by any of the above listed methods. I will now show you how it all goes. Internet fraud comes in different forms and sizes. Some can be scammed as low as $100.00. I will now analyze each of the mails I showed you above. I will start with the first scam mail. He claimed to be an attorney that is searching for a next of kin for his client that did a project for the Nigerian government. I decided to contact him, so that I will get details for this book, and not because I am interested in his deal. Immediately, I received the mail, I know it is scam. He told me that he has all the necessary documents and that all I need to do is to stand in as the next of kin and that the federal government said, "The next of kin should pay the sum of $10,000 for verification." He said, I should compare the verification fee with the amount I will inherit. ($16,000,000). That was the last time I mailed or contacted him, because I was thorough convinced that he was about to scam me. Beside, how can out of the whole Internet user, he found out that I am the person that stands the chance of being the next of kin?

Next is that of a man by name Donald that claimed he works for the anti-fraud commission in Nigeria. He claimed to be a member of the Nigerian Economic and Financial Fraud Commission. He did so, because he wants you to believe that he is from the commission and as such be ready to do what ever he told you. I contacted him and send to him those scam mails that I have been receiving. He mailed me back and said that they have catch up with one of the culprits and that what I claimed was true and to receive my reward of $150,000 that I should send my bank account number to them. They also send me pictures of the culprit they claimed they caught. I did mail a fake acct number to them, because I know it is fraud. Next, I received a mail from a man purported to be their bank representative. He said that, he received directives from their customer "EFCC" that the sum of $150,000 should be paid in to my account. He said that, I need to pay a transfer fee of $2,500.00 only before I will finally receive the money. As you can see, if you are under the illusion that you are dealing with someone from Economic and Financial Fraud Commission, you will rush and pay in the transfer fee and you have been scammed.

Next, is the one I received from a man that claims he wants to distribute his money to charity organizations. This one has two ways of attracting you, either you will want to genuinely help him use the money for charity work. Or you might want to get the money from him and use it for your own use. If the last option is what motivated your interest, you will end up being scammed in the process of trying to scam someone. I mailed him back and the man never replied my mail, because I told him that he is looking for people to part from their savings.

As for those seeking for sales representative, what they do is to send a false check to your home address, which you used to verify your identity. Then, you will go to your bank and cash the check and collect your 10% and send the rest to them. After, some days you will receive a letter or phone call from your bank that the sum of the amount you cashed has been deducted from your account balance. I am not denying the chance that some of such offers can be genuine. The best way to avoid been hit is to cash the check and hold the money until you have been cleared by your bank.

Ways you can avoid been hit by lottery scam mail is to ask yourself this question;
Did I enter in to any lottery, if yes then is it from that same company, if no then run as fast as you can. As you noticed from the above mails, some contains web links to support the story and make it look real. As you can see the lottery scam mail has the option of paying in some money in to a local account so as to prove that you are the winner. That goes to show you that they have partners outside the country, who they will use their bank account for the deal. And what they normally do is once their partner over there receives the money; he will withdraw it and freeze the account. He will now send his partner where he is his own share through Money Transfers like Western Union or Money Gram.

E-mail scam Part II:

One day, I logged in to my mail box and I found a mail from a man that say he needs someone or a company to supply 1,500 pieces of laptop set to his company in Nigeria, but that he the owner resides in UK. Since, I am an affiliate sale man of laptopshop.co.uk then, I was so happy, because I will get a huge commission if the deal for sales of 1,500 computer set goes through. I mailed the man back and told him that each laptop will cost him $750.00, so the total quantity he needs will cost him $1,250,000. Below is the mail I sent to the man.

Dear Sir,

I received you mail that you need 1,500 piece of laptop computer shipped to your company in Nigeria. Fortunately, I happen to be a laptop salesman. The normal price for each laptop is $850, but since you are buying large quantity. My company and I have decided to give you $100 discount each. It is expected that you pay up ¾ of the total amount and to complete payment upon reception of the laptops. Methods of payment available are Checks, Money Order and Bank Wire or Bank transfer.

I am expecting your feedback.

Yours faithfully,
Benedine J. Ofomah

Later in the day, I received a mail from the man that he wants to make complete payment for the goods. He said, I should give him the bank account detail that is needed for the payment through bank wire. I was stunned, because of his trust on me. Below is his reply.

Dear benedine,

I got your message and I was so happy that you responded immediately. I am okay with your business terms. I want to let you know that I will make complete payment for the laptops, before shipment. Also, I want you to send me the details of the bank account, which the money will be transferred to.

Hoping to hear from you as soon as possible.

Yours sincerely,
Akia Desta.

I was happy, thinking that I have struck a very profitable business deal. I called his UK phone number, which he gave me and it went through. So, we discussed about the bank account details and shipping address. We agreed that I will pay for the shipping bills and he told me that his bank would contact me on Monday, because that was on a Saturday. I completely believe that the man is for real, because I thought if he were to be in Nigeria, how come I can get him with a UK based phone number. On Monday, I checked my account balance and yet nothing showed up. So, I decided to mail him about the latest development. I logged in to my mail address to mail him and I saw a mail purported to be from First Bank Nigeria, plc. Below is a copy of the mail I received from the same man under the disguise that it is from his bank.

Dear benedine,

I am Mr. John Egwu, the senior accountant of first bank Nigeria, p.l.c Lagos branch.

One of our customers, by name Mr. Akia Desta, ordered that the sum of $1,125,000 be paid in to your account.
Acct #: *********
Bank Name:********
I will like to notify you that, before we make such transaction. It is required that you pay transfer fee of total sum of $2,000 in to the account number and bank below.
Acct #: ********
Bank name: First bank Nigeria, plc.

Hopefully, we will make the transfer, once you pay the transfer fee. We will deposit the total sum of $1,125,000 in to your account.

Yours faithfully,
John Egwu
Senior accountant,
First bank, Nigeria.
Phone number: 0802678**

Immediately, I got this message. I develop this feeling that I am about to be hit. But, I was a bit confused about his UK phone number. Then, I said to myself, it is possible that he have partners over there and besides they sell UK coded Phone Cards here which will allow you to receive call under the disguise that your phone number is UK based, but you can't make calls. Then again, I said to myself, how can a big company like first bank be using yahoo mail? They are big enough to have their own e-mail server. Their mail address should have be similar to stuffs like enquiry@firstbanknigeria.com, customercare@firstbank.com and not firstbankplc@yahoo.com, or any other web based mail service provider like @aol.com, @gmail, @myway.com and @anyname.zzn.com. Then I said, even if those assumptions were wrong, why must I be the one to pay the transfer fee. If their customers want to pay someone, they should be the one to pay for any transfer fee and not the recipient.

On 17th December 2005 I received a mail that I have won a lottery. In the message, I was told that I have won a lottery. I didn't reply the message. I later received another mail from them, that I should pay a remittance fee of $250. as you can see this scam mailers comes in different sizes. $250, might be small to you, but think about millions of people out there that also received the mail. Lets assume 10,000 people complied and paid the $250. That will amount to $2,500,000. I also received a mail from purported to be from Exxon mobile, which says that they are looking for representatives and any interested individual should pay the sum of £200, a foolish person, might think that by avoiding Nigerians that they will be safe. I want you to know that they are networked and distributed all over the world. They have partners and associates. Sometimes, they will first try to holla at you, saying, "I hope you are not one of these Nigerian criminals and scam mailers" once; some tells you these then believe that he is a scam mailer himself. Some will be foolish to make payments to any other country once it is

not to Nigeria, forgetting that a Nigerian scammer has a partner over there that will collect the money and pay him his own share. Don't ask for documents to prove that what the scammer is saying is true, because they are ready to do anything just to get what they want. They can easily provide you with false documents. Don't ever pay any of body that requested that you them through western union or money gram to claim your goods, these companies are mainly for sending money to friends and relatives or someone you trust, because if you got scammed by making payment through western union. There are little chances that the perpetrator will be traced.

One day, I went in to a cyber café to browse and it turned out that 2 young men besides me are Internet fraudsters. They are planning how they will scam a Japanese accountant. One of them called, "Slow Ice" said that the Japanese accountant said he will make payment once it is not to Nigerian bank or to anyone in Nigeria. I don't know the way they used to scam the man, but he was foolish to tell them such things. They now said they will call their partners in USA, Europe or other African countries and highlight them about the deal. They told the man to choose any part of the world where he wants to make the payment. They said that the man believed that they are for real, because they have partners all round the world.

Another hunting ground for these scammer and 419er's are online chat room. These fraudsters will log in to chat rooms and lay in wait for their prey. They will start post messages like, do you need a car, a house, we are in need of fund to complete our church and stuffs like that. They will keep posting about fake lucrative business. On 9th August, 2006, I disguised as a British young business man and entered yahoo Business and finance room. A fellow Nigerian was seeking for someone to supply latest desktop computer to him. I sent him a private message that I am a UK merchant that deals on stuffs like that. He said, he needed about 14 piece of Pentium IV computers. I asked him the payment method, he will use. He said, credit card. Credit card is consider as an something made only for the elites in Nigeria. He sent the billing information of the card to me and immediately I know he was looking for someone that will help him use someone's credit card to buy computers. Some people who are unaware of the possibility of such things happening will in the end, unknowingly help these fraudsters. Another method is to parade their selves as auto sellers in chat rooms. I will narrate to you my encounters with one fellow Nigerian guy. He sent me private message and below is the conversation I had with him.

Fraudster: hi,
Me: hi too, how are u?
Me: asl (meaning age, sex, and location)
Fraudster: 25, male, Nigeria
Me: me too,
Fraudster: I am a Nigerian, but I resides in Germany.
Me: so, what do you do there and you name mine is benedine.
Fraudster: well, I sell auto's here in Germany,
Fraudster: do you need a car?
Me: no, not now.
Fraudster: I can help you, buy one and I guarantee you free shipping. You won't have to pay for anything.

I was very hungry then, so I decided to buy some snacks and soft drinks to cool my nerves. I passed a section of the café and I saw the guy who was claiming to be an auto dealer in Germany. The conversation I had with him was hanging on his screen. I walked up to him and said, I thought you were in Germany and he said, "Bro, wetin you want make I do, any how, any how, we must survive! (meaning Brother, what do you want me to do, either by the hook or crook I must survive!)

I told him, "Bro, I need your help, I am writing a book about internet crime and fraud. I need you to give me details. He decided to help me. So, I asked him. How do you expect to hit a maga (what they call their victims or potential prey.) by acting as an auto dealer in Germany? He said, " well I have partners in Germany, and if the deal turns out well. I will ask him to make payment to my partner in Germany and once my partner receives the money.

He will send me my own share." Then he said, " The maga will be fast in making the payment, since it will made to a German bank." He also said, "I told you that I am from Nigeria, because you are from Nigeria too. So you can trust me as a fellow Nigerian and make the payment. I always tell foreigners that I am from Germany and if they ask for my contact information and phone number, I gave them my friends information." I always send him details of latest developments, so that he will know how to handle the maga if they decide to call or contact him. I asked him, "can you read or write German language." He said, " guy, u no go understand, abi online translators no de again." Meaning, you wont understand, I use online translators.

Another day, I entered yahoo chat room and I met a lady. She said, she works for Barclay's bank in Amsterdam, that she owns a very large plaza where she sells mobile phones, laptops and other complex electronic gadgets. She said that his store is experiencing a decline in sales that she needs a reliable sale partner in Africa. At that time, I was running an online store formally known as www.megaplazaonline.com (it is no longer functioning now) So I was interested in her business offer. We discussed about the partnership at length and finally I told her that for a start. She should just send 200 pieces of mobile phones. She sent me her picture. She also sent me a form and asked me to complete the form and mail it back to him. The form contains fields like my name, address, phone number and other things. She told me to check my mail morrow for her feedback. I checked my mail the next morning; I didn't receive any message from her. Later in the day, I checked again and I saw her mail. In the message, she said that she is traveling to London for a very important meeting, that is should call him with this phone number +44 0703**8**

We agreed on 200 pieces, but she said she would be sending 500 pieces. We also agreed that the shipment since it is small would be through FedEx courier service or DHL Company. She now told me that he couldn't use any of the companies we agreed on earlier. She said that she will be using one courier service that I have never heard about that based in Abuja (Nigerian federal capital). She gave me their phone number and said I should call them for procedures on how to claim those goods. I did call them and they said, I should come to their office in Abuja or that I should send some money to them for processing the stuff. They gave me the account number that I should pay in the money. I asked them for their address in Abuja and I called my cousin living there and told him to trail the address and found out if there is any courier service like that. He later said, there is, but that they don't do international services. I called the number, the number they gave me and told them why I learnt and that was the last time, they picked my call. Fortunately, for me I went to cyber café that even to browse and it turned out that Mrs. Frank, the name of the purported lady, was online. I told him that the company does not offer international service and that they said I should pay. She said, "Just pay the custom duties and after selling, deduct it from the proceeds." I decided to track the lady and found out her true identity. I used a software know as Magic logger, which enables you to login in and use as many yahoo id as you with easy. I used another mail id to chat him and it turned out, that the purported lady is a male, 25 years of age living in Abuja. I first told her that I am from UK and that I am looking for a male that will help me to organize my business in Nigeria. You know they love such deals. I told him, I have been to Nigeria twice. I then asked him to give me his phone number, so that when ever I come to Nigeria. I will give him a call. He gave me exactly the same number as that of the people he claimed were his courier agents.

Sometimes, they will try to tell you stories of how they have been cheated in the past. They do so, so that they will clear the least of feeling in you that they are fraudsters. Anybody that tells you stories of how he or she has once been scammed is a scammer himself. Anybody that didn't adhere to the initial agreement is a fraudster. They are ever changing their stand. They will agree to whatever you say at the initial stage just to draw you attention. As time goes on, they will try to change what they proposed initially in order to scam you. You can see that from the examples I gave you above. They always change to what you two agreed to. Again, don't believe any mail purported to be from a bank or other big organization that are using web based mail provider like @yahoo.com, @hotmail.com and @gmail.com, @katamail.com and others.

Never you under-estimate the strength of these fraudsters or how far they can go just to scam you. A group of about 3-4 smart guys are always working on how to snatch your money from you. They are not only smart, but also networked. I heard of a group called "SQUAD." They were scamming one foreign church that wants to build an extension here in Nigeria. First, they asked for 15,000 euro. They said the money would be use to buy land and for starting the building. They received the money, after a month, the church asked them for reports of how far they have gone with the project. They said that they have made all the necessary arrangements and that they have put necessary structures on ground. They said that they need 25,000 euros to complete the whole project. The church headquarters requested for the pictures of latest developments. Guess what they did? They went to a building under construction and sent it to the church building as they are setting up. They also took a picture of a clergyman (without his knowledge) saying that this is the clergy managing the church. They also said that so far they have been able to convert 300 people. In the end, I didn't know if, they received the money they asked for. From the above example, you can see how far they can go, just to get what they want. In fact, their motto is "NO RISK, NO REWARD."

You might be wondering how they get people's e-mail address. E-mail users are increasing everyday, so it presents very good marketing tools for Internet marketer. Some web sites sell e-mail addresses of people. These scammers either buy from other or use search engines to search for these e-mail address. They use keywords such as "e-mail address" of top richest men.

In this chapter, I explore and expose "some" of the method used by scam mailers to catch and hit their victims. These methods are just few out of the various methods they use. In fact, methods used by these scammers are evolving everyday. There are no particular methods they use. They are just exploring every chance. In the next chapters, I expose other various methods, apart from sending mails to their victim.

WEBSITE SCAM

The major aspect of the Internet that leads to it enormous popularity is the World Wide Web (www), which is a network of static and dynamic documents including texts, sounds, images and lots of other things. Many activities go on in the Internet today as a result of websites and web pages. There are lots of websites for various activities like gambling, online shopping, online banking, online auction, and lots more. In fact, with the introduction of websites the Internet became more popular than before. Almost every activity that takes place offline (that's outside the internet) can now take place in the Internet as a result of web pages. Since those activities take place online there are no physical contacts and there are bound to be frauds and scam. Most Internet crime is carried out by the use of websites. There are genuine website for any particular online activity as well as fake websites for that particular activity. Those fake websites were been set up just to scam and con people. I will now give you my personal encounter with one HYIP (high yield investment program for more details about HYIP please refer to my book FORMULA FOR RICHES) program.

On 17th March 2006, I received a message from Factory-HYIP that they have set-up a website where members can now invest and earn some certain percentage of their principal deposit daily. At that point in time I was searching for HYIP program to invest in, but since I didn't trust the program. I invested just $20 for a start because that's the minimum amount. After I deposited that $20 in their account nothing showed up in my factory-HYIP account and even till date, my balance is still $0.00. Immediately after making the payment I said to myself, "I have just been hit!" I also wonder how many people out there that has been hit by the same website. You might say that $20 is a little amount of money but think about many people that might been hit maybe more than $20 or less, besides $20 can feed a single individual in Nigeria for about two weeks. Lets assume that everybody that was hit deposited $20 and 10,000 people out of millions if not billions of people that use the Internet, that sums up to $20 x 10,000 that gives you $200,000. I hope you can now see for yourself the damages these fraudster causes in the Internet. Also remember that some will deposit more than the minimum, which is $20 dollars. Whenever you receive such an offer from unknown people please ignore it and if you feel it is true don't ever put in more than you can afford to lose. I can afford to lose that $20 and that why I invested it in an unknown program.

Some people today are making wrong use of their knowledge; they build up websites just to scam and fraud people. When I set-up my website www.megaplazaonline.com, one of these fraudsters approached me and said, "Ben, why not use this site as a shopping site for various electronics or even cars." I said to him, "well that's a very good idea, but I don't have any electronics or cars to sell in that site." Then he said, "You are stupid, just design the web with pictures of product you are willing to sell and advertise once people make payment for the goods. They will get nothing, but you will get the money." I refused to heed to his advice. He started pressurizing me to give him access to the web so that he will use it for scam and share the returns with me. I refused to do that too and that ends it all. Some shopping websites are not really selling those products that they claim to sell. They are just looking for means to rip-off and make people lose their money. I just want to you to know that for any genuine website out there, there are ones set-up to deceive those that are not aware of it.

On 23rd October 2005, I went into one cyber café (a building full of computers with internet access, where people can come, check, read, and send mails and also carry out other form of activities) to check my e-mail box and also as part of my research for this book. I normally go to cyber cafes because that's the office of these Internet fraudsters. Cyber café serves as their office where they perpetuate their evil act. On that particular day it turned out that the man next to me was designing website that will be similar to PAYPAL, E-GOLD, ALERTPAY, and others. The website will be providing online banking service to members that deposited their money with them. The website looks so real that if you are not aware of crimes and frauds that happen on the Internet. You will be tempted to deposit your money their. One funny thing about this website is that they accept deposit through western union and the payment is to be made to USA and CANADA. They claimed that that's where their offices are, but actually it is their partners in USA and CANADA that are going to collect the money. This was to clear your mind of anything that will make them appear as scam.

Once their partner in those countries received the money, they will update your account balance to the real value. The problem is that once you deposit money you can no longer withdraw it. If you ask for withdraw the admin will keep telling you stories until you give up. Besides, there is no way you can catch them. The real people that con you were not even in where they claimed to be. Since the payment is not to be paid to someone in Nigeria or any other country well known for scam, someone might be tempted to make some deposit. The person might think that he is making the deposit to the company in USA or CANADA without knowing that once their partners over there receives the money he or she will send their Nigerian counterpart his own share.

The factory-HYIP I mentioned above would have got more money from me, if I have seen my deposit correspond to the amount I deposited. So the best way out is to always try out new programs with amounts that you can afford to lose and try to withdraw to see if you will get your money back. I will talk more on how to avoid been hit in the chapter "HOW TO DRAW YOUR LINE OF DEFENCE." Another hunting ground for these fraudsters is auction websites, these are websites where members can display goods they want to sell and other members will bid on it and after a required period of time, the seller will now sell it to any bidder he likes. Some of the sellers are not real selling those products. What they do is to display the products and once they receive the payment for those products from the buyer that ends it. The buyers will never get those products that he or she requested for. The best way out of this kind of trouble is to always buy from people with reviews and ratings from their previous buyers. You can also be on the save side by buying from auction websites that uses ESCROW payment method (ESCROW is the system of payment whereby the buyer will pay the seller and the website that organizes the whole stuff will deposit the payment to the seller account, but he will not use it until the buyer confirms that he or she has received the product. More on this on the chapter where I will focus on how to avoid scam). One day, I went into a cyber café and I found one young man who was busy collecting pictures of exotic and exquisite cars and laptops. After collecting the pictures he will paste them at EBAY auction site. He said that he accepts payment through PAYPAL or western union as the only method of payment available. After about thirty minutes of pasting those pictures, he received a mail that someone has just placed a bid on the car. He wanted to sell the car at $250,000. It unfortunate that the person who bid on the car and those who are yet to do so on the cars and the laptops didn't know that they were bidding on how to lose their money. Once again, his partner in CANADA will collect the Western Union payment just to confuse the bidders, because if it were to be made to Nigeria then no one will ever make the payment.

Another hunting ground is yahoo Autos, this is the section of yahoo where sellers can display and sell their cars. I found out that this yahoo autos can be use to scam people when I saw one young man uploading pictures of expensive cars that he has in stock to the yahoo auto website. I don't really need to know about this man mode of operation, but all I know is that he don't even have a car, he was just looking for people to rip-off their life savings. The price tag for one of the cars is $30,000. An average worker here in Nigerian can't even such amount of money in a year let alone this young man I am talking about. He can't even buy any of the cars he claimed he was selling. Another type of Internet fraud I will like to expose in this chapter is that fraud that takes place in freelancing websites. I had this personal experience when I was working as a freelancer at GETAFREELANCER and GETACODER. I was only paid for just a few of the projects I did. I hardly won any project because I am a Nigerian. Whenever I do have one it is always from people looking for those to scam. Immediately I started using those companies ESCROW method I was relieved from this ugly trend. I decided to accept any project that was given to me and to work on any project after I have received confirmation letter from the freelancing company that the owner of the project has already escrow some part if not all of the money. Also if you are the owner of the project I recommend that you pay the service provider through escrow method because service providers too can run away with your money once you make payment before they finish the job. ESCROW method is very good, because either of the two parties involve can't cheat each other. If after completion of the project and you send the project to the owner and he refuses to ask the freelancing company to release the money from the escrow account to you can contact the ADMIN of the company and also attach

I worked as a freelance website designer, simple java application developer and also as an Internet marketer. I won a contract to design www.netbookonline.com (for the owner then, you have to know that domain names can be resell.) he wanted to be selling e-books at the site. He claimed to be Singaporean, when I asked him to make the escrow payment first, before I start his website. He told me that his mother is suffering from kidney disease. He told me he would pay up once he earns money from the sales of the e-books. After the completion of the project, I submitted the website files to the man and he cut off all contact with me. Till date he still owns me $350, I suspected the man to be a fraudster before the completion of the project. When I asked the man the kind of book he will be selling at the website he said he will be selling web designing books and Internet marketing books. I asked myself, "if this man is actually selling real e-books on website designing and Internet marketing how come he is looking for someone to design the website and market the e-books for him. Another encounter is the one I had with an auto surf website owner. He gave me the task of find and error that exist in his PHP website script and he promised to pay me $70 if I could find the errors and fix them with in an hour. I did that but in the end the man refused to pay up.

So far I have tried to expose all sorts of scam and fraud that takes place on the Internet. I have spent time giving you my personal encounter with these fraudsters. I have only give you little and insufficient tips on how to avoid being hit. In the next upcoming chapter, I will focus on scam and frauds that happens in shopping websites, online stores and shopping malls.

SHOPPING SITE SCAM

In the beginning of this book, I promise you that I will expose and unveil any method and means of hacking and scam known to me to you. So far, I have being able to that and in this chapter, I will focus on the type of scam that takes place in online stores. Millions of dollars are at stake due to poor or inadequate security measures. Thousands of people have their credit card information stolen everyday. Online shopping websites that accepts credit cards are another perfect ground for these fraudsters. These shopping websites are used as hunting ground because of poor security measures in their system.

I once came in contact with one of these fraudsters from Vietnam, he promise to teach me how to hack into database of shopping website and get credit cards information. He said, "I will teach you how to hack credit cards information from database with security loopholes, but you will have to pay me $600." Since I didn't pay up, he decided to cut off all contacts with me, but before then I have been able to get some important from him. He said, "Any website with database error can be attacked. The error is a result of mistake made by the database programmer. One of the most popular database error is called MYSQL injection error." This error is not the fault of the owner of the online store, but that of the website designer that made one or two mistakes in the coding of the site. The name of the Vietnamese man is PHLONG, he told me that any website with MYSQL injection error or any other form of database error can be attacked. I probed him further to know how the attack can be done, but he refused to tell me. Then I started on my own to learn how to identify websites with this error and also how it can be attacked. When you enter your credit card information in some shopping websites, the information is moved to their database where the shop Administrator will now view your order, payment information and the process them. When a website has a database error that makes those information stored in the database vulnerable and prone to attack by hackers and fraudsters. Once the database is prone to attack these fraudsters can now attack and steal credit card information of those that have buy anything from that website. I found out that stores that let independent credit card payment processing companies like PAYPAL, ALERTPAY, and lot more are less likely to have this kind of problem, because these companies provide them with secured and encrypted payment system. I also found out that Indian shopping websites are more likely to have these errors than others. I was busy searching for websites that have this error and that can be attacked and I found one. I met a man that gave me a web link that contains more than 300 credit card information that belonged to people and where stolen by hackers. For some security reasons I will not list the web here. I advise that you take the following steps before using your credit card information in any online shopping store.

1)Enter the main website url like www.domain.com

2)Then click on any leads to registration page, login page or order page or any page that interacts with the database using the information you provide. You can also use the search form. In the address bar or place where you type webs you want to visit. Type www.thewebname.com/login.asp?user=123' 0r 1=1 then press enter.

If the database has an error or is vulnerable to MYSQL injection attack, the web page will display an error message that might be something like, an error has occurred, you are trying to convert a string in to integer or vice versa. Another type of web site related scam is what is called phishing, but I prefer to call it fake login page or link. The name alone must have given you a feel of what it is. This is a very deadly form of scam especially Internet newbies. During my research for this book, I found out how these scammers use to generate fake pages and use it to confuse and scam their victims. Below are the steps they take.

1) They create replica of the web pages that are found in the original site. This is very is to do. They simply save the web pages, which will also save the logo, banner and other picture that are found in the site. Or those of them with very good knowledge of web designing can view the source code and re-edit it to match their ambition.

2) They will code up their own script and replace it with the one that handles the login. <form action= "their script url" method= "post"> other form elements</form> the function of the original script is to transmit your login details to the back-end database and process it to found out if you are an authorized user. When they replace it with theirs, they will code their own so that it will e-mail to them your login information instead of logging you in to your account.

3) The third step is hosting those fake web pages, if the original web address is www.mydomain.com, they will host the fake pages with domain name like www.my-domain.com or www.mydomain.net or www.mydomain.org

4) The next step after hosting the fake web pages is to dispatch mails to e-mail users. They will include the original web address in the search keyword, that's the words they will enter in search engines when searching for e-mails of people that are using or have accounts in the original web site.

5) They will design html message that's message formatted in web design styles. In the message, they will give you a link that will lead you to the web site. They will overlay their link with the original web link by using the following code www.theoriginalweblink.com when you click on the hyper link, it will take you to their web which is a replica of the original, but a fake web. An example I got from FBI anti-internet scam website is below:

1. The email address, From: eBay Administration [admin@ebayz.com] whilst looking like a genuine one from ebay is not correct as it reads @ebayz.com instead of @ebay.com
2. Often these e-mails will contain links that sometimes take you to pages on the genuine website to give it an appearance of being genuine. But they also can take you to fake pages set up to represent the genuine website.
3. The link to up date your records http://cgi1.ebay.com/aw-cgi/ebayISAPI.dll?Update, whilst looking genuine will take you a fake website, in this case http://johtnanx.com.phtemp.com/eb/. Always check the url shown in your web browser bar.

Always enter your on line auction or payment site through it's proper web address. Save this in your favorites. Never be tempted to enter it through a link sent to you, especially in an email, as it might lead you to a fake site and disclosure of your personal information. If your on line auction or payment site provides a toolbar down load that will advise you when you are on the genuine site, consider using this.
Copy of the Amazon spoof email is shown below:

-----Original Message-----
From: Amazon Security Department [mailto:service@amazon.com]
Sent: 04 July 2006 17:56
Subject: Fraud Prevention Measures

Amazon is committed to maintaining a safe environment for its community of customers. To protect the security of your account, Amazon employs some of the most advanced security systems in the world and our anti-fraud teams regularly screen the Amazon system for unusual activity.

We are contacting you to inform you that our Account Review Team identified some unusual activity in your account. In accordance with Amazon's User Agreement and to ensure that your account has not been compromised, access to your account was limited. Your account access will remain limited until this issue has been resolved.

To secure your account and quickly restore full access, we may require some additional information from you for the following reason:
We have been notified that a card associated with your account has been reported as lost or stolen, or that there were additional problems with your card.
This process is mandatory, and if not completed within the nearest time your account or credit card may be subject for temporary suspension.
To securely confirm your Amazon information please click on the link bellow:
https://www.amazon.com/cgi-bin/webscr?cmd=login-run

Above is a copy of a phishing mail that scammers sent out to people and was send to www.met.police.uk. Under the amazon link lays another fake link. In another attempt to gain your bank account details, rather than sending out a request from a bank, they are attempting to trick you into providing these details by claiming there is a problem with your Amazon account. Equally these type of emails could claim to be from any other online business.

DO NOT FOLLOW ANY LINK SENT TO YOU IN A E-MAIL IF YOU ARE BEING ASKED TO PROVIDE BANK ACCOUNT DETAILS. BANKS AND RETAILERS DO NOT ASK FOR THEM IN E-MAILS.
Also be aware of the fact some phishing e-mails are not providing a link, but a phone number for you to ring to confirm your details. No bank will e-mail you and ask you to ring a number to verify your account details and password.
DO NOT RING THESE NUMBERS. Always ring your bank on the number provided on the statement or documentation provided by them, or the number provide in a phone directory book or service.
This form of Internet fraud where by you are given a fake link to login is known as Phishing. Some fraudsters use fake yahoo login page or other types of web based e-mail service providers fake login page to fish for passwords of e-mail address of their victims. They can also access your online bank account, because once they have gained access to your e-mail address. Most online banking or payment system or other important organization will mail your password and even username to your e-mail address, if you have forgotten them. A hacker once told me the story of how, he gained access to someone's e-mail address and then went to SFIPAY, online account and entered that person's mail address and requested that they mail him the password that he has lost the password. They did and he logged in to that person's account and withdrew $950.

HACKING

It is now time for me to focus on another form of internet crime known as "HACKING", lots of internet users might have heard about it but only a few understands what it is and how it works. For those who don't understand the term "Hacking", I will explain it now. Hacking is the gaining of illegal and unauthorized access to computer networks and other useful information like passwords, online bank login information and accessing remote computer system in a network.

Hackers are those who undertake such acts. There are so many tools and techniques used by hackers to get the information they need and gain access to remote computers and online bank account and even e-mail account. These hackers can even delete or install programs in a remote computer once they gain access to that computer. Some can even send malicious codes or programs to your computer system. I will now illustrate how these hackers operate by giving you real life encounters with some of the hackers.

On 24th October 2004, that was when I was searching for details for this book. I entered yahoo hackers chat room, then I know nothing about how these hackers operate or attack their victims. I met an Egyptian man called Ahmed; I asked him how hackers obtain e-mail passwords especially Yahoo, Hotmail and AOL passwords. I will focus on yahoo, because almost everybody in Nigeria and all over the world uses yahoo chat messenger. Ahmed told me that it is possible to hack someone's password by using software called "password ripper." He told me that with that software you could steal yahoo passwords, through yahoo chat messenger. I asked him how and he said, "once that person is online and you have his or her yahoo ID (that's e-mail address), then that if you send file that contains anything like picture to that person through the password ripper. And the person accepts the file transfer that you will receive that persons e-mail password by instant message." I doubted him and he said, "You will receive request that I am sending you a file and once you accept the file transfer. I will instant message your password to you." When I got a request from him to send me a file I accepted the file transfer request and he instant message my password to me. As of them hacking was creeping in to the part of the country where I was living. Almost 80 percent of Internet users in Nigeria can only have access to the Internet by going to cyber cafes. Each day people complain that they have lost their e-mail password after browsing at cyber cafes, I set out to find out how and why these things happen. I found out that these hackers use software called "AUTO KEYLOGGERS." Once they install these program in any of the computers in the cyber café they can access any website you visit, in fact anything you type even you passwords. With that software they can view your e-mail address, passwords, login id or username and even letters that you typed. They can access and track anything you do once you did it by pressing the keyboard keys. Once their victim is through and left the café they will go to that particular computer and access everything you have done while using that computer. There is another form of KEYLOGGERS that they use. This one will be instant messaging them what ever you did every minute. They also use another software called "password stealer." This can only steal passwords alone. These KEYLOGGERS and the password stealers are password-protected meaning that the hacker can choose to access it by entering the password he used to set it up, meaning that no one else can access the information gathered by the software except him the person that set it up. If you have your own personal computer don't think that you are immune to these KEYLOGGERS, because they can still install this programs in to your system once your system has internet access by using another program. This program is called PRORAT, it serves as a launching system for this KEYLOGGERS because they can use it to monitor your system and at the same time install and delete programs from your system. In fact personal computer users are more prone to this kind of attack if they don't update and clean their system daily for bugs, than cyber café users because cyber cafes clean their system of bugs almost everyday.

There is another software called "BOOTERS" these hackers can use this software to restart and shut down your computer system. They can even disconnect you from yahoo chat rooms. There are different kinds of BOOTERS like big momma, boot the beast, electric disconnect. The major forms of attack they employ are:

1)Buzz Attack: this will create multiple chat windows until your system crash.
2)Disconnection: this will disconnect you from the yahoo messenger network and also restart or shut down your system.
These hackers achieve this by sending you the victim an invitation either to add you to their friends list or to view their web cam. Once you accept the request you will be automatically be disconnected from yahoo messenger. Sometime you see a pop up window containing the following message, "A serious error has occurred, do you wish to send a report." Once you click on any button in the pop up window, you will either be sign out of yahoo messenger or your system will restart or shut down. There is also another software they use to know when their victims are online, even when they sign in under invisible mode (by this I mean making it impossible for people to know that you are online even though you are on their friend's list.) And they can also view their victim web cams without their consent.

They also apply fake login page technique, I found out about this when I went in to a cyber café one Saturday morning to check my e-mail box. I opened Internet explorer and the default website address was www.anobscase.8k.com, and the content looks exactly like that of yahoo login page. The next thing that came up to my mind was that "this must be a fake login page." So I decided to put in wrong password to see what will happen. When I clicked the SIGN IN button, It took me to another web page with the following message "please click here to continue." And when I clicked on it took me to the genuine yahoo login web page. Meanwhile, I know my e-mail address and the incorrect password I put there have been e-mailed to whosoever put up that fake login page. One might ask of what use is the people e-mail password is to these hackers. If you have an online bank account or online account with any other important organizations, they normally send your passwords to your e-mail address when you request for it. For instance, if these hackers found out your e-mail password and they also know that you have an online account at any online organization. They can have access to your password by contacting the organization and tell them that they have lost their password, normally when you lose your password in any of this organizations it is send to your e-mail address. Some online organization will send an access pin to your mailbox, when they detect a change in your IP address. This is to prevent unauthorized person from accessing your account with them. For instance, if you have an e-gold account they will send access pin to your e-mail address whenever, someone or even you tries to access your e-gold account through another IP address. This is to make sure that if someone another person gains access to your account that he must also have your e-mail address password before he can access your e-gold account or that he is dong that from your IP address which means that you are likely going to be aware of it. It is also the same for those that use PAYPAL account, once you have lost your PAYPAL account password and you request for it. They will send the recovery link to your e-mailbox. Besides, they can gain access to other useful information like your credit card details for those that save their credit card information or other important information in their e-mailbox. This is very dangerous situation especially for those that use their e-mail address for online and even offline business transactions and other business activities. I will talk more on the in the chapter (how to draw your line of defense.)

There are other forms of hacking use mainly to attack those that own websites. They are known as:
1)DOS attack
2)Website defacing
3)Telnet
DOS ATTACK: I don't really know how this is done but one of these hackers told me that DOS Attack is sending of incorrect request to the web server until it disrupts the normal functioning of the server.
WEBSITE DEFACING: This is gaining access to a website host or server such that the hacker can modify, remove or re-edit the pages or change the login information.
TELNET: is a term that is used to refer to the set of procedures (actually a protocol) that enables a user of one computer on the Internet to login to

How To Draw Your Last Line Of Defense

In the preceding chapters, I exposed methods and forms used by Internet fraudsters to attack their victims. In those chapters, I just gave you examples of how they carry out each form of fraud. It is now time for me to give your extra tips that will help you to identify when you are about to be hit. This chapter will teach you how to draw your last line of defense.

In chapter two, I talked about e-mail scam and also gave you examples of how they will try to hit you. I also showed you samples of e-mails scams that I have received. Now, I will focus on how you can protect your e-mail address from falling in to this scam mailer e-mail harvester that harvest e-mail of those they will scam. If you can effectively protect your e-mail address from getting in to the hands of this scam mailers and fraudsters, you have reduced your chances of being hit by 70%. First let me explore the means through which this fraudsters gather e-mail address of their victims.

1.Mailing List Services
2.Search Engines
3.Online Forums
4.Others (I will explain later)

There are some websites that do business by selling e-mail address to Internet marketers. These scam mailers therefore buy these e-mail addresses and use it to send scam mails to the owners. The scam mailers can also choose the location of those they need their e-mail address, their profession and lot more. Some website will request for your e-mail address, before you sign up for their service and they will sell your e-mail to e-mail marketers. Some once you join their mailing list so that you will be receiving their updates, news and details of new products, they will sell it though they promised not to share your e-mail address with anybody. Another major method applied by these scam mailers is search for the e-mail address of their victims through search engines like Google, Yahoo and Ask. This greatly affect those that uses their e-mail address to sign up guest book at websites and also those that places their e-mail address in web pages. Below are examples of keywords, they use to query search engines like Google and others. "2006 @yahoo.com, or @aol.com, e-mail address of 20 richest men in the world" they use 2006, so that the e-mail addresses will be current and up to date. "@yahoo.com, or @hotmail.com e-mail address of doctors in Kuwait" they also use advance search methods to filter the e-mail addresses that will appear. "@Yahoo.co.uk, or @hotmail.co.uk e-mail address of UK based citizens." In fact, I once used this method and I found a website that contains more than 2000 e-mail address of UK based Medical Doctors. Once they have found the web sites, the next step is to use e-mail extractor to extract only the e-mails from the web page. The best way to reduce your chances of receiving scam mail is to stop using your personal e-mail address to sign up guest books, don't post your e-mail address in forums, in blogs, also don't sign up for newsletters of companies that you don't trust. Another important step is don't post any of your contact information like phone numbers in forums, Blogs and others. You can also contact your e-mail service provider and know how to activate your Spam filter. It will help reduce your chances of receiving scam mail. Some online job posting and searching websites will request that you provide your e-mail address for contacting you. It is advised that you be careful in the kind of online sites where you post or use your e-mail address. Not all online resume posting websites will expose your e-mail address.

I have said a lot about how you can protect your e-mail address from fraudsters. You will now learn how to detect a scam mail.

1. Consider any mail that tells you that you have won a gift, lottery, or anything even when you are sure you didn't enter for any draw.
2. Don't believe any e-mail you receive that says you must pay, before your gift; money that you win or whatever will be delivered to you.
3. Check out the e-mail header to know if that e-mail was sent only to you. I recommend this, because they normally use mass mail sender to dispatch the mails to their victims. So each copy of the mail normally contain the e-mail address of other recipients.

4. Don't believe any e-mail you received that tells you that you have won a gift, lottery and that you have to pay a remittance fee to claim it. I once received an e-mail that says that I have won $700,000 and the next thing that struck my mind was. I didn't enter for any draw, then how come I have won a lottery. Another thing that also cross my mind is if I really win $700,000, why wouldn't they deduct their remittance fee from it. Sometimes, the remittance fee will be around $200, $350 or even $50 depending on the amount involved.
5. Don't be fooled by the UK, USA or another countries phone numbers they normally include in the mail. They are distributed and have partners over there, besides they can use platform phone numbers. The contact numbers will be platform numbers (which start 0702, 0703, 0704) which cost 47p a minute to ring and will be linked to platform numbers subscribers own phone number, often a mobile, which whilst giving the appearance that the person is in the UK, they will often be anywhere.
6. When you receive mails from anyone that says that he is searching for someone to help him or her to claim some money left behind by his clients. Or someone to help him withdraw money paid to them by their clients and you will receive 10% or 15% of each transaction. Do not get involve, or if the offer sounds too good to be true then, don't be in a hurry to send the money to the person, wait until your bank cashes the check and confirms it to be genuine. Or contact your bank and other security agencies to help you verify if the check is valid.
7. Last but not the least, beware of any chat room business deals, especially those looking for people t buy or supply autos, mobile phones or raw material to them.

HOW TO AVOID WEBSITE SCAMS

1.Always be sure of the web address of website.
2.If you suspect that a website is a scam website, then check to see if they are certified by any certification company. Or try to see if there is anyone that has used their service before.
3.Try to know for how long the web or organization have been in service.
4.Always check for MySql injection error, before you use your credit card to purchase things or make payments in online websites.
5.Above all, always pay what you know you can afford to lose. If you can afford to lose $150, then pay it.

How To Avoid Internet Auction Scam

SCD6 Economic and Specialist Crime OCU is issuing warnings, as part of a crime prevention initiative against on Internet auction fraud and money transfer fraud. Often people, who become the victims of fraud through on line auction sites, are often persuaded to send the money fraudulently obtained from them through money transfer service providers.
1. Get to know the parameters set by the site - they are in place to ensure user safety. Read the safety advice provided by the on line auction site before trading. Never step outside of these or outside of the site no matter how enticing the deal. Fraudsters will try to trick you into doing this. Like any popular activity you must ensure you know 'the rules of the game' because 'A little knowledge is a dangerous thing'. When looking at an advertised item compare pricing. Beware of people offering you a deal below the current bid or reserve price, especially if they are contacting you direct. Remember 'If an offer sounds too good to be true it probably is'.
2. Get to know the seller by looking at their selling history and the goods they sale. Be extremely careful around the payment method used for persons selling with little or no selling history.
3. Don't get carried away in the excitement of winning an auction. Fraudsters rely on you being over keen and off your guard. It is never too late to ask questions of a seller to ensure that you are completely happy with what you are about to pay for. Do not follow through if you think it is a fraud, report the seller to the site.
4. Finally, if your site offers 'second chance' bidding on an auction verify that any notification of you qualifying for this 'opportunity' actually comes from the site and not from a fraudster impersonating them. You can do this by carefully checking the address from which the e-mail is sent or by contacting the site via its published website (Beware of using any hyperlinks or numbers attached to such a 'notification' as these may also be false). "Always ask yourself,

have I won the item, or have they won their next victim?" If you are a buyer that intends to buy something from an online auction site, below are the steps you should take.

1. Never use money transfers as a payment method whenever someone suggests this to you, even if it is by the seller after you have 'won' the auctioned item or when approached to step outside the on line auction site. There is little security in this, no matter what the seller says, and you are effectively sending your hard earned cash to a stranger 'on trust' alone.
2. Being extremely careful around direct banking transactions to pay for goods. There is still little security in this area also, which increases if the seller has no or little trading history with the on line auction site you are using. You are still effectively still sending your hard earned cash to a stranger 'on trust' alone. There have been instances where people have sent money to bank accounts and not received the goods. This has been more prevalent when dealing with people with no or little trading history on the auction site as a seller.
3. Use online payment options like E-Gold, PayPal, Moneybookers, SFIPAY or a reputable ESCROW account to pay for items. ESCROW is a payment system where both buyer and seller's financial details are held separately and in isolation by a legitimate third party company acting as 'middleman'. The buyer makes their payment into the Escrow account. The payment is only made to the seller the goods have arrived and been deemed satisfactory by the buyer. By doing so your transactions will be better protected and often insured. Never enter an Escrow account site through a link in an email sent to you by anyone, as it has not been unknown for fraudsters to set up fake Escrow websites. Use a search engine to locate the website or enter your chosen Escrow site through it's proper web address. Always check the url shown in your web browser address bar.

If you are a seller, below are the precautions you should choose:

1. When a cheque is accepted for payment, please be aware that although your bank or building society may after three days state that it has 'cleared', this only means that the money has passed between the banks. You remain liable if the cheque that you have paid into your account is forged or stolen, this may not come to light until the cheque is received by the other bank or the bank account holder queries a transaction on their account. This may take longer than you anticipate. The money is then taken back from you account so you lose not only the items that you have shipped to the 'Buyer' but also the money that the buyer 'paid' for the goods.
2. A common trick that fraudsters use is known as 'Criminal Cash Back' where a seller accepts a cheque for an amount higher than the value of the transaction, often to pay a 'shipping charge' to the buyers 'shipping agent'. This is actually paid to another fraudster who receives 'clean' money from you. You then find out at a later stage that although the cheque paid to you has 'cleared', it is a stolen or forged cheque, and you must pay the money back to your bank with no hope of getting the money back from the bogus 'shipping agent'.

Miscellaneous Forms of Scam and Preventive Methods

1. Money transfer fraud: Money transfer services are often the preferred method used by a variety of fraudsters in Online auction site frauds, 419 fraud, lottery fraud and criminal cash back.
2. Money transfer agents, which include Western Union provide a service for those who need to send money quickly and reliably to friends and family, and should not be used for money transfer to people that you do not know or whose identity you cannot verify.
3. Never pay for an item bought on an on line auction site through instant wire transfer service, whether it is suggested after making the winning bid or whether through another approach, such as second chance offer or offer the goods at a reduced price suggesting you step outside on the online auction site. There is little security in this, no matter what the seller says, and you are effectively sending your hard earned cash to a stranger 'on trust' alone.
4. Never send money via money transfer service if you have been in receipt of lottery fraud email, during which you are encouraged by the fraudster to send money in the form of advance fees to gain the release of the lottery funds, as genuine lotteries will never ask you for such funds to pay taxes or release fees. In fact genuine lotteries, such as the UK Big Lottery

has no idea who has bought the winning ticket, so will never be able to contact you telling you about your 'unclaimed' prize money. Never send these people money by any method.
5. Never send money via money transfer service if you have been in receipt of a '419' email offering you a cut of a large sum of money then if you help to release it from a bank account. If you respond, during the discussions with the fraudster you will be encouraged by them to send them money in the form of advance fees to gain the release of the funds mentioned in the email, usually a ridiculous figure mentioned that is in the millions. Never send these people money by any method.
6. Never send money via money transfer service if you have been in receipt of cheque payment from someone in a sum greater that that you are asking (known as criminal cashback) for the item you are selling or property you are renting. After the cheque has been paid into your account, the fraudster you will encouraging you to send to them or someone else the difference by money transfer or bank transfer. Never send these people money by any method. If the cheque is stolen or forged it often can take more than 3 days, sometimes considerable longer, before that cheque is identified as being stolen or forged. Not only have you already sent the funds by money transfer with no means of recovering it, you will find that you bank account will have the original debt reversed, leaving you with the loss of the funds withdrawn and sent via money transfer.
7. When money transfer services are being used in connection with fraudulently activity, whilst the person collecting the money has to produce identification, the documents produced by these fraudsters are often false, making the recovery of any money sent by this method extremely difficult.
8. Western Union recently joined forces with the Metropolitan Police Service to combat 'high volume' fraud.

What is West African "419" fraud?
Advance fee fraud or '419' fraud (named after the relevant section of the Nigerian Criminal Code) is a popular crime with the West African organised criminal networks. There are a myriad of schemes and scams - mail, faxed and telephone promises designed to facilitate victims parting with money. All involve requests to help move large sums of money with the promise of a substantial share of the cash in return.
This type of scam, originally known as the "Spanish Prisoner Letter", has been carried out since at least the sixteenth century via ordinary postal mail. These scams have come to be associated in the public mind with Nigeria due to the massive proliferation of such confidence tricks from that country since the mid-eighties, although they are often also carried out in other African nations, and increasingly from European cities with large Nigerian populations, notably London and Amsterdam.
The laws from Section 419 and laws in place in other jurisdictions criminalizing the offences do not scare away the criminals who profit from these crimes. The stakes and profits are simply too high and many government officials are believed to be involved with the criminal gangs.

Identity theft is the unlawful taking of another person's details without their permission. The information stolen can be used to obtain many financial services goods and other forms of identification i.e. Passports and Driving Licences. The information stolen can range from a copy of birth certificate to copies of discarded bank or credit card statements and utility bills.
Once the criminals have copies of someone's identity they can embark on criminal activity in their name with the knowledge that any follow up investigations will not lead automatically to them. With your details they can obtain documents that are in essence real, but containing false information thus making it difficult for organisations to known who they really are dealing with.

Protect yourself!
Be careful with your personal information. If you receive a telephone call from a credit card company, bank or other retail company asking to confirm certain details about yourself decline

them and ask to call them back preferably through a central switchboard. When destroying personal correspondence such as bank and credit card statements consider a shredder or even burning them on the garden refuse. If you cannot do either then tear the papers up into very small pieces and place in the refuse bin with other waste products.
If you move address remember to inform all of the companies that send personal information to you in the post. Always consider re-directing your post with Royal Mail. If you fail to do this people moving in might have free access to your personal details and misappropriate them.
How do you know if are victim to this type of fraud?
Are you missing your regular monthly statements?
Have you noticed charges to your accounts that are not yours?
Remember to check all statements especially bank and credit card.
Being contacted by a debt collection agency about outstanding payments for items or services that you have not ordered.

Take Action - Act Quickly
Firstly do not ignore the problem it might not be you that has ordered some goods or opened an account but the debt falls to your name and address.
Once blacklisted for credit it may take many years to fully recover the problem you might have difficulties in obtaining a mortgage or other bank credit.

Cash machine fraud is not a type of fraud but describes the location where it occurs i.e. where the person withdrew money at an ATM (Automated Telling Machine) and had their account compromised.

Although fraud at cash machines in the UK has increased significantly in the last five years, it accounts for less than ten per cent of total plastic card fraud losses. Skimming at ATMs is a growing trend, often perpetrated by organised Eastern European criminal gangs.

How the frauds work
Card Reading Devices
In the case of skimming at ATMs a skimming device is attached to the card entry slot and a separate miniature pinhole camera is hidden overlooking the PIN pad. This enables the criminal to produce a counterfeit card and withdraw money at a cash machine using the legitimate PIN. These devices are highly sophisticated and look as if they are part of the machine itself. The device may only be placed on a machine for a very short period of time whilst the fraudsters remain nearby. The fraudsters will eventually take the reading devices off and move to another location and do the same again.
Shoulder Surfing
Shoulder surfing - where criminals look over a cardholder's shoulder to watch the PIN being entered, and then steal the card using distraction techniques or pickpocketing. This may be by dropping money on the floor and pointing out to the person at the machine that they have dropped it.
Card Trapping Devices
A device, inserted into a cash machine's card slot, retains the card inside the cash machine. The criminal tricks the victim into re-entering the PIN while the criminal watches. After the cardholder gives up and leaves, the criminal removes the device, with the card, and withdraws cash.
The Association for Payment Clearing Services (APACS) are working hard with industry and law enforcement to reduce the volume of criminality relating to ATMs. In the meantime there are some basic things you can do:
If you suspect a device has been placed on an ATM DO NOT ATTEMPT TO MOVE IT . These are expensive devices and suspects may use violence if they think their precious commodity is likely to be interfered with.
Instead call the police or contact the bank immediately
Do not keep your card and PIN number together

Be mindful of people behind you at cash machines. Do not let others see your PIN number When keying in your PIN try to cover your typing hand.

Lotto frauds are becoming prevalent in the UK with promises of huge winnings arriving in the form of unsolicited e-mail or letters to UK residents.

Invariably the communication will purport to come from an overseas lottery and claim that the recipient has been allocated winning numbers.

The recipient will contact the organisers, whether directly through telephone, by post or e-mail and will be invited to send money in to assist in the administration for the release of the winnings.

These winnings do not exist. This is merely a scam and attempt to illicit money from unsuspecting victims. As the winnings on offer are substantial, so too can be the advance fees required to release the funds.

The real cruel part of this scam is that suspects will build up a rapport with victims through telephone contact in order to continue the flow of money.

Who are the victims?
In the case of e-mail anyone can be a victim. These spam e-mails are sent en-bloc and anyone can become a potential victim.

With letters the criminals can be a little more specific and in many cases the elderly are most at risk. Suspects pay good money for mailing lists and they do target those lists that deal with the elderly.

Hard copy letters complete with certificates of winnings will be sent to the unsuspecting victim. On the face of it these look genuine.

The victim may respond and after sending a fee to the fraudsters may have telephone contact. The fraudsters will gain the confidence of the victim, hence where the elderly are most at risk.

Communications are often sent to drop or P.O. Box addresses. These are then collected by couriers or third parties and sent on to the fraudsters, in most cases overseas.

Payments are made through cheques, credit / debit card transactions or through sending cash via money transfer services.

Cheques can be cleared through international clearing services and the money will go through a series of further transactions before finally arriving in the pockets of the fraudsters.
To learn more visit the following websites or contact the following,
enforcement@sec.gov
http://www.sec.gov/investor/pubs/cyberfraud/questions.htm
www.met.police.uk
http://www.consumer.gov/idtheft/
mail scam mails to :**spam@uce.**govor contact
the FBI at **http://www.ifccfbi.gov/**. To fight computer criminals, they need to hear from you.
If a scammer takes advantage of you through an Internet auction, when you're shopping online, or in any other way, report it to the Federal Trade Commission, at **http://ftc.gov**. The FTC enters Internet, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.
Send phisphing mails to **reportphishing@antiphishing.org** and also contact the organization that the scammer tries to use to phish you, **http://www.consumer.gov/idtheft/, http://onguardonline.gov**