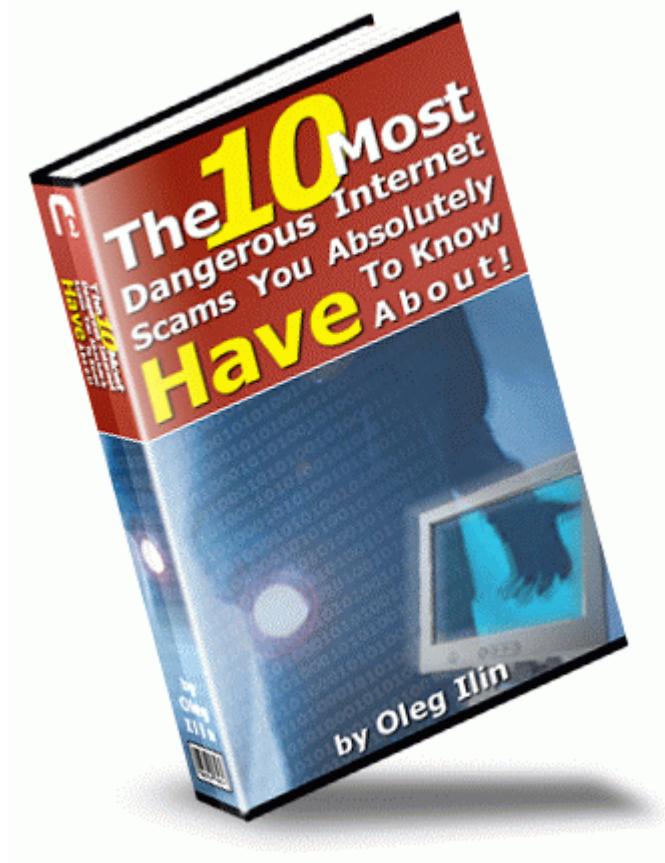


# **The 10 Most Dangerous Internet Scams You Absolutely Have To Know About**



**Attention: This e-book can save you thousands of dollars and potentially can help you Save Your Life.**

## **Free Redistribution Rights To This E-book !**

**Congratulations!!**

You now own the redistribution rights to this e-book, "The 10 Most Dangerous Internet Scams You Absolutely Have To Know About". It's your free! **This is a \$199.00 value!**

You can use the e-book as a free bonus or premium and give it away. It's your choice.

The only restriction is that you cannot modify this e-book in any way.

© Copyright November 2005 By Oleg Ilin

**ALL RIGHTS RESERVED.** No part of this e-book may be reproduced or transmitted in any form whatsoever, electronic, or mechanical, including photocopying, recording, or by any informational storage or retrieval system without express written, dated and signed permission from the author.

**DISCLAIMER AND/OR LEGAL NOTICES:** While every attempt has been made to verify the information provided in this e-book, neither the author nor his affiliates/partners assume any responsibility for errors, inaccuracies or omissions. Any slights of people or organizations are unintentional. The e-book is intended for information only. The publisher and author do not imply any results to those using this e-book, nor are they responsible for any results brought about by the usage of the information contained herein.

The publisher and author disclaim any personal liability, loss, or risk incurred as a result of the use of any information or advice contained herein, either directly or indirectly.

If advice concerning legal or related matters is needed, the services of a fully qualified professional should be sought. This e-book is not intended for use as a source of legal or accounting advice. You should be aware of any laws, which govern business transactions or other business practices in your country and state. Any reference to any person or business whether living or dead is purely coincidental.

© Oleg Ilin - All Rights Reserved

## ABOUT THE AUTHOR

Oleg Ilin has been marketing online since 2002. He is the publisher of [InterPreneur Newsletter](#) and the co-owner of 1EzHost L.L.C.

Recognized as an expert author on Internet marketing, web development, search engine optimization and RSS development, he has a passion for cutting edge technological solutions that could help facilitate the process of online communications and improve the safety of Internet environment.

Check out his websites:

<http://www.1ezhost.biz>

<http://www.web-feed.com>

<http://www.1ezhost.com>

## TABLE OF CONTENTS

About author.....	3
Introduction.....	5
1. Nigerian Fraud.....	7
2. “Dutch Lottery” Scam... ..	13
3. “Russian Bride” Scam.....	18
4. Health Scam.....	22
5. Job Posting Scam.....	25
6. Online Auctions Scam.....	27
7. EBay/PayPal/Any Bank “Account Confirmation” Scam.....	29
8. Identity Theft – Viruses, Worms, Trojans and their most dangerous variation –RATs.....	36
9. Identity Theft – Spyware, Adware, Malware, Help Objects, Automatic Logins.....	38
10. “Change of Hearts” – shift from OS to software.....	41
Conclusion.....	43

## INTRODUCTION

Internet created one of the most profitable professions on earth – Internet entrepreneurs. There are numerous ways for entrepreneurs to earn very good living online. You can sell physical and infomercial products, offer millions of services, sell ad space, start your own place to hang out, even create your own radio station... Possibilities are endless.

In short, Internet is a goldmine, Klondike of the 21<sup>st</sup> century, but Internet can also be a very dangerous place. The goal of this e-book is to let you know about the most dangerous Internet scams, and to help you avoid them. After all, when you become aware of those schemes, there is a good chance that you won't fall into a trap.

According to Federal Trade Commission report from February 1<sup>st</sup>, 2005 (FTC is the American regulatory organization):



*“A total of 388,603 of the Consumer Sentinel complaints were fraud-related. Internet Auctions was the leading complaint category with 16% of the overall complaints, followed by Shop-at-Home/Catalog Sales (8%), Internet Services and Computer Complaints (6%), Foreign Money Offers (6%), Prizes/Sweepstakes and Lotteries (5%), Advance-Fee Loans and Credit Protection (3%), Business Opportunities and Work-at-Home Plans (2%)”*

*“Consumers reported fraud losses of over \$547 million; the median monetary loss was \$259.*

**• Internet-related complaints accounted for 53% of all reported fraud complaints, with monetary losses of over \$265 million and a median loss of \$214.”**

[http://www.consumer.gov/idtheft/pdf/clearinghouse\\_2004.pdf](http://www.consumer.gov/idtheft/pdf/clearinghouse_2004.pdf)

According to Office of Fair Trading report from February 1<sup>st</sup>, 2005, scams and cons from overseas are set to cost Britons £1 Billion the year of 2005 alone. (OFT is UK regulatory organization).

I will be using different order to discuss Internet Frauds in this e-book than the order shown above in the FTC report. Of course, it's not good that there are many complaints in the Internet Auctions and in Shop-at-home/Catalog Sales, but at least those frauds are not lethal. I will cover the frauds in the order of damage they cause to the victims; starting from the scam I consider to be the most dangerous.

## “The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

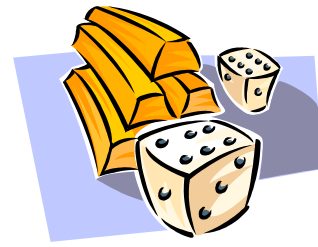
Why am I writing this e-book, you ask? Simple. I got sick and tired of all the emails that I receive daily. Those emails either notify me about “security breach” in my accounts or describe different “opportunities” for me to earn quick cash.

All the notifications from “paypal” and “ebay” and “e-gold” about temporary suspension of my account (please note the quotes – real companies, such as eBay and PayPal, have nothing to do with those emails), all the requirements to change my account information in different banks, even in those where I don’t have any account whatsoever, all the offers to participate in unbelievably profitable partnerships where I can quickly earn a few million dollars. They just roll in my inbox like a snowball.

Probably, I would still continue deleting such emails, but one day I realized that people are actually getting hurt in those scams and what’s even worse; people are kidnapped, held for ransom and killed.

So please read this e-book very carefully, because it will help you recognize and avoid the most lethal Internet scams.

**Ok, so what is the deadliest fraud on the Internet you should be absolutely aware off?**



## 1. NIGERIAN FRAUD

This scam is also known as “Advance Fee Fraud”, “419 Scam” or simply “419”. 419 is a number of Nigerian anti-fraud statute. This is not just a fraud anymore. This is the whole “industry”. It can’t be called an industry per se, because it’s an illegal operation. But it can be called an “industry” based on its revenue, profits, turnover, number of participating “companies” and “employees”.

Victims lose billions of dollars in this scam every year. The scale of this scam is so huge that it’s considered to be from 5<sup>th</sup> to 2<sup>nd</sup> largest industry in Nigeria (there are different opinions about the “position” of this “industry” among other Nigerian industries, but even if it’s number 5, it’s too damn impressive for the fraud).

Scammers are hugely successful in their operations, because they are skillfully playing on several positive and negative human emotions that serve as an underlying foundation for a decision-making process. Those emotions are: desire, faith, love, sex, hope, greed and fear, conceit (ego).

Unfortunately this scam will continue to work for a long time. In fact, it will be effective as long as human behavior remains the same. And I don’t see the basis of human behavior changing in the foreseeable future.

Here is a quote about Nigerian Fraud from the official United States Secret Service website:



*“Unfortunately, there is a perception that no one is prone to enter into such an obviously suspicious relationship. However, a large number of victims are enticed into believing they have been singled out from the masses to share in multi-million dollar windfall profits for doing absolutely nothing.”*

<http://www.secretservice.gov/alert419.shtml>

You can also find the brief description of Nigerian Scam at the official website of the Federal Trade Commission (FTC):

<http://www.ftc.gov/bcp/online/pubs/alerts/nigeralt.htm>

### Here is how Nigerian Scam works

Individual receives unsolicited e-mail from Nigeria, sender of this email claims to be either the person holding high administrative or authoritative position himself (general director in the Ministry of Agriculture, president of the oil company, son of the president

## “The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

of Nigeria) or the person acting on behalf of such an individual. Or the sender simply can present himself as a “very rich” person who is trying to secretly transfer money from Nigeria.

The email sender is asking victim’s assistance in a “highly confidential” and “urgent” operation. Usually recipient is informed that he was “hand-picked” to participate in this operation based on his business skills and/or his reputation.

Email recipient is offered anywhere between 20% and 30% for providing his own business account for this operation. And this is not a pocket change either. The amount of transfer ranges between **\$10 Millions and \$60 Millions**, hence, victim’s potential share in this operation could range from a few Millions to close to \$20 Millions.



There is a catch though. It’s clear from the very beginning that the legal side of the operation is questionable. It’s questionable enough to keep the victim from seeking help from police or other authorities in the future, but on the other hand, it’s not serious enough for the victim to not even think about participating in this operation.

There are many different scam “stories “ explaining the “origin” of money that should be transferred. Here are several examples:

- ◆ Over-invoiced contracts, where the sender of the email claims that his department and or Ministry received more money for the product then they should have and that he has access to that money, he wants to hide them from government by transferring them to foreign account (presumably, the account of the victim).
- ◆ Money from some politician trying to smuggle them out of the country because of the change of the political regime or because he’s ready to leave his post for retirement.
- ◆ Marked, stamped, blackened (covered with black coating) or defaced banknotes that we brought into such condition for security purposes by the dictator or other government officials that stole that money or received them as a bribe. Those banknotes are useless at the moment, but could be returned to their original condition after treating them with a secret and very expensive chemical dye remover.
- ◆ Money left as a heritage of the wealthy individual when no relatives left and victim is offered to act as a “next of kin”, that is distant relative from abroad.
- ◆ There are hundreds of variations of those “stories”; criminals are very creative in their explanations.

## “The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

After the victim responds to such email expressing his will to participate in the “operation”, he receives a bunch of officially looking documents (sent by fax or email), sealed with Nigerian government seals. He also might receive a letter of credit and other bank statements if required. All those documents are forged. The purpose of those documents is to establish further credibility with the victim.

Victim is asked to provide blank forms, letterheads, and invoices for the company that is going to be used to transfer funds to the victim. Real reasons for obtaining those documents are:

- ◆ to fool other victims,
- ◆ to use them as a forged “invitations” when applying for visas in American and European Embassies. The Embassy to present forged papers to is chosen based on the origin of the victim. For example, if a victim is an American – then his company “letter of invitation” is presented to American Embassy, etc.)

After criminals receive documents from a victim, victim is informed that there is a problem with “insider man”- an official who has access to the funds, and substantial amount of money is required from the victim to bribe this official to make him release the funds.



After that portion of money is received, criminals involve the victim in an endless sequence of other “unexpected fees”, “taxes”, etc. Each “fee” is promised to be the last one. At that time victim already spent enough money to be deeply involved emotionally in the process and he is willingly giving more and more. He can’t stop hoping that this particular fee is the last one, and then he would finally receive the money and all his worries and troubles would be over...

Finally victim realizes that he’s out of money, he can’t borrow anymore. He refuses to pay the next fee. Then he is invited in Nigeria or border country to talk to “an official” responsible for the release of the funds and to see for himself that funds are almost ready to be transferred (or criminals may come up with hundreds of similar lame explanations). If visitor rejects to come and stops sending money, he is often threatened. He’s reminded that he can’t go to police because he is participating in an illegal operation. It’s not pretty, but at least in this scenario victim has a better chance to survive, he is in his own country, he can contact authorities, etc.

The worst-case scenario would be if the victim decides to go to Nigeria to rectify the problem himself. Victim is usually told that visa is not necessary to visit Nigeria. Then criminals illegally bring him in a country by bribing airport and Custom officials. In reality, this is a serious crime in Nigeria to enter the country without proper traveling documents and clearing procedures, and this fact could be used later on to press the victim and extort additional money.

## “The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

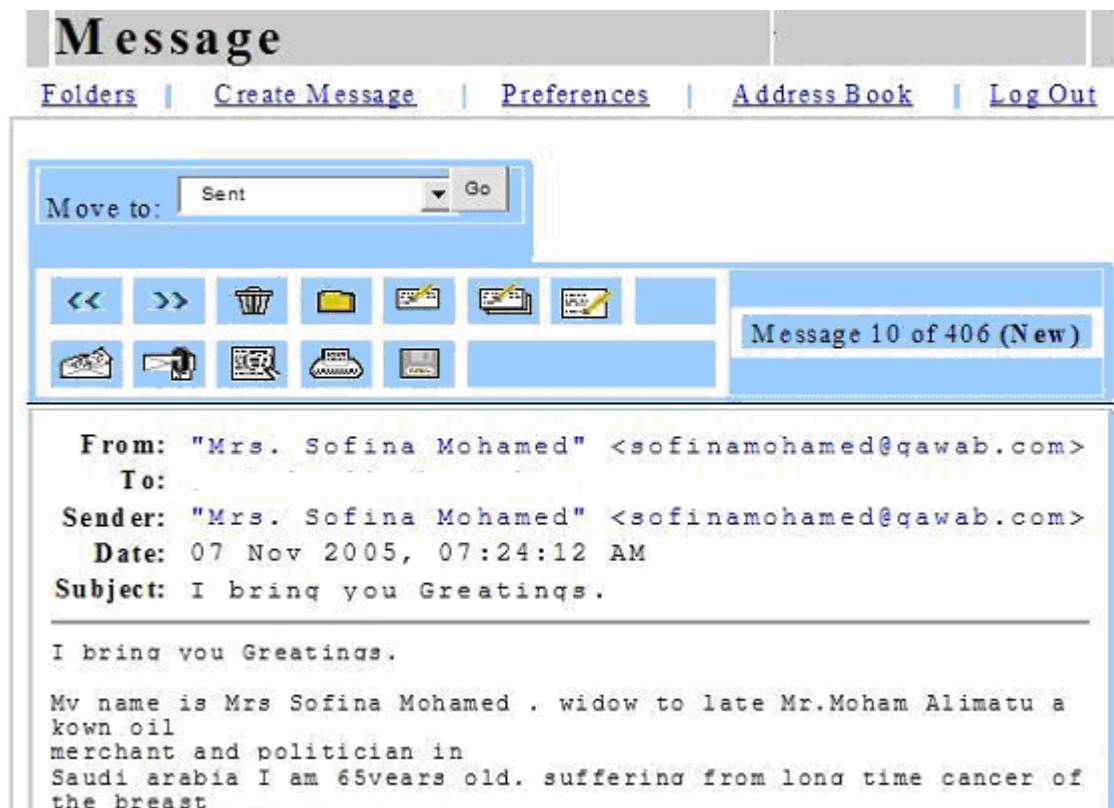
The criminals may take a victim to meet an “official” in the government building to show their credibility. This “official” may be imposter, but there were also numerous cases when actual officials were involved in a scam.

If after this meeting victim is convinced and pays whatever “fee” he should pay this time, he stays in the hotel until the next “obstacle” arises, and so on. Victim is held in Nigeria until criminals are convinced he has absolutely nothing left.

If victim refuses to pay a “fee” after meeting with the “official”, he may be kidnapped and held for ransom. And unfortunately he may be killed or disappear at the end.

### **That’s why Nigerian scam is the most dangerous scam.**

Here is an **example** (snapshot) of a typical Nigerian Fraud letter (I decided to show you the latest letter I received). I mentioned before that scammers are rather inventive in their emails; they use different variations of the same idea. You will notice that in this particular email “Nigeria” is changed to “Saudi Arabia”, and “General Director” of some Ministry changed to a “widow”, and “charity organization of your choice” is used to lower the defense of the email recipient, but other than that it’s absolutely the same scam.



## “The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

,From all indications my condition is really deteriorating and it's quite obvious that I won't live more than 2 months according to my doctors. This is because the cancer stage has gotten to a very bad stage. I don't want your pity but I need your trust.

My late husband died early last year from heart attack, and during the period of our marriage we couldn't produce any child. My late husband was very wealthy and after his death, I inherited all his business and wealth. The doctor has advised me that I will not live for more than 2 months, so I have now decided to spread all my wealth, to contribute mainly to the development of charity in Africa, America, Asia and Europe.

Am sorry if you are embarrassed by my mail. I found your e-mail address in the web directory, and I have decided to contact you, but if for any reason you find this mail offensive, you can ignore it and please accept my apology.

Before my late husband died he was a major oil tycoon, in Saudi Arabia and deposited the sum of \$18.5M Dollars (Eighteen Million and five hundred thousand united states Dollars) with a financial institution in Europe some years ago, this is all I have left now, I need you to collect this funds and distribute it yourself to charity, so that when I die my soul can rest in peace the funds will be entirely in hands and management.

I hope you will have mind and wisdom to touch very many lives, that is my main concern, I have also decided that 10% of this money will be for your time and effort, while 90% goes to charity.  
Yours sincerely

Mrs. Sofina Mohamed.

### History of Nigerian Fraud

It may surprise you, but Nigerian Fraud, in its current form, is not “invented” recently. This is nothing more than creative and technologically improved variation of “Spanish prisoner” scam that is dated as far back as to the 16<sup>th</sup> century. That’s another proof that human psychology is not changing in leaps and bounds and the basic principles of human behavior are rather stable.



“The Spanish Prisoner is a confidence game dating back to 1588. In its original form, the confidence artist tells his victim (the mark) that he is in correspondence with a wealthy person of high estate who has been imprisoned in Spain (originally by King Philip II) under a false identity. The alleged prisoner cannot reveal his identity without serious repercussions, and is relying on the confidence artist to raise money to secure his release.

The confidence artist offers to let the mark supply some of the money, with a promise that he will be rewarded generously when the prisoner returns both financially and by being married to the prisoner's beautiful daughter. However, once the mark has turned over his money, he learns that further difficulties have arisen, requiring more money, until the mark is cleaned out and the game ends.

Key features of the Spanish Prisoner are the emphasis on secrecy and the trust the confidence artist is placing in the mark not to reveal the prisoner's identity or situation. The confidence artist will often claim to have chosen the mark carefully based on his reputation for honesty and straight dealing, and may appear to structure the deal so that the confidence artist's ultimate share of the reward will be distributed voluntarily by the mark.” (Quote From Wikipedia, the free encyclopedia)

The principal difference between “Spanish Prisoner” and Nigerian Fraud is the lack of Internet power and current technological abilities in the first scam. After all, there are only so many letters you can hand-write and send.

The Nigerian Fraud however, is much more dangerous. Letter only has to be written once, plus there is no mailing costs whatsoever. And the target auditory is almost unlimited. There are billions of Internet users with email addresses. And that means potentially unlimited damage. Imagine the scam letter that is sent to 10 000,000 potential readers.

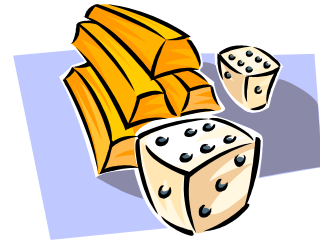
Current technology can handle this task rather easily. If the response rate to the email campaign is only 1%, it's a potential of 100 000 victims. And the response rate can be much higher than 1%. And there is no need for scammers to stop at 10 000,000 email addresses. They can continue to harvest email addresses again and again by utilizing different email harvesting programs.

Email harvesting is also often used in another scam called “lottery scam” or “Dutch lottery” scam.

## Useful Resources:

Fraud Eliminator protects you from online fraud, including online scams, phishing, and pharming; Identity Theft Prevention Software helps protect your family, and more:

[http://www.1ezhost.biz/identity\\_theft\\_prevention.html](http://www.1ezhost.biz/identity_theft_prevention.html)



## 2. “DUTCH LOTTERY” SCAM

The name of the scam was originated based on the fact that most “Winning Lottery Notifications” were sent from Amsterdam, and in this scam victim was notified about “winning” in some electronic “Dutch Lottery”.

What is interesting, many of the lottery scams are also orchestrated by Nigerians acting from suburban areas of Amsterdam. In fact, sometimes lottery scam is considered to be a variety of Nigerian Fraud, as it also involves advance fee fraud.

Of course now Nigerians are not the only ones participating in this fraud. And Netherlands is not the only “country of a sudden fortune” either. Some of those lottery schemes are conducted from Great Britain (at least Netherlands and Great Britain are often shown as places where “drawings” take place and from where those “Winning Notifications” are sent. In reality, email could be sent from any country, Canada and China are among the most active “participants”).

People lost thousands upon thousands of dollars in this scam. And not only dollars are lost. People all over the world, with different currencies, suffer the consequences of this fraud.

Here is a quote from Colin Brown, Director of Co-regulation, Codes and Coordination at the OFT (Office of Fair Trading) about the Canadian Lottery scam:



*“Millions of pounds are being lost by UK consumers to this scam so it is vital that we tackle the problem through continued cooperation and it remains a top priority for all involved in crime enforcement.”*

### Here is how “Dutch lottery” works

“Lucky” recipient receive an email with a subject “Winning Notification” or “Award Notification” or “Congratulation, You Have Won Lottery Award” or something of this nature.

Within this email recipient find the stunning news that he won a big amount of money usually somewhere between **\$1 Million and a \$10 Millions**. If it’s a Great Britain “drawing” the prize money may be “won” in GBP, not in US dollars.

## “The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”



In order to collect the “winnings” the recipient has to contact a “claims agent”. Funny thing about “claims agents” is that usually they use free email addresses (like yahoo, hotmail, etc). Of course, officials from **real lotteries** never use free email addresses.

OK, so victim contacts this “claim agent” and is asked to fill out the form “to verify his true identity”. And the unsuspected victim provides all his personal details, address, date and place of birth, working details, next of kin details, plus a copy of passport and/or his driver’s license.

This gives criminals enough information to commit identity theft. But that’s only the part of the scam. When scammers receive all this data, they offer several options to collect the “winnings”.

Either victim can go to Amsterdam personally (or to London, or Liverpool or any other place indicated as a place of “drawing”), or check may be delivered by a “courier company” or wired to recipient’s bank account (options differ in different lottery scams).

If the option with check is chosen, victim is notified that he has to pay various upfront fees, such as notarization fee, clearance fee, insurance fee and the fee to the “Courier company” for “secure delivery” of the “certified check”, etc.

When all the “fees” are collected, often to the tune of \$6,000-\$10,000, victim never hear from those “helpers” again.



If victim chooses the wire option instead, he incurs the same notarization/clearance/insurance fees and then he is asked for his bank account details “to receive bank transfer”. If recipient is very naïve, he may provide details of his real bank account where he keeps his money. Of course those money quickly disappear.

In a more secure position are those victims who provides newly opened empty accounts for this purpose. But there is a still big possibility that those accounts will be used by scammers for fraudulent transactions in the nearest future.

Or scammers may ask victim to open an online account with a specific bank in order to collect money. As you would have guessed by now, this bank primarily serves “corporate clients” and has a minimum deposit requirement of \$3,000- \$7,000 and there is no bank in reality, just fake papers.

The third option is the most dangerous out of all three; it’s the main reason why “Lottery Scam” keeps second position on our scam scale of danger.

## “The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

If victim will choose to get money personally, he again has to pay upfront fees; this time it's a “release fees” (and there may be other fees as well). The good scenario is that after paying fees he receives a bag full of paper, covered with just a few real banknotes. Why it's a good scenario? Because **the bad scenario would be that victim is kidnapped and held for ransom.**

Here is an **example** (snapshot) of a typical Lottery Scam letter/email:



## “The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

which subsequently won you the lottery in the 2nd category i.e. Match 5 plus bonus. You have therefore been approved to claim a total sum of 616,268Euro(Six hundred and sixteen thousand, two hundred and sixty-eight euro) in cash credited to file KTS/9023118308/03. This is from a total cash prize of 2,465.072Euro shared amongst the four (4) lucky winners in this category i.e. Match 5 plus bonus. All participants for the online version were selected randomly from World Wide Web sites through computer draw system and extracted from over 100,000 unions, associations, and corporate bodies that are listed online. This promotion takes place weekly. Please note that your lucky winning number falls within our European booklet representative office in Europe.

In view of this, you have therefore been approved to claim a total sum of 616,268(Six hundred and sixteen thousand, two hundred and sixty-eight euro) which would be released to you by any of our payment offices in Europe. Our European agent will immediately commence the process to facilitate the release of your funds as soon as you contact him. For security reasons, you are advised to keep your winning information confidential till your claims is processed and your money remitted to you in whatever manner you deem fit to claim your prize. This is part of our precautionary measure to avoid double claiming and unwarranted abuse of this program. Please be warned. To file for your claim, please contact our fiduciary agent:

MR. MARIANO LUIS ALVAREZ

Email: [winning001@katamail.com](mailto:winning001@katamail.com)

Tel: [0034 676 771 699](tel:0034676771699)

For the immediate release of your funds you are to provide the following details our fiduciary agent:

FULL NAMES OF BENEFICIARY:.....  
CONTACT ADDRESS:.....  
CITY/STATE:.....  
COUNTRY:.....  
NATIONALITY:.....  
SEX:.....AGE:.....  
MARITAL STATUS.....  
TEL NO:.....  
NEXT OF KIN:.....  
AMOUNT WON:.....  
REFERENCE NO:.....BATCH NO:.....  
LUCKY NO:.....TICKET NO:.....  
SERIAL NO:.....LOTTERY DATE:.....

## “The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

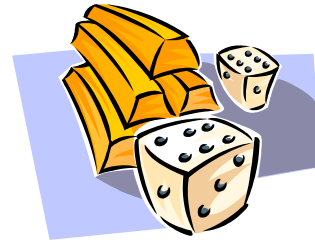
NEXT OF KIN:.....  
AMOUNT WON:.....  
REFERENCE NO:.....BATCH NO:.....  
LUCKY NO:.....TICKET NO.....  
SERIAL NO:.....LOTTERY DATE:.....  
  
Good luck from me and members of staff of the SPANISH NATIONAL LOTTERY. You can  
check the  
attachments.  
  
Yours faithfully,  
MR ANTHONIO VIDA PARKER  
  
Online coordinator for SPANISH NATIONAL LOTTERY  
Sweepstakes International Program.  
  
WARNING!!!  
  
ANY MAIL RECIEVED OF THIS SUCH WITH ANY OTHER TRADE MARK OR ADDRESS SHOULD  
BE FOWARDED TO THIS BOX IMMEDIATELY, THIS WILL HELP US TO FIGHT SCAM AND  
LOTTERY IMPOSTERS. THANK YOU FOR YOUR ANTICIPATED CO-OPERATION.  
  
Copyright © 1994-2005 The Spain National Lottery Inc.  
All rights reserved. Terms of Service - Guidelines.

### Useful Resources:

Award-winning anti-spam software for Microsoft Outlook and Outlook Express, and  
more:

[http://www.lezhost.biz/prevent\\_spam.html](http://www.lezhost.biz/prevent_spam.html)

### 3. “RUSSIAN BRIDE” SCAM



While Nigerian scam and Dutch lottery scammers play on the victim's desire to quickly earn some money, desire for sex and romance is used as a main “joker” in a Russian Dating scam. It's a well – known fact those brides from Russia, Ukraine and other countries from former Soviet Union are very popular in the world because of their beauty, charm, and faithfulness.

Unfortunately, con artists use natural man's desire to find a life partner and they cheat victims out of their money. Americans alone lose millions of dollars in this scam every year.

Please don't get me wrong. The majority of Russian ladies who place their profiles on the Internet with different matchmaker agencies, they are honest and genuine. They want to find a partner to build a future family home with. I'm a Russian myself, so I know what I'm talking about. But there are many crooks operating as “Russian brides”, thus giving real Russian brides a bad name.

Sad thing is that many of those who present themselves as “Russian brides” actually are citizens of other countries – Americans, for example, or Nigerians. And even more than that, they are not even women – they are men!

Here is a quote from San-Diego Union-Tribune Newspaper, as of June 23, 2004:



*“A San Bernardino County man was sentenced to five years in federal prison yesterday for cheating men out of more than \$1 million in a Russian bride scam.*

*The sentence was imposed from an April plea bargain in which Robert McCoy, 40, of Rancho Cucamonga admitted defrauding more than 250 men and agreed to pay back his victims \$737,521”*

<http://www.signonsandiego.com/news/metro/20040623-9999-1m23brides.html>

I'm not implying that Russians do not participate in this type of scam at all. Unfortunately, criminal groups from Russia and FSU exploit men's need of romance and sex too, so it may be very dangerous for a “groom” to visit a “bride” in person in Russia, since in reality it's a well set up trap. The consequences may be similar to visiting Nigeria. That's why I listed this scam as a #3.

The good news is that it is fairly easy to recognize this trap and distinguish between genuine women and criminals. You just need to know how this scam works and to

remember a few tips that will help you find out the truth. Keep reading, they are listed below.

## Here is how “Russian Bride” scam works

Criminals post on the Internet pictures of beautiful Russian girls who are supposedly looking for foreign partners and/or future husbands.

Victim from another country starts communicating with a “girl” he likes, via e-mail. After 5-7 letters girl “fell in love” and want to visit her gullible “future husband” in person. There is only one problem. Girl doesn’t have money to buy tickets, pay for visiting visa, etc. (other bogus “reasons” may be used too). So if man wants to see the “girl”, he has to help her, with few thousands of dollars. And, by the way, money should be sent through Western Union.



### Warning Sign

Western Union is the preferred method of payment in almost any scam. If you’re asked for whatever reason to pay through Western Union to your international customer/partner/ “lover” etc, chances are very good that this is a scam.

Victim is excited by the illusive perspective to meet beautiful woman soon, so he sends the money.

On the day when “the bride to be” is expected to arrive, poor victim is notified by a fictitious “Dating service agency” that there is another problem. Recently a new regulation was passed that requires a woman to carry a few thousands dollars (or euros) in cash before she’s allowed to enter the foreign country.

“Agency” agreed to lend a woman part of the money (usually about 25-30%), but the victim has to wire the rest. And yes, you guessed it right. Money should be wired by Western Union.

When the cash is wired, man never hears from “agency” or woman again. Email accounts used for communication with “beauty” and “agency” are deleted, and that’s the end of a story.

Variation of the scam may be that girl writes to a victim and “shares” with him that she is in some sort of trouble – her wallet is stolen, one of her parents is ill and may die unless expensive operation is performed. I can’t describe all the bogus stories used for the purpose of parting the victim with his money. Simply use common sense to avoid the trap.

## “The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

The worst scenario may occur if the groom will decide to visit “bride”, instead of sending money. Victim can be kidnapped and held for extortion. Of course this will happen only if a victim is dealing with criminals, not with real brides.

Now when you know how this scam works, if you want to try finding your love in Russia or FSU, all you need is a **few tips** that will help you distinguish between real brides and criminals.



The process of getting to know each other is very personal and gradual. Real woman wouldn't “fell in love” with you during the first month of communication. And she wouldn't ask to send her money right away, especially by Western Union.

Also, in her letters she would try to address your personal questions. If you see your name only in the beginning and the end of the letter, and if your questions are not properly addressed, and letters only cover “love you” topic, then most likely it's a scam. Your name appears only at the beginning and the end of the letter, because criminals simultaneously send the exactly same letter to hundreds or even thousands of other gullible grooms. They are not willing to spend time thoughtfully answering your questions; they will avoid mentioning the names of any particular places (otherwise the letters sent to groom in LA won't work for the guy in New York).

Let's suppose that a groom in question is a doctor. So real girl would write to him mentioning his profession, asking where he works, what medical college has he graduated from, etc.

Criminals usually wouldn't bother to write such personal letters, because in this case a letter for doctor won't fit if it's written to a programmer, for example.

Pay close attention to the photos you see on a profile. If photo is too good to be true, probably it is. If you see several shots that done by professional photographer in a model-like environment, chances are pretty good that those are indeed the pictures of some foreign model or actress, not of a real girl. Real girl simply doesn't exist.

Another way to diminish chances of being defrauded is to ask for phone conversation with a girl. Criminals don't like that. And if you require several conversations, most of them will disappear, it becomes too difficult to “manage” you, easier to find another prey.

Even if you think that girl is genuine, don't send her money directly; offer to pay for the ticket. There is no interest for criminals to get the ticket with exact departure date earmarked for exact person, especially if you buy e-ticket. That is the ticket the girl should pickup at the airport the day of departure.

And one more thought. (This is especially true for the grooms from the USA, and somewhat true for the grooms from other countries.) It's not so easy for a young lady from Russia or FSU to obtain a visiting visa. Lady should be able to show that she's

## “The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

independent, has assets and property, etc. Not many are lucky enough to have this level of income. Believe me, if a young lady from Russia can meet all current requirements made by an embassy, especially by the USA embassy, for those who wish to enter it's country, then this lady most likely has enough money not only to buy a ticket for herself, but for you as well!

**Bottom line:** never offer money yourself, do not offer girl to visit you in your country. If criminals are very clever, they may answer on your personal questions, and they won't ask you for money right away, but they will have to ask for it eventually. That's the only point of communicating with you. If you become a “high-maintenance” guy – asking for phone conversations, sending many letters requiring personal response and not offering money despite of their hints – they will loose interest in you soon. I would say that you will start receiving rather direct hints or requests for money from crooks at the end of the first month of communication, the latest.

Real girl will continue to communicate with you if she's interested in you as person, not in your wallet. She won't mind to talk with you over the phone. And she won't write to you in her first letters that she “felt in love with you”.

Nigerians also use this scam. Details of the scam are very similar. Only money should be sent in Nigeria instead of Russia and the legend may be that “girl” is not a Nigerian by origin. If “she” is communicating with American guy, she could be an American who is in trouble in Nigeria. If “she” is talking with European, then she is a girl from Europe, etc.

That's basically all there is to know about Russian Dating Scam.

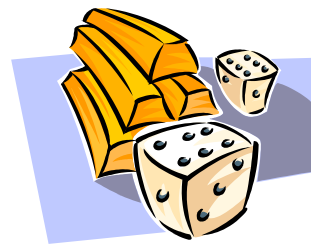
## Useful Resources

If your marriage is in a shaky phase or you could use some help finding your significant other, check the following sites:

How To Be Irresistible To Women/Men, How to Put an End to the Stress and Anxiety of Not Knowing What to do to Save Your Troubled Marriage, and more:

<http://www.1ezhost.biz/romance.html>

## 4. HEALTH SCAM



The scammers, who bilk out millions of dollars out of consumers in this scam, use another emotion as a trigger point – hope.

They give false hope for quick cure from a variety of problems and diseases, from cancer and AIDS to obesity or offer expensive medicine for a very cheap price. Let’s talk about “cheap medicine” first.

### Here is how Health scam works

There are hundreds of websites out there that sell expensive drugs below market price. What they are really selling is hope.

What should person do if she/he can’t afford healthcare insurance? What if all the money is already spent on expensive drugs and there is no way to pay for visit to the doctor to get the prescription required for buying that drug in a pharmacy?

What many people will do, they visit those “pay less for the same medicine” sites and hope to finally get that necessary medicine that otherwise they couldn’t afford. And prescription on those sites is not required either.

So people pay for the drug and may even get it delivered to them. In order to pay for the drug, they submit their credit card information, their addresses, etc. And rather often later on they see other charges on their accounts for the products and services they never ordered.

That is how they become victims of Identity Theft. I will describe this threat in details later, but I wouldn’t list the Health scam as a 4<sup>th</sup> most dangerous online scam if it only would threaten your wallet. This scam is listed so high, because it could potentially threaten your life.

In reality, consumers never receive actual drug, they receive either expired medicine or faked and potentially dangerous counterfeit drugs that were too strong or too weak, contained dangerous ingredients, etc.

Here is a quote from official FDA (Food and Drug Administration) website:



*“Patients who buy prescription drugs from Websites operating outside the law are at increased risk of suffering life-threatening adverse events, such as side effects from inappropriately prescribed medications, dangerous drug interactions, contaminated drugs, and impure or unknown ingredients found in unapproved drugs.”*

## “The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

*“...sale of unapproved drugs and the illegal sale of approved drugs over the Internet poses a serious public health risk. We know, for example, of many adverse events resulting from the use of the drug GBL and the date rape drug GHB, which are unapproved drugs sold illegally over the Internet.*

*FDA learned recently of a person who was harmed by the use of Viagra purchased from a Website without an examination by a healthcare professional. Unfortunately, the man had a family history of heart disease and died after taking the drug.*

*We also know of cases where people choose the Internet for treatment to avoid consulting a health care professional. These consumers, however, run the risk of purchasing inappropriate drugs or unknowingly purchasing counterfeit or sub-potent drugs. “*

<http://www.fda.gov/oc/buyonline/faqs.html>

### **So how to make sure that you purchase drugs from a legitimate site?**

**Note:** This advice is mostly related to the consumers from the USA, but I’m sure that similar procedures should be followed for the consumers from other countries. Find the health control organization in your country, similar to FDA, and follow its recommendations.

If you’re a consumer from the USA, first make sure that website in question is US state-licensed pharmacy. You can consult your state’s board of pharmacy to find out if this website is in a good standing.

You can find your state’s board of pharmacy on the National Association of Boards of Pharmacy (NABP) website: <http://www.nabp.info/>



### **Warning signs**

- ◆ Prices are dramatically lower than that of other legitimate sites.
- ◆ No phone provided in a contact information for the website.
- ◆ Prescription is not required.

Other fraudsters target people with serious conditions for which no cure has been found yet, such as multiple sclerosis, diabetes, Alzheimer's disease, cancer, arthritis, HIV and AIDS.

It’s not easy to prevent fraud for this group. Those people know that there is no cure, so they are ready to try anything that could give them even a slightest glimpse of hope.

If you (or somebody you love) have one of these diseases, please know that there is always hope, and God is able to help you, but you need to carefully research the source that is offering, “cure”, before buying it.

## “The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

The least I can do is provide information about resources that are offering help and working on solutions for those diseases.

### **For information**

#### ***On Cancer research and treatment:***

Please call the National Cancer Institute's Cancer Information Service at 1-800-4-CANCER (1-800-422-6237) or visit <http://cancernet.nci.nih.gov/>

#### ***On HIV and AIDS:***

Please call HIV-AIDS Treatment Information Service at 1-800-HIV-0440 (1-800-448-0440) or visit <http://www.hivatis.org/>

#### ***On Arthritis:***

Please call Arthritis Foundation at 1-800-283-7800 or visit it's website at: <http://www.arthritis.org/>

#### ***On Alzheimer's disease:***

Please call 1-800-438-4380 or visit NIA's Alzheimer's disease information website: <http://www.alzheimers.org/>

#### ***On Diabetes:***

Please call CDC Diabetes Public Inquiries Call toll-free 1-877-CDC-DIAB or visit: <http://www.cdc.gov/diabetes/>

#### ***On multiple sclerosis:***

Please visit National Institutes of Health website: <http://www.nlm.nih.gov/medlineplus/multiplesclerosis.html>

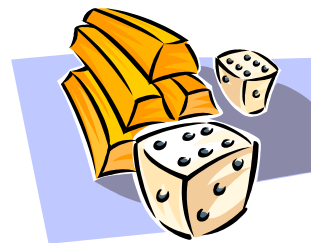
## **Useful Resources**

On this page you can find solution for some of the most widespread health problems, such as:

- acid reflux and painful heartburn,
- anxiety and panic attacks,
- how to stop using low carb, low calories or low fat diet,
- how to loose fat permanently and without drugs,
- and more ...

<http://www.1ezhost.biz/health.html>

## 5. JOB POSTING SCAM



Let's say a person works for some company as an employee. He's tired of his current job, or he wants to change it for some other reasons, maybe he's moving to another place. He is not ready yet to start his own business (or simply doesn't want to do it at all.). He just wants to find a new job with a steady (and preferably bigger) paycheck.

Ok, so what does this person normally do? He looks for a desirable position either in the newspapers or on the Internet. More and more people go to the job postings sites like Monster.com, HotJobs.com, etc and they look for the job positions that match their requirements. Victim may also submit his resumes on job posting sites.

### Here is how Job Posting scam works

Let's assume our victim found the post describing the position that he likes, so he submits his resume for this position. Or he might receive a letter from a potential employer that notifies the victim his resume was found online and that he might qualify for particular position.

Either way, the victim is required to fill out additional information. He might even be asked to provide his SSN for "routine background check". Victim, in a foretaste of great job, submits all the required info. But instead of getting a great position, he ends up being a victim of Identity Theft.

As you realize by now, this job opportunity was not real. It's a scam.

Unfortunately, victim gave up a little too much information, so criminals not only use his credit cards and bank accounts to buy goods and services (as in ordinary identity theft), but they also open new accounts, apply for new credit cards.

In fact, they may decide not to use his current cards at all, to avoid triggering his attention after he would receive a huge bill. Instead, new credit cards and bank accounts are created and the bills are sent to a different address. And victim has absolutely no idea that this is happening. Until one not-so-bright day he applies for a new credit card himself or for a loan/mortgage and his application is denied. When he requests the reason for denial, he finds out that he is in debt up to his ears.



### Warning signs

- ♦ Look at the contact information on the website. If there is no contact phone number listed, this is the major warning sign.
- ♦ Search the name of this company on one of major search engines – I usually use Google for this purpose. If the company is phony,

## “The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

chances are pretty good you will find other references for “scam” or fraud” related to the name of this company.

- ◆ Also, you might want to check how long ago the domain name for this site was registered. If the domain was registered a few months ago, then in most cases this is a scam too. A well established company should have website that has been online at least for a few years.

Go to: <http://www.networksolutions.com/whois/index.jhtml> and enter the domain of the website in question, click “Search” and on the page that appear look for “Domain Registration Date”.

Less dangerous option of the job scam is when “government jobs” are advertised, such as a Post–Office openings. In this case scammers want you to pay for a “study course”.

More details about it you can find on a FTC website:

<http://www.ftc.gov/opa/2005/11/jobscam.htm>

## Useful Resources

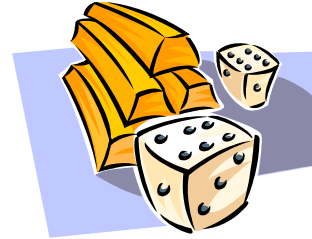
If you’re looking for a new job or want to completely change your carrier, you might find this page helpful:

<http://www.1ezhost.biz/find-job.html>

You will find there the following:

Complete Interview Guide  
Professional Resume Writing Service  
17-Yr Hr & Interview Expert Reveals All,  
and more ...

## 6. ONLINE AUCTIONS SCAM



This scam is also often called “Overpayment Scam”.

### Here is how Online Auctions scam works

Criminals usually peruse online auction sites like e-bay and target sellers of high-ticket items, such as cars, horses, pets, etc. Then they send a request to seller asking if he is ready to ship an item to another country. They often offer to pay more than seller’s asking price to compensate him for an “inconvenience of shipping to another country”. Another question they are asking if the seller is ready to ship the goods right away after receiving the payment, because, for one reason or another, they need to get this item as soon as possible.

When the seller answers that he is ready to ship as soon as he receives money order or when bank check is cleared, buyer informs the seller that another business owes buyer substantial amount of money, usually much more than buyer have to pay for the merchandise, so it will be simpler if that business would send a check or money order for the whole amount directly to the seller. And the seller would subtract his payment from that amount and send the rest to the buyer.

Seller receives money order or bank check from that third party for the amount that is much bigger than he agreed to sell his merchandise for. Money order or check looks real and is accepted by the bank. So seller ships the merchandise to the buyer and also wires him through Western Union or Money Gram the difference between the money he received and the selling price of his merchandise.

Unfortunately, about a week later, seller is informed by his bank that the check is fake. And the bank holds the victim responsible for the amount he wired out of his account. So seller loses not only his merchandise (car, for example), but a lot of money as well.

What wholesaler doesn’t know about is that it takes up to 2 weeks to clear international payment. And that if bank Okayed the check, it doesn’t mean it won’t hold you responsible in case of a fraud.

Sometimes, to make a seller feel secure, “buyer” offers to use an escrow company for the transaction. Of course it’s always should be only an escrow company recommended by the buyer, because “he was burned by other escrow companies”, etc. There could be many different reasons why that particular escrow company should be used for this transaction.

So seller is assured by an officially looking letter from an “escrow company” that money from the buyer are received and will be released to the seller as soon as he ships the

## “The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

merchandise. Merchandise is shipped; the seller never receives money. “Escrow company” disappears. As you guessed by now, it’s never existed in a first place.

### How to avoid this scam?

For starters, read about safe online trade recommendations on FTC website:

<http://www.ftc.gov/bcp/online/pubs/online/auctions.htm>

Never agree to send an item until check actually clears. Never go for a sob story and agree to accept the payment when you should send part of the money back.

For all the transactions, especially international ones use the escrow company of your choice, not the one recommended by “buyer”.

Many auction sites offer feedback rating of some sort. Always check this rating. Keep in mind that a seller and his accomplices can artificially boost high feedback rating. However if a buyer has a Power Seller status or a positive feedback over 90%, it might indicate some reliability. You only should take this into consideration as one of the factors. I wouldn’t recommend to completely rely on a feedback rating.

### Latest modification



Lately I have noticed more sophisticated scam that is somewhere in the middle between “Job Posting” Scam and “Online Auction” scam. Victim is offered a job as a “payment processor”. Foreign company contacts a victim, informs him that it wants to hire him.

Victim’s job is to accept the payments for the services provided by the company in the victim’s country and to transfer those payments by Western Union to the company. As a payment, victim is offered from 5 to 15% of the amount of the transaction. The rest of the story is the same. Check is accepted by the bank as legitimate, money is wired, later on fraud is discovered and the victim is hold accountable.

### Useful Resources

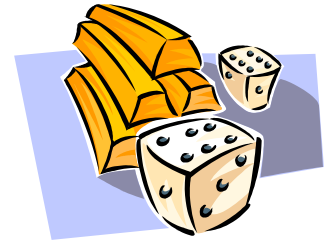
If you’re interested to learn how to find real bargains through online auctions, here is a web page you might want to check out:

<http://www.1ezhost.biz/online-bargains.html>

You will find:

- Car Bargains
- Dirt-cheap electronics
- Guide to Government and police auctions,
- and more ...

## 7. EBAY/PAYPAL/ANY BANK “ACCOUNT CONFIRMATION” SCAM



This scam is also known as phishing scam. Principle of this scam is very simple. Nevertheless people loose a lot of money in it.

### Here is how Online Auctions scam works

Victim receives notification by email from “PayPal”, “eBay” or his “bank”. Victim is notified that for security reasons he needs to verify that this email address belongs to the holder of the account, so he needs to click on a confirmation link, which is provided within the e-mail, and log in to his account. Or he may be notified that there are some billing issues that should be resolved. Or hundreds other reasons could be used.

Email looks legitimate, it’s been sent from company’s email address (at least that what victim thinks). So victim clicks on a link, and logs in to his account. What he will do further is not important, because he just gave his account details to the criminals. And they will study his account, find credit cards and will use them as they see fit. They also will clean up his account from any money he has.

Below are just a few emails I received lately; I lowered my anti-spam filter in order to receive all this junk and to show you examples of phishing emails.

Here are just a few subjects of phishing emails:

- ◆ PayPal Billing department  
Subject: Please Restore Your Account **Acess**

NOTE: I don’t correct grammar mistakes on purpose; I just highlight them for your convenience.

- ◆ Customer Support  
Subject: PayPal Notification (Your account is suspended)
- ◆ Info@paypal.com  
Subject: Unlock your account
- ◆ “service@paypal.com”  
Subject: Inactive Customers Removal - Please Update Your Account
- ◆ Safeharbor Department Notice

## “The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

Subject: eBay Safe Harbour Section 9

- ◆ eBay Services Online Banking  
Subject: System maintenance, Please Reactivate your eBay Online Access!
- ◆ eBay Inc.  
Subject: Password Change Required
- ◆ eBay Billing Department  
Subject: Warning ! Credit/Debit card update
- ◆ eBay Security Center  
Subject: Billing Issues
- ◆ “eBay”  
Subject: Become an eBay Power Seller



NOTE: This one is more dangerous, because you're not asked to update account info, instead you're offered to join EBay Power Seller program. In reality, there are rather strict requirements you have to meet in order to become E-bay Power Seller).

- ◆ Wells Fargo Online  
Subject: Important Notice!
- ◆ Wells Fargo Staff  
Subject: Please Restore Your Account Access
- ◆ update@amazon.com  
Subject: Please Update Your Amazon Account!
- ◆ Commercial Federal Bank Security Service  
Subject: Confirm your Online Banking records
- ◆ Credit Union National Association  
Subject: CUNA Limited Account

So **how to protect yourself** from this scam? It's actually very simple. Delete all those emails. And never click on a link within such an email. If your credit card really expired or you have other billing issues, EBay, PayPal and any other legitimate service will notify you about it when you login to your account. Just don't login through the links sent in an e-mail, go to the website, for example, to login to PayPal, go to PayPal.com, to login to eBay, go to eBay.com, etc.

## “The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

If you click on a link, the best thing you can get is to be re-directed to the fraudsters website and the worse thing, you can actually catch a very dangerous virus that will cause you a lot of problems.



If you want to play a detective, I can show you a few things that will help you to define that this email is a scam. Then report a scammer to the [Internet Fraud Complaint Center](#).

This site is a product of combined efforts of FBI and National White Collar Crime Center.

Ok, here is what you should do. First of all, you need to find the full header of the email. In some email programs you may see a full header when you click on “forward” button, others have “full headers” button, yet in others you have to know where to look. In Microsoft Outlook, for example, when you open an email, you need to go to “View” – “Options” – and at the bottom of the screen you will see a box labeled “Internet Headers”. That’s what you need.

Ok, I will analyze one email as an example of how it could be done.

**From:** "PayPal Inc Department" <service@paypal.com>  
**Reply-To:** "PayPal Inc Department" <service@paypal.com>  
**To:** \*\*\*\*\*  
**Date:** 26 Nov 2005, 03:51:21 PM  
**Subject:** Verify And Update your Paypal account !

HTML content follows

As part of our security measures, we regularly screen activity in the PayPal system. We recently noticed the following issue on your account:

We would like to ensure that your account was not accessed by an unauthorized third party. Because protecting the security of your account is our primary concern, we have limited access to sensitive PayPal account features. We understand that this may be an inconvenience but please understand that this temporary limitation is for your protection. Case ID Number: PP-072-838-482

<https://www.paypal.com/us/cgi-bin/webscr?cmd=complaint-view>

For your protection, we have limited access to your account until additional security measures can be completed. We apologize for any inconvenience this may cause.

To review your account and some or all of the information that PayPal

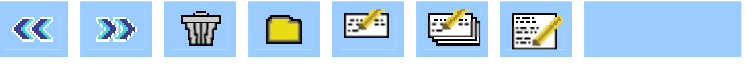

## “The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

To review your account and some or all of the information that PayPal used to make its decision to limit your account access, please visit the Resolution Center <https://www.paypal.com/>. If, after reviewing your account information, you seek further clarification regarding your account access, please contact PayPal by visiting the Help Center and clicking "Contact Us". We thank you for your prompt attention to this matter. Please understand that this is a security measure intended to help protect you and your account. We apologize for any inconvenience.

Sincerely,  
PayPal Account Review Department

PayPal Email ID PP645495

Top of Form

delmsg	INBOX
	
Message 12 of 515 (New)	
	

Move to:	Sent	Go
11	1133038004.M98	

Bottom of Form

As you can see the short header looks legitimate, and email address service@paypal.com theoretically may belong to paypal.

Now let's analyze the full header:

**Delivered-** \*\*\*\*\*  
**To:**  
**Return-Path:** <service@paypal.com>  
**Received:** from 10.0.0.1 (softdnserr [::ffff:85.204.169.108])  
by server\*\*\*.\*\*\*.com with esmtp; Sat, 26 Nov 2005  
15:46:42 -0500  
**Received:** from 108.112.55.75 by ; Sat, 26 Nov 2005 15:45:21 -  
0500  
**Message-Id:** <OHNIWFDKDPDEDQVOFLTNMI@yahoo.com>  
**From:** "PayPal Inc Department" <service@paypal.com>  
**Reply-To:** "PayPal Inc Department" <service@paypal.com>

## “The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

**To:** \*\*\*\*\*  
**Subject:** Verify And Update your Paypal acoount !  
**Date:** Sat, 26 Nov 2005 13:51:21 -0700  
**X-Mailer:** Microsoft Outlook Express 6.00.2600.0000  
**Mime-Version:** 1.0  
**Content-Type:** multipart/alternative;  
boundary="=\_server\*\*\*\*.\*\*\*.com-32257-1133038004-0001-2"  
**X-Priority:** 1  
**Priority:** High  
**X-Msmail-Priority:** High

You may notice \*\*\*\*\* in the header, I changed my email address and the server on my side that received e-mail to \*\*\*\*\*.

What is important though, is to look at the Received: from field, I marked the IP address of the sender in yellow.

In this case IP address is provided instead of email address, sometimes you see email address instead, such as cisp1.c-i-s-pl.com or james@ns.ratchaburi.com

Obviously those email addresses have nothing to do with PayPal, so you can tell right away it's a scam.

In our case it's a little more complicated. First, we can ping paypal.com to find out its IP. We got: 216.113.188.34 Of course, PayPal probably has hundreds of different IPs, but they all will be “216.113.188.” Last 2 digits may vary.

Now let's go to [ARIN WHOIS Server](#) and find out the network hosting 85.204.169.108

Here is what we got:

### Search results for: 85.204.169.108

OrgName: RIPE Network Coordination Centre  
OrgID: [RIPE](#)  
Address: P.O. Box 10096  
**City: Amsterdam**  
StateProv:  
PostalCode: 1001EB  
**Country: NL**

## “The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

ReferralServer: whois://whois.ripe.net:43

NetRange: [85.0.0.0](#) - [85.255.255.255](#)

CIDR: 85.0.0.0/8

NetName: [85-RIPE](#)

NetHandle: [NET-85-0-0-1](#)

Parent:

NetType: Allocated to RIPE NCC

NameServer: NS-PRI.RIPE.NET

NameServer: NS3.NIC.FR

NameServer: SEC1.APNIC.NET

NameServer: SEC3.APNIC.NET

NameServer: SUNC.SUNET.SE

NameServer: TINNIE.ARIN.NET

NameServer: NS.LACNIC.NET

Comment: These addresses have been further assigned to users in

Comment: the RIPE NCC region. Contact information can be found in

Comment: the RIPE database at <http://www.ripe.net/whois>

RegDate: 2004-04-01

Updated: 2004-04-06

So now we know that this email was actually sent from the server located in Amsterdam. And obviously PayPal staff wouldn't send you email from Netherlands. Now you know for sure it's a scam.

However, don't jump to conclusion that if email was sent from this server, then your offender is in Amsterdam. The fact is, he may be anywhere. Yes, this server was used to send you email, but it could be used as a “departure point” only. Sophisticated hackers use a chain of proxy servers before finally re-directing their emails to the “departure points”. So chances are that that ISP in Amsterdam is innocent.

To investigate this deeper, you have to be an expert. This subject is out of scope of this e-book. I just showed you a few steps that could help you verify that email you received is a scam.

You can also verify that you received a scam by clicking on a link in the email itself, but I would recommend you to go the root described above instead. Why? Because when you click on this link, you may catch some nasty viruses, and then you will have Identity Theft problem.

I will describe to you what will happen when you click on the link in the email, OK? So, after I clicked on the link in the email (I marked this link in red), I was re-directed to the site that has the following link in the address bar:

<http://reform21.co.kr/webscr/update.html>

This page mimics PayPal login page to the “T”.

## “The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

But, as you understand, this link has nothing to do with PayPal. If it would be a real request from PayPal, I would end up on a login page that would look something like this:  
[https://www.paypal.com/cgi-bin/webscr?cmd=\\_login-run](https://www.paypal.com/cgi-bin/webscr?cmd=_login-run)

Notice the “www.paypal.com” part, it has to be present in a real link, if it’s from PayPal. Also, you may notice that “https” is used in the link instead of “http”. This identifies SSL, a secure protocol used by legitimate companies for secure connections.

Also, the same re-direction will occur if you click on a link for “PayPal Resolution Center”. This link is marked in red too. If you will move your mouse over this “www.paypal.com” link, you will notice that it’s actually re-directing you to the same link:

<http://reform21.co.kr/webscr/update.html>

When I checked the register information for this domain, it turned out that it’s registered in Korea! Obviously, has nothing to do with PayPal.

It’s not always that simple to identify a scam.

When fraudsters are smart, they actually re-direct you to the right page when you click the link in the email. What you don’t see is that when you clicked on that link, a virus may be installed on your computer with a tiny piece of software called keylogger. Keystroke logger is software that monitors each keystroke you type on your keyboard. So now when you type your user and password, this info is transferred to the scammer.

Bottom line: simply delete those emails and you will save yourself a lot of trouble.

Another version of phishing scam is when a victim receives an offer to buy highly priced software, such as Adobe Suite, for example, for pennies. Well, fraudsters don’t care at what price will they sell software, because they are not going to deliver it at all. All they need from a victim is payment information – Credit card, address, name, etc, so that they could commit Identity Theft.

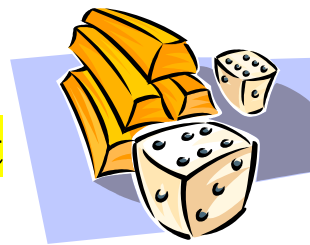
## Useful Resources

eBay® is one of the most powerful sources for generating passive income, so you might want to start selling some junk from your house. Surprisingly, you could get a pretty good price for what you consider to be a “junk”

If you’re interested to learn more about eBay, you might want to check out this page:  
[http://www.1ezhost.biz/online\\_auctions.html](http://www.1ezhost.biz/online_auctions.html)

Discover the ultimate garage sale techniques and secrets of how to find the high profit items just like the eBay® pro's, find out how to Get Rewarded For Helping People Save Money On eBay®, and more ...

## 8. IDENTITY THEFT – VIRUSES, WORMS, TROJANS and their most dangerous variation – RATs



When viruses, worms and Trojans sneak in the victim's computer, it means this victim is in a lot of trouble... His PC soon may be crushed, hard drive can be completely wiped out and a poor victim may even find himself a victim of Identity Theft. All usernames and passwords from his computer may be maliciously exploited. God forbid if a victim holds crucial information on his computer (such as his SSN or mother's maiden name or user and password to access online banking account).

### How those “creatures” penetrate into user's PC?

There are many ways. The most popular one is through emails and online greeting cards. Basically, the rule of thumb is if you don't recognize a recipient – do not open email. Delete it immediately. Especially if this email came with attachment. Basically, any email, unless it's a text only email, can include a virus or worm of some sort, even innocent-looking html emails could be dangerous. We also talked earlier about phishing scams, please remember not to click on links that invite you to change your payment information. Go directly to the web site itself and log in there.

Another way for all those things to get into user computer is if a user visits “questionable sites” – porn sites and WAREZ sites would be a good example. User thinks he is downloading useful shareware program or desirable video, but what he's really getting is a big headache – a bunch of viruses of all sorts and kinds.

As I mentioned previously, keyloggers may be installed along with viruses and Trojans. In this case, even if you don't keep crucial personal information on your computer, hackers can still get it when you log in into your online banking account.



Trojans now are even more dangerous than before. If in their previous versions, they had to be downloaded to the computer by user, one way or another (through emails, shareware downloads, etc). Now there are Remote Access Trojans (RATs) that crawl the Internet and self-install on computers without user “participation” whatsoever. Those RATs exploit various software vulnerabilities to break into user's PC.

Unfortunately, in this case, user has no idea that he's under attack and his crucial personal and financial data soon might be stolen.

**Is there a protection from this evil?** Yes, there is.

## “The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

First of all, you should use firewall for your computer, either software firewall or hardware one. It's better to have both.

You will need not only firewall, but anti-virus/anti-spyware program as well.

So I would recommend you to get Norton Internet Security, which includes Norton AntiVirus™, Norton™ Personal Firewall and many other goodies.

[ZoneAlarm® Internet Security Suite](#) is good too. If money are tight, at least install [ZoneAlarm®](#), you can download it for free. It's limited in functionality, but it's still better than keep your computer wide-open to malicious attacks.

Here are a few inexpensive hardware firewalls that I would recommend you to use along with your software firewall:

**D-Link** Express EtherNetwork DI-604

**Linksys** Etherfast Cable/DSL Firewall Router BEFSX41, 4-port, VPN, DMZ, SPI

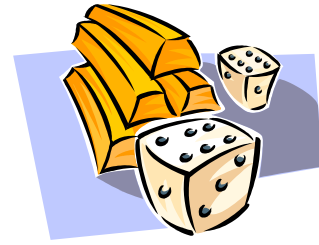
**Netgear** FR 114P ProSafe Firewall

### Useful Resources:

Free Spyware Scan from a company that offers leading edge integrated application solutions to give you peace of mind that your computer is secure and your privacy is protected. They will protect you from unwanted Spyware, Adware, Malware, W32/Spybot, Keyloggers, Unwanted Toolbars, Browser Hijacking, Pop-up Generators and more:

<http://www.1ezhost.biz/anti-virus.html>

## 9. IDENTITY THEFT – SPYWARE, ADWARE, MALWARE, HELP OBJECTS, AUTOMATIC LOGINS



In the previous section we discussed viruses, worms, etc. The main difference between them and miscellaneous spywares is that viruses can harm your computer and usually like to propagate to other computers as well (through your address book, for example).

Serious viruses will crush your computer. Purpose of viruses is to create enough wholes in the walls of your “home” so that the key from the door is no longer required. After that your computer will be hacked and the hacker will gather all the data you have on your computer. Different “wares” on another hand won’t destroy your computer. You won’t even notice them. Adwares are less dangerous, because it’s a pieces of software installed by legitimate companies. What it does, it embeds ads in the free version of a program you download. When you open freeware software, those ads will show up. If you don’t want the ads – pay for the registered version and ads will be disabled.

There are also different types of spyware that often are represented as “adware”. Those to programs track and analyze your Internet surfing habits, identify what products you buy online, etc. Usually the fact that a user may get a spyware along with a freeware he downloads, is not mentioned. Very convenient for advertising and marketing companies, less convenient for you as a user, because your privacy is violated without your consent. Spyware, despite of its name, is considered to be legal type of software.

There are other types of “ware” that are very dangerous. Sometimes they are called spyware, but actually they are malwares or collectwares. They sit quietly on your computer, gather crucial information and then mail it to fraudsters.

I already recommended in the previous section a few protection solutions, which include anti-spyware programs as well.

Another anti-spyware program worth exploring is Microsoft Windows AntiSpyware (Beta). You can download it here:

<http://www.microsoft.com/athome/security/spyware/software/default.mspx>

However you need to understand that all those firewalls, anti-virus and anti-spyware programs won’t save you if you don’t follow other **common-sense procedures**.

- ◆ Do not use automatic log in option. It’s not only easier for you to login, it’s also easier for hacker to login instead of you. When creating passwords, use digits and letters, use upper case and low case, use not less than 8-9 symbols in your password. Don’t forget to log off from your account when you’re done.

If you use short passwords, you make a life of a hacker much easier.

## “The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

- ◆ Regularly update your virus protection programs, don't forget to install patches for your operating system.
- ◆ I would highly recommend NOT to store your financial information on your computer.
- ◆ And remember about those un-known emails and e-greeting cards – just delete them.
- ◆ It's also a good idea to regularly back up your system. This way if your computer is compromised, you may always restore it to the previous condition.



It's better to use image based back up tool, not file based.

Excellent software for this purpose is Acronis True Image, you can also try Tk8. You can find both of these backup software, plus other recommended resources on this page:

[http://www.1ezhost.biz/backup\\_software.html](http://www.1ezhost.biz/backup_software.html)

- ◆ To find out, if your identity is safe, order your credit report. You're entitled to one free report per year from each of the credit reporting companies - Equifax, Experian and TransUnion, so go grab yours now from [annualcreditreport.com](http://annualcreditreport.com). I would advise you order 1 report at a time. You can order one today, next in 4 months, and the last one in another 4 months. This way you will have information about your credit status all year around. If you didn't check your report for a while, do it now! However, you don't get a free credit score with federal law credit reports. Here is how you can find out your credit score:

[http://www.1ezhost.biz/credit\\_report\\_check.html](http://www.1ezhost.biz/credit_report_check.html)

### **What should you do if you suspect your Identity was stolen?**

If you noticed some suspicious activity on your report, such as request to change address or a new account/credit card is open that you didn't open yourself, you need to contact all 3 Credit Bureaus and ask them to put a “fraud alert” on your credit file.

#### **TransUnion**

Fraud Victim Assistance Department

Phone: [800-680-7289](tel:800-680-7289)

Fax: [714-447-6034](tel:714-447-6034)

P.O. Box 6790

Fullerton, CA 92634-6790

#### **Equifax**

Consumer Fraud Division

Phone: [800-525-6285](tel:800-525-6285) or: [404-885-8000](tel:404-885-8000)

“The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

Fax: [770-375-2821](tel:770-375-2821)

P.O. Box 740241  
Atlanta, GA 30374-0241

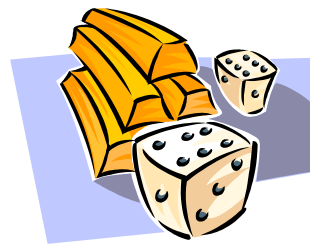
**Experian**

Experian's National Consumer Assistance  
Phone: [888-397-3742](tel:888-397-3742)

P.O. Box 2104  
Allen, TX 75013

Also, you might want to read FTC article about fighting identity theft:  
<http://www.ftc.gov/bcp/online/pubs/credit/idtheft.htm>

## 10. “CHANGE OF HEARTS” – shift from OS to software



*According to Reuters “Online criminals shifted their attacks in 2005 from computer operating systems such as Windows and others to media players and software programs”.*

*The most vulnerable and often attacked programs are Internet Explorer’s browser, Office and Outlook Express.*

*Also, hackers more often started targeting anti-virus programs and hardware routers (used as firewalls). Those routers often have their own operating systems, which could be targeted the same way as any other OS.*

Another big threat you should aware of comes from your “toys”. You think you have pretty cool gadget -your new cellular phone with pretty pictures, your i-pod, and wireless gadgets for your laptop... Unfortunately, they all are even less secure and more vulnerable than your desktop PC. And experts predict that there will be more viruses next year that will specifically target all those wireless devices. Do not store critical data there. Or scammers will take advantage of you.

And finally, the last “trend” for 2006. Earlier hackers spread viruses and spyware randomly, they usually didn’t target any company in particular. Now attacks become more and more targeted. Gambling sites are among those who suffer the most losses through cyber-extortion. Hackers contact them and blackmail to shut down the operation by launching DDOS attack if they don’t pay. Billions of dollars are in stake for gambling sites, so they often prefer to pay a relatively small amount (about \$30 - \$50 thousands) in order to stay online during such events as Superbowl.



Unfortunately, criminals begin targeting independent Internet marketers as well. Even small companies can be attacked. Of course, small companies are not interesting for big organized crime groups, so they become a prey for not-so knowledgeable hackers who can’t attack banks and bookmakers.

If you want to know how to protect your site from most attacks, I would recommend you to get excellent report written by security expert Nick Temple “Don’t Get Hacked “  
<https://paydotcom.com/r/260/1ezhost/134282/>

Also, you might be interested to know that our company, [1EzHost L.L.C.](http://www.1ezhost.biz/) now offers complete design and development of secure e-commerce websites. As you know, such solutions cost many thousands of dollars, but not with us. With us, you pay an affordable down payment and then we together work out a payment plan that suits your budget.

“The 10 Most Dangerous Internet Scams You Absolutely Have To Know About”

We're offering you a unique opportunity to develop your Custom e-commerce solution that won't cost you arm and leg! Interested?

<https://paydotcom.com/r/3794/hunteridge/134323/>

## CONCLUSION

Now you know about the 10 most dangerous Internet scams.

Go ahead and tell your loved ones, your friends and family about them. May be somebody close to you already received similar letter. He knows that the offer sounds to good to be true, but deep down he hopes that he was uniquely chosen for the conduction of this operation. And that's his chance to finally get what he wants – that new car, house, the vacation he dreamed about his whole life... And may be he is considering to try his “luck”.

Don't wait until it's too late, use this e-book to educate and help others.

Be safe,

Oleg Ilin

© Oleg Ilin, [1EzHost.biz](http://www.1ezhost.biz) All rights reserved. No portion of this e-book may be changed or reproduced in any way without the expressed written permission from Oleg Ilin. This is a Free E-book and it cannot be sold.

It can be given away free as long as it is not used in any form of Spam or non-permission based marketing. All violators will be prosecuted to the fullest extent of the law.

### Trademarks

Company names or product names mentioned in this e-book are trademarks or US registered trademarks of their respective companies.

eBay and PayPal are either registered trademarks or trademarks of EBay Inc. in the United States and/or other countries. All other trademarks are the property of their respective owners.