

Exposing Email-Borne Fraud

Volume 1 - Advanced Fee Frauds

a.k.a. Nigerian 419 scams, 419 scams, 419 fraud, Nigerian scams or 419

www.vircom.com



© 2004 Vircom, Inc. All rights reserved.

Table of contents

Preface	3
Contributing experts	
Introduction	4
Methodology	4
The scam	5
Step 1 - The introduction	5
Step 2 - The setup	8
Step 3 - The suits	10
Step 4 - The paperwork	12
Step 5 - The score	13
Step 6 - The aftermath	15
Our Advanced Fee Fraud scammer	15
Another instance of Advanced Fee Fraud	16
Fraud FAQ	17
Protecting yourself against Advanced Fee Frauds	18
About Vircom	19
About the SpamBuster Team	
For more information	
Appendix 1	20
Appendix 2	21

Preface

As part of our mission to improve and help fully legitimize email communications—and in an effort to educate the public on the complexities of Internet scams and frauds—Vircom presents the first in a series of studies explaining cyber crimes and how to avoid them.

Based on an actual fraud attempt, this study demonstrates step-by-step how Advanced Fee Fraud scams unfold and outlines the different modus operandi used by the scammers.

Important advisory

Under no circumstances should anyone attempt to contact a scammer or any sender of suspicious unsolicited email. Con artists are very talented at manipulating people and they make a living defrauding unsuspecting individuals.

Although easy to detect by a messaging professional, Advanced Fee Frauds can easily fool a well-intentioned person. In fact, these frauds generate in excess of a billion-and-a-half dollars annually. The idea is to send out millions of solicitations that will eventually reach someone who, while perhaps skeptical at first, desperately wants the deal to be legitimate. Thus, it is not a good idea to do anything with Advanced Fee Fraud emails other than delete them.

Contributing experts

The following Vircom contributors are quoted throughout this document, imparting extensive industry knowledge, messaging security expertise and important advice to readers.



Michael Gaudette
Vircom spam expert



Marc Chouinard
SpamBuster Team

Michael Gaudette

Michael is Vircom’s director of product strategy. With a background in Internet infrastructure management, Michael leads Vircom’s product development efforts and is responsible for maintaining synergy between Vircom’s solutions and their respective markets.

Marc Chouinard

As head of the SpamBuster Team, Marc oversees Vircom’s Internet spam monitoring efforts. Constantly developing preemptive tools that analyze spam patterns instead of instances, Marc ensures that the technology driving Vircom’s Sequential Content Analyzer™ engine remains ahead of the latest spam tactics.

Introduction

Like most scams, Advanced Fee Frauds predate the Internet. In fact, even though it may seem to be a recent phenomenon, the concept of Advanced Fee Frauds has been around for as long as fraud itself has existed.

Despite their long history, Advanced Fee Frauds have only recently become a widespread threat due mostly to the simplicity and efficiency of bulk emailing.

The success of an Advanced Fee Fraud relies on a scammer's ability to convince victims to respond to an invitation or proposal, send money and/or divulge financial information in exchange for a large sum of money to be received at a later point in time. Payments made by victims are said to cover taxes, legal fees and in some cases, bribes to government officials. Victims are assured that the money they pay out will be reimbursed once the frozen funds are released and transferred out of the country of origin.

The following excerpt from *popsubculture.com* describes a classic example of an Advanced Fee Fraud:

In the 1920's (though research has revealed evidence leads to examples of this con as early as 1588), a type of advance fee fraud flourished that became known as "The Spanish Prisoner" con. In the Spanish Prisoner con, businessmen were contacted by someone trying to smuggle the child of a wealthy family out of a prison in Spain. But of course the wealthy family would richly reward anyone who helped secure the release of the boy. Those who were suckered into this paid for one failed rescue attempt after another, with the fictitious prisoner continuing to languish in his non-existent dungeon, always just one more bribe, one more scheme, one more try, away from being released.

In actuality, however, the millions of dollars in question do not exist, and victims eventually end up losing all of their money and facing financial ruin.

According to the United States Secret Service, "The goal of the criminal is to delude the target into thinking that he [she] is being drawn into a very lucrative, albeit questionable, arrangement."

"The intended victim must be reassured and confident of the potential success of the deal. He [she] will become the primary supporter of the scheme and will willingly contribute a large amount of money when the deal is threatened."

Methodology

Vircom's SpamBuster Team monitors thousands of emails per day. The scam used in this study was chosen from one of the honey pots created by Vircom.

All correspondence between Vircom and the scammer was done via email and lasted approximately six weeks. The email examples contained in this document are just a sample of the many exchanges between Vircom and the scammer.

All personal information Vircom provided to the scammer was fictitious. For example, we claimed that the phony victim's address was 1245 Rogers Street, New Rochelle, Massachusetts, USA.

NOTE: The SpamBuster Team offered to send copies of all correspondence to the law enforcement agencies where each scam originated; no offers were accepted, however.

The Scam

Step 1 - The introduction

Vircom's SpamBuster Team analyzes thousands of online frauds and email scams daily. Advanced Fee Frauds make up over 15 percent of all email fraud and scam messages reviewed by Vircom.



"Email frauds and scams are one of the fastest growing types of spam categories. In January, frauds and scams accounted for 1.24 percent of all email traffic. By September that percentage had risen to 3.15 percent."



"The following Advanced Fee Fraud is a typical example of this type of cyber crime. Although certain traits may vary among scammers, the characteristics of the pitch remain the same for the most part."

Characteristics of Advanced Fee Frauds

- **Calls to action:** In every instance of Advanced Fee Frauds, scammers phrase emails as a call to action, prompting recipients to respond urgently and without thinking carefully.
- **Offers of cash rewards or commissions:** Advanced Fee Fraud scammers promise victims millions of dollars in exchange for access to their banking information or for paying up-front service fees.
- **Identity theft:** Senders usually impersonate someone in power or with authority, such as a government official. They believe this adds credibility to the scam.
- **Use of free web-based email services:** Scammers rely on a variety of free web-mail services to deliver their messages.
- **Capital letters:** Advanced Fee Fraud emails are frequently written entirely in capital letters.
- **Poor grammar:** English is not the first language of most scammers. Many Advanced Fee Frauds are filled with grammar mistakes and spelling errors.
- **Email correspondence:** Most correspondence is handled by email because it is efficient and easy to distribute.
- **Request for confidentiality:** Scammers emphasize the need for keeping all transactions confidential.

Note: For the sake of efficiency, we condensed the following examples of our correspondence with the scammer into six steps. In actuality, Vircom experts had over 60 email exchanges with this particular scammer.

Our correspondence: introduction

>From: Senator Luisa Ejercito Estrada [mailto:sen_lestradap@yahoo.co.uk]
 >Sent: Monday, June 07, 2004 6:27 AM
 >To: misterlennyvircom.com
 >Subject: VERY PRIVATE AND URGENT PLEASE

Free web-based email

HELLO,

Typical capitalized text

THIS MAIL MIGHT BE COMING TO YOU AS A SUPRISE OR UNSOLICITED,BUT I BEG OF YOU TO BEAR WITH ME AND ASILIMILATE THE CONTENT OF THIS MAIL.

Identity theft - Impersonation

Call to action

I AM SENATOR (DR.) LUISA EJERCITO P. ESTRADA (FORMER FIRST LADY OF THE REPUBLIC OF PHILIPPINES), MY HUSBAND WAS THE PRESIDENT OF PHILIPPINES FROM THE YEAR 1998 TO 2000 UNTIL HE WAS IMPEACHED FROM POWER AS THE PRESIDENT AND DETAINED FOR FALSE ALLEGATIONS BY HIS POLITICAL OPPOSITION MASTER MINDED BY HIS VICE-PRESIDENT GLORIA M. ARROYO, NOW THE PRESENT PRESIDENT OF THE REPUBLIC OF PHILIPPINES. BELOW ARE SOME OF THE FALSE ALLEGATIONS THAT WERE FILED UP AGAINST MY HUSBAND IN THE IMPEACHMENT TRIAL:

1. GOV. LUIS SINGSON, A LOGTIME FRIEND OF MY HUSBAND, SAID THAT HE PROVIDED MY HUSBAND WITH MORE THAN \$8MILLION IN PAYOFF FROM ILLEGAL GAMBLING AND \$2.7MILLION FROM TOBACCO TAXES(MONEY PLUNDER).

2. ON DEC 31ST FIVE SYNCHRONIZED BOMB ATTACKS KILLED 22 PEOPLE AND LEFT OVER 110 INJURED IN MANILA THE CAPITAL CITY OF THE REPUBLIC OF PHILIPPINES, DAYS BEFORE THE TRIAL. THE SECURITY AGENCY ACCUSED THE MUSLIM REBELS FOR THE ATTACK, BUT MY HUSBAND POLITICAL OPPONENT INSTIGATED THAT MY HUSBAND PLANNED THE ATTACK TO DISRUPT THE TRIAL FROM TAKING PLACE.

Poor spelling & grammar

3. THAT MY HUSBAND PARTICIPATED IN A REAL ESTATE BUSINESS,CONTROLLED BY ME AND MY SON JOSE DESPITE A PROHIBITION ON OUTSIDE BUSINESS WHILE IN OFFICES.

I WILL WANT TO STATE HERE SINCERELY THAT ALL THIS WERE FABRICATED STORIES ANDPOLITICAL SCANDAL TO GET MY HUSBAND OUT OFF OFFICE WHICH THEY HAVE SUCCEEDED IN ACTUALISING.PLEASE I WILL WANT TO DRAW TO YOUR ATTENTION TO PERUSE THE FOLLOWING WEB-SITE BELOW TO ASCERTAIN THE AUTHENTICITY OF THE CONTENT OF MY MAIL:

Call to action

http://www.inq7.net/specials/erap_trial/2001/background/26558.htm

http://www.bworld.com.ph/Impeachment/documents/d14_am_transcript1.html

<http://www.inq7.net/impeachment/logs3.htm>

<http://www.888.ph/pressrel/pressrel20031205.php>

<http://www.sunstar.com.ph/static/man/2003/07/11/news/rp.asks.australia.to.freeze.dante.tan.assets.html>

Large sum of money involved

DURING THIS TRYING PERIOD OF OUR LIVES,WHEN I WENT TO VISIT MY HUSBAND AT THE VETERAN MEMORIAL MEDICAL CENTER (HOSPITAL PRISON) IN QUEZON CITY OUTSIDE MANILA, MY HUSBAND INFORMED ME THAT HE DEPOSITED SOME MONEY (\$30MILLION) IN A SECURITY COMPANY IN AMSTERDAM, NETHERLAND IN A SECURITY COMPANY AS A CONSIGNMENT IN A DIPLOMATIC SUITE WITH SEAL WITH MY NAME AS THE DEPOSITOR, AND HE URGE ME TO CONTACT A RELIABLE AND TRUST WORTHY FOREIGNER WHO WILL BE WILLING TO ASSIST US RETRIEVE THE CONSIGNMENT AND INVEST THE MONEY CONTAINED IN IT IN ANY PROFITABLE BUSINESS OUTSIDE PHILIPPINES,THUS I DECIDED CONTACTED YOU AND SOLICIT FOR YOUR ASSISTANCE TO EXECUTE THIS TRANSACTION AS THE SOLE BENEFICIARY TO THE CONSIGNMENT AND MY REPRESENTATIVE.

Commission promised

DUE TO THE POLITICAL VICITIMIZATION AND TRAVELING EMBARGO THAT WAS PLACE ON EVERY MEMBER OF OUR FAMILY AND CLOSE FRIENDS OF OUR'S, WE CANNOT EXECUTE THIS TRANSACTION ON OUR OWN.WE HAVE ALREADY FINALIZED THAT YOU WILL BE GETTING 15% OF THE TOTAL MONEY CONTAINED IN THE CONSIGNMENT AND ANOTHER EXTRA 5% TO SETTLE ALL YOU FINANCIAL EXPENDITURE YOU MEANT AS WELL INCUR IN THE COURSE OF EXECUTING THIS TRANSACTION. PLEASE BE REST ASSURED THAT THIS TRANSACTION IS 100% RISK FREE AND DUE TO MANY UNSOLICITED MAILS YOU MIGHT BE RECIEVING FROM TIME TO TIME, I WILL ALSO WANT TO ASSURE YOU THAT THIS MAIL IS NOT A SCAM MAIL AS YOU ARE DEALING WITH HIGHLY REPUTABLE FIGURE IN THE SOCIETY AND THE WORLD AT LARGE DESPITE MY PRESENT PREDICAMENT. I HAVE EVERY PROOF TO BACK IT UP.

Email-only communication

I WILL BE COMUNICATING WITH YOU STRICTLY BY EMAIL, BECAUSE ALL MY TELEPHONE LINES ARE NOT SAFE FOR THE TRANSACTION BECAUSE OF THE HEIGHTEN SECURITY AROUND ME AND MY FAMILY,BUT IF SO WISH TO COMMUNICATE VIA PHONE I WILL INSTRUCT MY LAWYER TO CALL YOU.

Request for confidentiality

PLEASE NOTE THAT THIS TRANSACTION IS HIGHLY AND STRICTLY CONFIDENTIAL. AS SOON AS YOU GET BACK TO ME I WILL INSTRUCT YOU OF THE MODALITIES THAT WILL ENABLE US EXECUTE THIS TRANSACTION SUCCESSFULLY.

I LOOK FOWARD TO ESTABLISH MUTUAL PERSONAL RELATIONSHIP AND BUSINESS RELATIONSHIP WITH YOU AND I URGE YOU TO HANDLE THIS TRANSACTION WITH A HIGH SENSE OF MATURITY AND TRUST.

Calls to action

I SINCERELY OPT YOUR URGENT RESPONSE TO THIS MAIL.

BEST REGARDS,

SENATOR (DR.) LUISA EJERCITO P. ESTRADA



"We responded to this scammer by posing as Mr. Lenny, a Boston-area gentleman in his late 70s living on a fixed income. During our correspondence, we asked the scammer why he solicited Mr. Lenny instead of someone with more influence. Among other questions, we asked the scammer about the legality of the monetary transaction and how Mr. Lenny was to collect the funds."

Step 2 - The setup



"Twenty-four hours after replying to the Advanced Fee scammer, we received a response to our questions. In his email, the scammer exhibited many more typical characteristics of an Advanced Fee scam."

Additional characteristics of Advanced Fee Frauds

- **Request for banking information:** Most Advanced Fee Fraud scammers will request recipients' banking information; they use this to withdraw funds and obtain other financial documents like credit cards or to open new bank accounts or lines of credit.
- **Travel required:** In many cases, Advanced Fee Fraud scammers ask their victims to travel to a foreign country to claim their money. This can turn into a very risky situation for the victim, because there have been reported instances of physical assaults and even murders in some cases of fraud attempts. If travel is not possible, scammers will usually offer to send money to recipients if they pay some type of legal/bribe/tax/transportation fee up front.
- **Recipient identity theft:** By requesting personal and confidential information, Advanced Fee scammers are able to steal recipients' identities and obtain credit cards and forge travel documents.
- **Social engineering:** Advanced Fee Fraud scammers use social engineering techniques to identify and prey upon potential victims.



"Social engineering is common among Advanced Fee Frauds. Since scammers cannot use information that is specific to a single person, they will create a generic email and later use cultural or other references to connect with the victim. In the case of Mr. Lenny, the scammer appealed to his religious sympathies to assure Mr. Lenny of the operation's legitimacy."



"Often when victims stop sending money, scammers will use the personal information they obtained and any cheques they received to drain victims' bank accounts and max-out their credit cards until all assets are depleted."

Our correspondence: the setup

GOOD DAY MR. LENNY,

I AM IN RECEIPT OF YOUR MAIL AND IT CONTENT WAS WELL UNDERSTOOD.

THERE IS NOTHING TO BE CUIOIS ABOUT, I CHOOSED YOU BECAUSE I STRONGLY BELIEVE THAT I CAN TRUST YOU IN THIS TRANSACTION AND THAT YOU WILL BE WILLING TO HELP ME.

Social engineering

IT IS TRUE THAT A PERSON IN MY POSITION SHOULD HAVE A LOT OF FRIENDS TO ASSIST ME.YES I HAVE AWHOLE LOT OF FRIENDS BUT NOR I COULD TRUST BECAUSE OF MY PASTED EXPERIENCE WITH SOME OF THEM WHO BETRAYED OUR TRUST AND FRIENDSHIP

I DECIDED TO CONTACT A FOREIGN PERSON WITH THE HEART OF GOD AND I BELIEVE THAT GOD SENT YOU TO ME.

Social engineering

THE MONEY IS IN A SECURITY COMPANY IN IRLAND DEPOSITED AS A FORM OF CONSIGNMENT AS YOU HAVE ALREADY KNOW. LIKE I SAID I WANT YOU TO HELP IN RETRIEVING THE CONSIGNMENT AS THE NOMINATED BENEFICIARY TO THE CONSIGNMENT AS THE NOMINATED BENEFICIARY TO THE CONSIGNMENT AND REPRESENTATIVE. THIS MEANS YOU WILL HAVE TO TRAVEL TO IRLAND AS MY REPRESENTATIVE AND MEET WITH THE OFFICIALS OF THE SECURITY COMPANY THAT WILL HANDOVER THE CONSIGNMENT TO YOU AS MY NOMINATED BENEFICIARY.

Request to travel

I HOPE THIS TASK IS NOT TO MUCH FOR YOU? I WILL WANT YOU TO PROVIDE ME WITH THE FOLLOWING DETAILS TO ALLOW ME THAT I CAN FORWARD IT TO THE SECURITY COMPANY AND INTIMATE THEM THAT I HAVE APPOINTED YOU AS THE SOLE BENEFICIARYTO THE CONSIGNMENT.

PLEASE SEND THE FOLLOWING DETAILS:

YOUR FULL NAME

Identity theft attempt

TELEPHONE/FAX NUMBER

RESIDENTIAL/OFFICE ADDRESS

Request for banking information

BANK ACCOUNT / NUMBER

A SCAN COPY OF YOUR INTERNATIONAL PASSPORT AND DRIVER'S LICENSE

DO NOT WORRY ABOUT BREAKING ANY LAWS I WILL HAVE MY LOWYER IN IRLAND DRAFT OUT A REVOCABLE TRUST AGREEMENT THAT WILL BEND US TOGETHER.

PLEASE ENDEVOUR TO SEND THE LISTED INFORMATIONS TO ME AS SOON AS POSSIBLE.

HAVE A NICE DAY AND GOD BLESS.

SENATOR (DR.) LUISA EJERCITO P. ESTRADA

Step 3 - The suits

To add credibility to their ploy, scammers often introduce a third party such as a financial advisor or lawyer who will request some sort of service fee.

Additional characteristics of Advanced Fee Frauds

- **Request for fees:** Regardless of the pitch, potential victims will eventually be asked to pay money up front to cover some aspect of the operation. These transactions may be for:
 - ▶ Attorney expenses
 - ▶ Export fees
 - ▶ Insurance costs
 - ▶ Transaction charges
 - ▶ Transportation fees
 - ▶ Cable or communication time
 - ▶ Bribes
 - ▶ Demurrage, storage or release fees by a security company
 - ▶ Gifts
 - ▶ Tender fees
 - ▶ Processing, licensing or registration rights
 - ▶ Taxes, VAT
 - ▶ Deed stamps
 - ▶ Bonds
 - ▶ Anti-terrorist or other types of certificates

- **Introduction of a third party:** Posing as a person in authority, Advanced Fee scammers use this tactic to make the transaction and request payment seem official.



"We responded to the scammer, expressing hesitation and requesting that his security company contact us with more details regarding the transaction. Within 24 hours, we received our first email from the scammer posing as a financial advisor."

Our correspondence: the suits

The following is an extract taken from an email correspondence between Mr. Lenny and the so-called third-party contact:

ATTENTION: Mr. Lenny

Dear Sir,

The above subject matter and your last mail refer.

Introduction of third party

We have lowyer offices in London, United Kingdom and the Republic Of Irland where we attend to our clients daily. Presently I am in the Dublin Office and will be handling the consignment on behalf of all parties until it is deposited as refered above is in our custody.

Conventionally, you are supposed to come personally to the office to clear the consignment with evidence of certificate of deposit and receipt of payment of the accrued demurrhage charges. But we sugest for you to alow us to send it directly toyou, we will have our delivery officers deliver the consignment to you personally at your designated address anywhere in the world.

Request for money (fees)

The legal fees for this transation is \$16,000 US, we can extredite this for \$14,000 US if we can conclude our transation by Friday.

Urgency to act

On taking one of the above options, we will process all the necessary documentation in your favour. Should you have any inquiry or further questions regarding this notice, you are at liberty to contact the undersigned in the Dublin Office with the number given below.

Always quote your reference number in every correspondence.

Treat as priority.

Yours faithfully,

Free web-based email

Felix Johnson
felixj@financier.com



"We noticed several writing traits—such as the misspelling of *lowyer*, *alow*, and *Irland*—which suggested that the same writer created both scams."



"When scammers impersonate lawyers or financial advisors, they often use free web-mail addresses that look official, such as *lawyer.com* or *financier.com*. All of these web-mail addresses are available to anyone free of charge."

Step 4 - The paperwork

Providing phony documentation from officialdom containing legal stamps is a common trick used in Advanced Fee Fraud scams. Seemingly official, this type of documentation gives credibility to the operation and fools victims into thinking their money will be protected by international regulations and laws.



"The purpose of this documentation is to convince recipients of the proposal's authenticity. Numerous documents bearing official-looking government letterhead, stamps or seals can be very convincing. The quality of these documents can vary, but they are all meant to further deceive the victim."

Additional characteristics of Advanced Fee Frauds

- **Forged documents:** There are many types of official-looking forged documents, including government letterhead and forms from phony financial institutions.
- **Bogus/unverifiable information:** The organizations allegedly represented in these documents are often bogus; what's more, the information they contain is practically impossible to verify by the victim.

The following are examples of phony documentation our scammer sent to Mr. Lenny during the course of the attempted Advanced Fee Fraud:



"The paperwork that we received was of very poor quality and easy to detect as forged documentation. Nevertheless, for typical victims, such documents may be the convincing factor in agreeing to a scammer's proposal. In addition, completed documents give scammers enough information to steal their victims' identities."

Step 5 - The score

Once scammers convince their victims, they then request payment for fees or services. Victims are given various payment options: scammers may withdraw funds from victims' bank accounts, or they may request the transfer of funds via money transfer agencies.



"Our scammer was confident that he had completely convinced Mr. Lenny of his legitimacy. He then needed to collect his \$14,000. In order to do so, he asked Mr. Lenny to send the payment to one of his accomplices in Ireland."

Additional characteristics of Advanced Fee Frauds

- **Promised delivery of funds:** Scammers request up-front payment of service fees and will certify that the fortune promised will be delivered within a short time period, usually within 24 to 48 hours.
- **Payment of funds:** Scammers asks recipients to send cash through money transfers.
- **Payment in increments:** Because of laws governing the transfer of funds, most scammers will ask victims to transfer funds in increments rather than all at once.

Our correspondence: the score

The example below shows how our scammer tried to facilitate payment by suggesting various methods and by adding a sense of urgency to the email.

ATTENTION: Mr. Lenny

Dear sir,

The above subject matter refers.

Since you cannot come to our office personally, we will send our delivery officers to you at the designated address given by you. In this regard, you will have to bear the cost of shipment to you and demurrage accrued so far before our delivery officers can travel.

The total cost is computed and calculated to be US\$14,000.00 Due to time constrain, this amount should be sent to the Head of our Accounts deaprtment by Western Union Money Transfer. Details given below:

Request for money transfer

NAME: JOSEPH KELVIN STENSETH

ADDRESS: 169, BALCURISS ROAD, DUBLIN IRLAND.

Make your payment in the following incremnts

US\$5,000.00

US\$5,000.00

US\$4,000.00

Incremental payments

On receipt of the final payment today and confirmed by the Accounts Dept, the delivery officers will be despatched immediatly and will be in the designated address within 48 hours. The relevant papers will be signed by you upon arrival of the officers.

Funds promised

Do comply with the above instruction to enable us act swiftly and accordingly. You can contact the office on the phone should you have any question regarding this notice.

Treat as priority.

Yours faithfully,

Felix Johnson.

Step 6 - The aftermath

Once a victim has paid the scammer, he or she will, in all likelihood, never again hear from the scammer.



"We have come across several cases where victims paid thousands of dollars to scammers, only to be told that further funds were needed to clear the millions. Feeling desperate, many victims fell for it and lost even more money."

If scammers can acquire enough information about victims, they can ruin them financially by draining their bank accounts and acquiring lines of credit and credit cards in the victims' names. Sadly, it can take victims years and thousands of dollars in legal fees to clear their names and regain credibility.

Our Advanced Fee Fraud scammer

After several email exchanges, Vircom experts divulged the real purpose behind our email exchanges and explained the nature of our organization. Following that, Vircom asked our scammer the following questions:

How long have you been doing this type of scam?

How much money have you bilked from your victims?

How do you target your victims?

Where do your victims come from?

Initially, our scammer was in complete denial about our true identity and kept up the charade for several weeks. Vircom was finally able to convince him of who we are, and he promptly changed his story.



"The scammer claimed that he is a 22-year-old Nigerian student doing this as part of a school project. We later discovered that he had been scamming for two years with accomplices in Ireland and Canada, that he was simultaneously conducting a series of different scams and that most of his correspondents were elderly Americans."



"One of the human traits that our scammer demonstrated—and that many scammers we have dealt with in the past demonstrated—is frustration. To be successful, scammers must get their victims to act without forethought. When Mr. Lenny questioned the scammer or acted like he didn't understand the requests, the scammer quickly became frustrated. If Mr. Lenny did not respond quickly enough or did not answer all of the scammer's questions, he would inevitably receive another email asking the reason for the delay."

Another instance of Advanced Fee Fraud

Below is another mass-mailed Advanced Fee Fraud attempt by the same scammer. Note the commonalities: promises of large sums of money, requests for confidentiality and urgent calls to action.

>From: universallotto
>Subject: Lottery Payment Notifcation(Second Quarter Bonanza)
>Date: Tue, 15 Jun 2004 19:18:37 +0200

UNIVERSAL LOTTO PROMOTIONS (BRANCH OFFICE)
169, BALCURISS ROAD,
DUBLIN-REP. OF IRELAND.

REF NUMBER: 014/060/532

BATCH NUMBER: 762901-PCD03

Sir/Madam,

We are pleased to inform you of the result of the Lottery Winners International programs held on the 4th of June,2004. Your email address attached to ticket number 27522465896-6453 with serial number 3772-554 drew lucky numbers 7-14-18-23-31-45 which consequently won in the 2nd category, you have therefore been approved for a lump sum pay out of 2,000,000 (EUROS) (TWO MILLION EUROS) CONGRATULATIONS!!!

Funds promised

Request for confidentiality

For security purpose and clarity, we advise that you keep your winning information confidential until your claims have been processed and your money remitted to you. This is part of our security protocol to avoid double claiming and unwarranted abuse of this program by some participants. All participants were selected through a computer ballot system drawn from over 20,000 companies and 30,000,000 individual email addresses and names from all over the world. This promotional program takes place every year.

This lottery was promoted and sponsored by eminent personalities like the Sultan of Brunei. We look forward to your active participation in our next year USD50 millions lot.You are requested to contact our Clearance Officer(Lenox Anderson) to assist you with the claim and transfer of your winnings fund into your instructed account by acknowledging the receipt of this mail with the email address below: address@bogus.example.com

Call to action

Note that, all winnings must be claimed not later than one month. After this date all unclaimed funds will be null and void.

Urgency to act

Please note in order to avoid unnecessary delays and complications, remember to quote your reference number and batch numbers in all correspondences. Furthermore, should there be any change of address do inform our Clearance Officer as soon as possible.

Congratulations once more and thank you for being part of our promotional program.

NOTE: YOU ARE AUTOMATICALLY DISQUALIFIED IF YOU ARE BELOW 18 YEARS OF AGE.

Sincerely yours,

Raymond Willis (Lottery Director)
For: Universal Lotto Inc.

Fraud FAQ

Q. How do Advanced Fee Fraud scammers get email addresses?



"The important thing to understand is that, despite the criminal nature of Advanced Fee Frauds, they are distributed in exactly the same manner as spam. Scammers purchase lists or harvested email addresses and then mass-mail them like spammers do."

Q. Who sends these types of scams?

Advanced Fee Frauds can originate from any country; however, they are most prevalent in Africa—especially Nigeria. According to the United States Secret Service, Advanced Fee Frauds are estimated to be the third or fourth largest source of revenue for the Nigerian economy, which is a major concern for the country's government.

Earlier this year, the Nigerian Government announced a large-scale operation it has begun to put an end to the problem of Advanced Fee Fraud, which has grown into an industry in Nigeria and neighboring countries.

Q. What types of Advanced Fee Fraud exist?



"Although Advanced Fee Frauds have become mostly synonymous with Nigerian 419 scams, they can take on a number of variations that Internet users should be aware of, including the following":

419 emails or business relationship: Recipients get an email stating that they have been chosen to receive a large sum of money, usually from a corrupt politician. They are asked to send money up front in order to cover service fees for releasing the funds. 419 Frauds originate from the Nigerian Criminal Code, which oversees this type of criminal activity.

Wills: Recipients are told that they have been named beneficiary of millions of dollars by some deceased person. In order to get the money, recipients are told they must first pay legal or inheritance-tax fees.

Health/Medical Fee Pleas: This type of scam can take two forms. In one, recipients receive an email asking them to donate money to a fictitious charity. A variation of this scam involves asking recipients to donate money to the sender for crucial medical procedures.

Lottery (lotto) Frauds: Recipients receive an email notifying them that they have won a fortune. They are told they must either forward their banking information to the sender so that the winnings can be placed into their accounts, or that they need to pay some type of legal fee to have the money released.

Protecting yourself against Advanced Fee Frauds

- Learn to identify its characteristics:
 - ▶ Calls to action
 - ▶ Offers of cash rewards or monetary commission
 - ▶ Impersonation of influential people
 - ▶ Use of free web-mail addresses
 - ▶ Email text written in capital letters
 - ▶ Poor grammar & spelling
 - ▶ Request for email-only correspondence
 - ▶ Request for confidentiality
 - ▶ Request for banking information
 - ▶ Travel requirements
 - ▶ Victim identity theft
 - ▶ Introduction of (fictitious) third-party lawyers or advisors
 - ▶ Use of social engineering techniques
 - ▶ Promised delivery of funds
 - ▶ Use of forged documents
 - ▶ Request for use of money transfers
 - ▶ Demands for payment in increments
- Never respond to any email that looks suspicious or sounds too good to be true.
- Upon receiving an Advanced Fee Fraud email, contact your Internet Service Provider via the designated email abuse address (e.g. *abuse@provider.com*). Include the original message and your complaint; the provider should be able to close down the offending account.

Conclusion

We hope this study helps to explain the nature of Advanced Fee Frauds and offers useful advice on how to avoid being victimized by this underhanded and illegal type of email communication.

While the Internet is a vast and instant source of information to anyone with access, it has also become an effective means for unscrupulous individuals to take advantage of the public at large. The concept of Advanced Fee Fraud is not a new one, but its dissemination via email has dramatically increased the possibility of individuals being victimized.

Law enforcement agencies around the world are well aware of online Advanced Fee Frauds. They strongly recommend against recipients responding to these types of emails and urge people to delete them immediately.

Visit the following links for further useful information on online scams:

US Federal Trade Commission

<http://www.ftc.gov/bcp/online/edcams/spam/index.html>

US Secret Service

http://www.secretservice.gov/financial_crimes.shtml

The Royal Canadian Mounted Police

http://www.rcmp.ca/scams/index_e.htm

About Vircom

Montreal-based Vircom is a leading developer of cutting-edge Internet infrastructure and secure messaging solutions for the demanding needs of Internet Service Providers (ISPs) and corporate clients. Vircom's mature Modus™ secure email management technology incorporates over 10 years of industry expertise, making it a powerful driving force in the defense against spam and email-borne fraud.

Labeled the Best Microsoft® Windows®-based Anti-Spam solution by Network Computing magazine, Modus has gained important recognition, among which is a 2004 CATAAlliance Innovation & Leadership Award and a record-breaking five-award distinction including "Best Software Product" and "Most Innovative Product" from Windows IT Pro magazine.

Vircom is also the developer of VOP Radius, a full-featured all-in-one RADIUS server that supports the latest RFCs, vendor specific attributes, NAS templates and has a multitude of preconfigured settings.

About the SpamBuster Team

Vircom's SpamBuster Team is a group of highly trained email professionals who track, adjust and constantly improve the performance of all Modus™ anti-spam solutions to ensure they maintain the highest performance and accuracy levels.

The SpamBuster Team is also heavily involved in analyzing spamming trends and ensuring that Modus™ solutions always stay a step ahead of spammers.

For more information

Vircom has published several others studies on email security:

Facing Consequences

A 6-month statistical study on the effects of spam on unprotected email networks

Why Spammers Spam

An incursion into the world of spammers

Can Laws Block Spam?

An analysis of the effect of international anti-spam legislation

The Modus Manifesto

Vircom's approach to the spam problem

The Anti-Spam Buyer's Guide

Shedding some light on anti-spam technologies

These documents are available for download at: www.vircom.com

Appendix 1: forged documentation



122 Commissioner Street
Johannesburg, South Africa.

**SOUTH AFRICAN HIGH COURT
SOUTH AFRICAN MAGISTRATE COURT.
OFFICE OF THE COMMISSIONER OF OATH**

SWORN AFFIDAVIT

I/EK _____ Age/Ouderdom _____

ID. _____ Tel: _____

Address/Adres _____

Statement/Verklaring _____

I know and understand the contents of the declaration.
I have no objection in taking the prescribed oath.
I consider the prescribed oath as binding on my conscience.

Ek is vertrouwd met die inhoud van die verklaring en begryp dit.
Ek het geen beswaar teen die afle van die voorskrewe eed nie.
Ek beskou dit voorgeskrewe eed as bindend op my gewete.

(DEPONENT/VERKLAARDER)

Signed before me on the (DAY) _____ OF (MONTH) _____ (YEAR) _____

GETEKEN VOOR MY OP (DAG) _____ VAN (MAAND) _____ (YAAR) _____

COMMISSIONER OF OATH
KOMMISSARIS VAN EDE

Appendix 2: forged documentation



MINISTRY OF FINANCE

DEPT. OF CONTRACT FUNDS RECOVERY


PRETORIA HQ, SOUTH AFRICA.

Tel: 27 73 312 3668
Fax: 27 73 159 1200

P.M.B:2000/ESSV

Your Ref:

Date : 23th MARCH 2004



BENEFICIARY FORM

THIS IS TO CERTIFY THAT..... THE OWNER OF THE BELOW INFORMATION STAND TO BENEFIT THE CONTRACT FUNDS OF ROAD CONSTRUCTING THROUGH MPUMULANGA WEST AND NORTHERN ROAD IN 1989. THE TOTAL SUM TO BE PAID TO THE CONTRACTOR HELDING THE ENTIRE JOB FROM 1989 TO 1993 IN TERMS OF SECTION (3.1) IN THE MINISTRY OF S. AFRICA, WORTH TO TWENTY MILLION UNITED STATE DOLLARS.

FOR CLAIMING OF THE FUNDS, THIS FORM HAS TO BE FILLED AND RETURN WITH AN ACCOMPANY AFFIDAVIT OF SWORN FROM THE HIGH COURT OF SOUTH AFRICA AND ALSO WITH AN ENCLOSURE FEE OF US\$4,630.00. THESE TWO DOCUMENTS HAS TO BE IN, FOR 24HRS VERIFICATION, IF THE INFORMATION IS BEING APPROVED, THEN A CERTIFICATE OF APPROVAL WILL BE ISSUE TO THE BENEFICIARY FOR IMMEDIATELY PAYMENT.

PLEASE FILL THESE FORM AND RETURN TO THE DEPARTMENT OF CONTRACT FUND RECOVERY.

FIRST NAMEMIDDLE NAME.....

SURNAME.....

COUNTRY OF BIRTHNATIONALITY.....

PASSPORT/ ID No.....

CONTRACT NO.....

CONTRACT AMOUNT.....

DESCRIPTION OF CONTRACT.....

DATE OF ISSUED..... DATE OF ACCOMPLISHED.....

WE APOLOGIZE FOR ANY DELAY. THIS FORM MUST BE DELIVERED THROUGH SUBMISSION.

DATE _ _ _ _ _

SIGNED _ _ _ _ _

CLASSIFIED DOCUMENT OF THE REPUBLIC OF SOUTH AFRICA