Purchase scams
The most straightforward type of purchase scam is a buyer in another country approaching many merchants through spamming them and directly asking them if they can ship to them using credit cards to pay.
An example of such email is as follows:
From: XXXXXX XXXXXX [XXXXXXX@hotmail.com] Sent: Saturday, October 1, 2005 11:35 AM Subject: International order enquiry
Goodday Sales, This is XXXXXX XXXXXXX and I will like to place an order for some products in your store, But before I proceed with listing my requirements, I will like to know if you accept credit card and can ship internationally to Lagos, Nigeria. Could you get back to me with your website so as to forward you the list of my requirements as soon as possible? Regards, XXXXXX XXXXXX, XXXXXXXX Inc. 9999 XXXXX street, Mushin, Lagos 23401, Nigeria Telephone: 234-1-99999999, Fax: 234-1-9999999, Email: XXXXXXXXX@hotmail.com
Most likely, a few weeks or months after the merchant ships and charges the Nigerian credit card, he/she will be hit with a chargeback from the credit card processor and lose all the money.

Counterfeit Postal Money Orders
According to the FBI and postal inspectors, there has been a significant surge in the use of Counterfeit Postal Money Orders since October 2004. More than 3,700 counterfeit postal money orders (CPMOs) were intercepted by authorities from October to December 2004, and according to the USPS, the "quality" of the counterfeits is so good that ordinary consumers can easily be fooled.
On March 9, 2005, the FDIC issued an alert [1] stating that it had learned that counterfeit U.S. Postal Money Orders had been presented for payment at financial institutions.
On April 26, 2005, Tom Zeller Jr. wrote an article in The New York Times regarding a surge in the quantity and quality of the forging of U.S. Postal Money Orders, and its use to commit online fraud. The article shows a picture of a man that had been corresponding with a woman in Nigeria through a dating site, and received several fake postal money orders after the woman asked him to buy a computer and mail it to her.
Who has received Counterfeit Postal Money Orders (CPMOs)?
Small Internet retailers.
Classified advertisers.
Individuals that have been contacted through email or chat rooms by fraudsters posing as prospective social interests or business partners, and convinced to help the fraudsters unknowingly.
The penalty for making or using counterfeit postal money orders is up to ten years in jail and a US$25,000 fine.

Online automotive fraud
There are two basic schemes in online automotive fraud:
A fraudster posts a vehicle for sale on an online site, generally for luxury or sports cars advertised for thousands less than market value. The details of the vehicle, including photos and description, are typically lifted from sites such as eBay motors or Autoscout24 and re-posted elsewhere. An interested buyer, hopeful for a bargain, emails the seller, who responds saying the car is still available but is located

overseas. He then instructs the buyer to send a deposit via wire transfer to initiate the "shipping" process. The unwitting buyer wires the funds, and does not discover until days or weeks later that they were scammed.
A fraudster feigns interest in an actual vehicle for sale on the Internet. The "buyer" explains that a client of his is interested in the car, but due to an earlier sale that fell through has a certified check for thousands more than the asking price and requests the seller to send the balance via wire transfer. If the seller agrees to the transaction, the buyer sends the certified check via express courier (typically from Nigeria). The seller takes the check to their bank, which makes the funds available immediately. Thinking the bank has cleared the check, the seller follows through on the transaction by wiring the balance to the buyer. Days later, the check bounces and the seller realizes they have been scammed. But the money has long since been picked up and is not recoverable.
In another type of fraud, a fraudster contacts the seller of an automobile, asking for the vehicle identification number (VIN), putatively to check the accident record of the vehicle. However, the supposed buyer actually uses the VIN to make fake papers for a stolen car that is then sold.
COUNTERFEIT CASHIERS CHEQUE SCAM: This recent scam has been reported in Atlanta and Minneapolis. Real estate property owners placing advertisements on Craigslist or rent.com receive an e-mail response from a "24 year old in the U.K. on a research program in the United States". Addresses include john.yearwood__@yahoo.co.uk and kevin_taylor@excite.com.
The first inquiry seems legitimate. The second usually comes with request for more information, and a bogus attachment from JAPAN TOBACCO INC (who has posted information about this scam on its site) indicating that the "student" has won a part time scholarship from the JT UK office. The scam comes with the third e-mail, a request for name and address so that the counterfeit cashiers checks can be sent. The amount supposedly includes the rent and fees plus an overage for the "student's" travel.
The owner is instructed to cash the checks and wire the difference back to the student so that they can travel to the U.S. The photos often include a young man in graduation uniform from his college (Note: U.K. colleges are the equivalent to high schools, not universities. One photo includes a rather dumpy, depressed looking girlfriend who must be aware of the scam). Because of the lag between the cashing and clearing of the checks, the owner does not realize he/she has been had until their account is debited the counterfeit cost and the wired sum. Greedy owners may even decide to keep some of the checks, only to be had themselves later. It is best not to respond to this type of e-mail and requiring background checks before cashing first rent payments.

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

check, will the merchant's account be debited.
In some cases, the fraudsters agree to the wire but ask the merchant for their bank's address. The fraudsters send the counterfeited check directly to the merchant's bank with a note asking to deposit it to the merchant's account. Unsuspecting bank officers deposit the check, and then the fraudster contacts the merchant stating that they made a direct deposit into the merchant's account.
In other cases, fraudsters approach merchants for smaller orders: $2000 to $10,000 offering to pay with a check. They send the check and the instructions state that the merchant has to deposit the check, wait for it a couple days to clear and send the "excess" funds via Western Union money transfer to an account in another country. The fraudsters send fake checks but drawn on the real accounts of large U.S. companies, which will probably clear immediately.

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

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

East European version
This is a variant of the Nigerian Version, in which criminals recruit people through classified advertising. The criminals present themselves as a growing European company trying to establish a presence in the U.S. and agree to pay whatever the job applicant is looking to make, and more. The fraudsters explain to the unsuspecting victim that they will buy certain goods in the U.S. which need to be re-shipped to a final destination in Europe. When everything is agreed they start shipping goods to the re-shipper's house. The rest is similar to the Nigerian Version.

Sometimes, when the criminals send the labels to be applied to the boxes, they also include a fake checks, as payment for the re-shipper's services. By the time the checks bounces unpaid, the boxes have been picked up already and all communication between fraudster and re-shipper has stopped. Here's an example recruiting email received via SPAM on Oct 2, 2007:
XXXXX Inc. invite residents of the various countries to cooperation. We found your resume on some Job Website because we are searching for reliable professionals or your information has been passed to us by your friends/relatives. Our clients need to accept goods from the various countries. Therefore we creating a network of regional agents which functions are reception of goods and further transferring goods to our shipping managers. We pay you 40$ per received package. We guarantee worthy payment of your work. This job is for you If you want to earn from $150 to $800 per week and work Only 2-3 hours then! This job requires punctuality, good organizational skills and proficiency with Microsoft windows and office programs to maintain inventory and fill forms if necessary. This job is ideal for: housewives, students, older persons, and people with restrictions. No money needed to start. This is a business requiring only limited amount of your time. Requirements: 1. A computer with access to the Internet, e-mail 2. We don't work with persons under 18 3. 1-3 hours free during the week 4. Check your e-mail several times a day (each hour is perfect) 5. Reply to e-mails immediately 6. PayPal account to receive payments (optional, WU is also accepted) 7. Be responsible, hard working and communicable We offer competitive compensation, including commission and expense reimbursement. Please send your resume to xxxxxxxxxxx.com Thank You XXXXXX XXXXXXX Manager XXXXXXX Inc.

Known Scams
There is a sophisticated scam from D.Mancene (stands for Diane Mancene) which is currently circulating. It asks you to receive money in your bank account and deduct 10% as payment. Obviously this is a scam however it is very sophisticated employing their own website, http://www.ii-holding.com/index.html, giving the guise of a professional place. Do not be fooled. This is a phishing scam.

Chinese version
This is a variant of the East European Version, in which criminals recruit people through spam. The criminals present themselves as a growing Chinese company trying to establish a presence in the U.S. or Europe and agree to pay an agent whatever the unsuspecting victim is looking to make, and more. Here is an example of a recruiting email:
Dear Sir/Madam, I am Mr. XXX XXX, managing XXXXXXXXXXX Corp. We are a company who deal on mechanical equipment, hardware and minerals, electrical products, Medical & Chemicals, light industrial products and office equipment, and export into the Canada/America and Europe. We are searching for representatives who can help us establish a medium of getting to our costumers in the Canada/America and Europe as well as making payments through you to us. Please if you are interested in transacting business with us we will be glad. Please contact us for more information. Subject to your satisfaction you will be given the opportunity to negotiate your mode of which we will pay for your services as our representative in Canada/America and Europe. Please if you are interested forward to us your phone number/fax and your full contact addresses. Thanks in advance. Mr.

XXX XXX. Managing Director"

Australian version
In the Australian version, the U.S. company is contacted by a potential customer stating they would like to place an order with their company. The first initial email represents the "Direct Solicitations" outline. Once the company responds and verifies that the desired product(s) is in stock, the fraudster will then ask to quote shipping to Australia, and that they will be paying via credit card. Once the quote has been sent to the fraudster, the fraudsters will then reply back that they will have their U.S. agent or freight representative come to the location and pick up the merchandise, and then they will ship it to the fraudster. The fraudster then tells the company to simply add an additional charge of $700 – $1500 onto the total cost, which will be their "agents" compensation fee. And that when the person is to arrive to pick up the parts, that the amount charged be paid to their agent. There will also be an additional compensation fee added in too for the company, for the extra trouble of paying their agent the money. The reasons range from the agent or freight company only accepts cash or the company is unable to process credit cards. Once the fraudster is told it will not be done, the communication between them and the company will stop immediately. There are also many grammar and spelling mistakes in the communications. Here are two variations of what the re-shipper email will look like:
Example one
Dear XXXX, Thanks for the total quote of my order. The total cost of my order is quite correct and okay by me and I'm ready to pay the bills. I shall inform my freight forwarder who will be coming to pick up the order to hold on and come immediately you inform me that the items are ready for pick up then I can give you a call on that day to get the items packed for pick up and they will call you on their arrival at your address. Also I want you to help me Charge another $1200.00 from my card to the shipping agent who will be coming to pick up my ordered items from you. The $1200.00 that will be sent to the freight forwarder is for the shipping of my order and other items I ordered from different part of the country which is to be picked up by him and should be deducted from my credit card. Also, I'm compensating you with the sum of $150.00 for the transfer fee and for your efforts. Please note that I should have given the shipping agency my credit card for him to deduct the shipping funds but he told me that he doesn't have the facilities to charge or debit credit card, so that's why I bring my vote of confidence in you and I want you to assist me in this measure, so I want you to transfer the funds to him after you have make the charges and the money charged from my credit card is in your account, then you can now make the transfer to the agent via western union. I will have love to do this my self but there are no western union here around me cos I am out of town to monitor my estate construction at a remote village, So the charges you'll make on my credit card will be Order Fee: 3,114.61 Agent fee with shipping fare: $1,200.00 Transfer Fee plus Your Compensation: $150.00 Total: $4464.61
Note that my credit card will be charged for the amounts above. Please do get back to me if you are in the office right now so that I can forward my credit card details to you, then you can charge the funds I await your quick response. Kind Regards.
Example two
From: XXXXXX Sent: Tuesday, December 4, 2007 4:40 PM To: XXXXXX Subject: RE: mail order - don't worry I will give you $300 for the stress and you can charges the

money and send the money with the US what about that so let me hear from you today
XXXXX wrote: xxx, We will not be able to transfer the extra $700 to your agent. We can charge you for the motors; however, we have them at two different warehouse locations. What you have your agent do is up to you, we can either will call the motors at each warehouse for him to go and pick them up, or have them shipped to his U.S. address. However, if we do have them shipped to his location, shipping charges will apply, and then I suppose you can deduct that from the $700 you would send to him to come and pick them up. Either way you handle it, the motors are in stock and available for purchase.
From: XXXXX Sent: Tuesday, December 4, 2007 4:28 PM To: XXXXXX Subject: RE: mail order - What I just want you to know is that I will forward my credit for the bill tomorrow to charges and you will charges extra $700 usd to my agent that will come over there to pick up the goods so let me know if you can charges extra $700 then send it to him via western union money transfer

Example three

Hello xxxxx, I am interested in purchasing some of your products, I will like to know if you can ship directly to Australia, I also want you to know my mode of payment for this order is via Credit Card. Get back to me if you can ship to that destination and also if you accept the payment type I indicated. 37 O'Connell Street North Melbourne Victoria 3051 AUSTRALIA Phone:(613) 9329 65433 Fax: (613) 9329 65434 Email(brysuppliersworldwide@gmail.com) Kindly return this email with your Website. I await your quick response. Kind Regards. Managements

Call tag scam

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

Business opportunity/"Work-at-Home" schemes

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

a fee for the kit, but after assembling and returning the item, it’s rejected as substandard, meaning the applicant is out of pocket for the materials. Similar scams include home-working directories, medical billing, data entry (data entry scam) at home or reading books for money.
The latest work at home scam is very elaborate, which includes an entire website dedicated to feigning the existence of a fake organization. Example: Timothy Scott (not his real name) emails to offer a job with the so-called Henry Gilbert Foundation. To lure gullible participants, they offer unrealistically generous salaries for part-time unskilled labor. (If they were real opportunities then naturally such positions would fill quickly without the need to email the offer to thousands of strangers.) The main responsibility of this well paying job is to be a middleman for "donations" which are intended for victims of natural disaster. In this capacity, it gives the scammer an excuse to ask for bank account numbers (allegedly to deposit "donations" into the victim's account for redistribution) as well as the victim's SSN and DOB (allegedly to fulfill the typical paperwork obligations of a new employer). Once these vital numbers have been disclosed, the criminal uses that information to monitor account balances. On the day that a larger than normal amount appears in the bank account, such as a weekly paycheck for example, then the account is drained. Generally the scammer will feign to be located in a country other than where he is located. Example: Travis Gilbert Foundation's website lists an address in The Netherlands, but the registration of the domain name is in Beijing. In addition, victims in Western countries are targeted by using a non-threatening pseudonym like Timothy Scott, which doesn't sound so foreign, while the domain name tgilberthome.org is actually registered to Li Xiang.

Money Transfers Fraud
This type of Fraud consists of an employment offer to help transfer money to a foreign company, supposedly because it costs too much to do it through other methods (which is usually not the case). The prospective victim receives an email like these 4 examples:
Example one
Dear Sir/Madam, XXXXXX is a small scale company in XXXXXX. We supply XXXXXXX to clients in some countries. We have reached big sales volume in the Europe as a starter, and now we are trying to penetrate the US/Canada market. Quite soon we will open representative offices or authorized sales centers in the US and therefore we are currently looking for people who will assist us in establishing a new distribution network there. The fact is that despite the US market is new for us we already have regular clients also speaks for itself. The international money transfer tax for legal entities (companies) in XXXXXX country is 25%, whereas for the individual it is only 7%. There is no sense for us to work this way, while tax for international money transfer made by a private individual is 7%. That's why we need you! We need agents to receive payment for products in money orders, checks or bank wire transfers) and to resend the money to us via Money Gram or Western Union Money Transfer. This way we will save money because of tax decreasing. JOB DESCRIPTION? 1. Receive payment from Clients 2. Cash Payments at your Bank 3. Deduct 10% which will be your percentage/pay on Payment processed. 4. Forward balance after deduction of percentage/pay to any of the offices you will be contacted to send payment to (Payments are to be forwarded either by Money Gram or Western Union Money Transfer). HOW MUCH WILL YOU EARN? 10% from each

operation! For instance: If you receive 7000 USD via checks or money orders on our behalf. You will cash the payment and keep $700 (10% from $7000) for yourself! At the beginning your commission will equal 10%, though later it will increase up to 15%! ADVANTAGES: You do not have to go out as you will work as an independent contractor right from your home office. Your job is absolutely legal. You can earn up to $3000–4000 monthly depending on time you will spend for this job. You do not need any capital to start. You can do the Work easily without leaving or affecting your present Job. The employees who make efforts and work hard have a strong possibility to become managers. Anyway our employee never leaves us. MAIN REQUIREMENTS: 18 years or older legally capable responsible ready to work 2–4 hours per week. with PC knowledge e-mail and internet experience (minimal) And please be informed that Everything is absolutely legal. If you are interested in our offer, please reply to the following email address: XXXXXX@XXXXX with your; (1)Your full names: (2) Contact address: (3) Tele/cell numbers: (4) Occupation: (5) Age: (6) Sex: Thanks for your anticipated action. And we hope to hear back from you soon.

Example two

Dear Sir/Madam, I am XXXXX XXXXX, Human Resources Manager of XXXXX located in XXXX. We deal in XXXXXXX articles such XXXXXX worldwide. Our website is XXXXXX. We are currently in search of a book-keeper/company representative who would assist us in receiving payment from our customers in America/Canada/Asia and other part of Europe. This offer is absolutely legal and you do not need any capital to start. Your Job description is as follows: (1) You would receive payment on our behalf from our various clients which would come in the form of cashiers checks, traveler's checks and official checks. (2) You then get the payments deposited/cashed at your bank. (3) You then deduct a commission of 10% of each payment you would be receiving, as been our representative and then send the balance money via western union to any of our agent or offices that you would be instructed. HOW MUCH WILL YOU EARN? 10% from each operation! For instance: you receive 7000 USD via checks on our behalf. You will cash the money and keep $700 (10% from $7000) for yourself! At the beginning your commission will equal 10%, though later it will increase up to 12%! Our payments will be issued out in your name, as we would inform our clients to do so. If you are interested in this offer, kindly provide us with the below details. 1) Full name 2) Full house address Street/Ave, City, State and Zip Cope 3) Phone numbers 4) Age & Sex 5) Present Occupation PLEASE NOTE THAT ALL REPLIES SHOULD BE SENT THIS E-MAIL ADDRESS: XXXXXXXXXXX Thanks for your anticipated action. And we hope to hear back from you. XXXXXX XXXXXX (Human Resources Manager)

Example three

Transactions specialist - part-time work opportunity. An international investment company is looking for communicative and skillful individuals to join the Receivables Team of our Finance & Infrastructure Group in the United States on part-time basis. This position involves monitoring and processing of our company's funds. Your duties will not involve any direct client interaction, and you will be reporting to the Receivables department manager in Russia. We are looking for numerate individuals who are also able to multi-task efficiently in a team. Relevant previous experience and/or education is a plus, but not a prerequisite. The position is entirely home-based, and no relocation is required from the successful candidate. This role does not involve any fixed working hours and is suitable for senior citizens or self-employed

individuals. Estimated average salary starts from $3,000.00 per month. In order to qualify for the position, you must be a permanent US resident aged 21 and above and have a verifiable personal/business banking relationship with a US bank. Since most communication with the head office will be via email/fax/phone, you should have reliable access to these facilities and be reachable during regular business hours. To apply for this position or to request additional information on our company, please contact us at xxxxxxxxx@XXXXXXXX. Please make sure to provide your contact phone number. Please note that only applicants under serious consideration will be contacted.

Example four

FROM XXXX and YYYY ZZZZZZZZZZ. XXXXXXXXXX ABIDJAN DANANI REFUGEE CAMP, ABIDJAN REPUBLIC OF COTE-D'IVOIRE

Dearest One,

My name is XXXXXXXX and my Sister's name YYYYYYYYY we are the children of Late General ZZZZZZZZZZZZ the former Director of military intelligence and special acting General Manager of Sieria Leone Diamond mining corporation (SLDMC). I am contacting you to seek your good assistance to transfer and invest Five million seven hundred and twenty thousand united state dollars ($5,720,000.00) belonging to my late father which is deposited in a bank here in Abidjan. This money is revenues from solid minerals and diamonds sale which were under my father’s possession before the civil war broke out. Following the break out of the war, almost all government offices, operations and parastatals were attacked and vandalized.

The SLDMC was looted and burnt down to ashes, and diamonds worth millions of dollars was stolen by the rebel military forces who attacked my father’s office. Many top government officials and senior army officers were assassinated and my father was a key target because of his very sensitive military position and appointment in the SLDMC. Regrettably, my father was captured and murdered along with half brother in cool blood during a mid-night rebel shoot-out when our official residence in Freetown was ambushed by Fordey Sanko the notorious rebel leader. My mother sustained very sever bullet injuries which resulted to her untimely and painful death in a private hospital here in Ivory Coast.

Now we are alone in a totally strange country without parents, relatives or any body to care for us at our tender ages. Before our mother died, she told us that our father deposited some money which he made from diamond sales and deposited it in a bank here in Ivory Coast and that we should pray and find a trust worthy foreign business partner who will help us to transfer and invest this money in profitable business venture overseas.

She told us to do this quickly so that we can leave Ivory Coast with our cousin brother-Arthur who is here in the camp with us and, then settle down abroad. She gave us the bank document to prove the deposit and then told us that my father used my name as the only son to deposit the money in the bank. She told us that this is the reason why we came to Ivory Coast. My mother died after wards. May her spirit rest in perfect peace.

I have gone to the bank to make inquires about this money and I spoke with the Manager of International remittance who assured me that everything is intact and promised to help me transfer this money to my foreign partners bank account as soon as I provide my partners foreign bank account for them. However, the manager is very concerned because of my age. I am 19 years old and as such advised that I should look for a matured person that will represent me at the bank.

If you are willing to assist us, please let us know immediately so that you will arrange the transfer of the money to your account with the bank. Please note that we will offer you 20% of the total money as compensation for your noble assistance in accordance with my mothers advise. We are interested in any profitable commercial venture which you consider very good in your country and you would also get a school for me and my little sister and cousin so that we can finish our college education in your country.
Please there is urgent need for the money to be transferred to your account and I am hoping to hear your urgent response so that I can not look for another foreign partner.
Thank you and may God bless you and your dear family.
Yours sincerely
XXXXX and YYYYYY ZZZZZZZ

Example five

Dearest.
Reply in My E-mail:(XXXXXXXXXXX@YYYYYYY.ZZZ)
I am Miss XXXXXX YYYYYYY. My reason of contacting you is that I need your assistance to receive the sum of (US$10.500.000,00) into your account for a profitable investment in your country. I have made all the necessary arrangement for successful transfer of this fund into your account without any problem I will give you full detail on how this process will be done. It’s 100% risk free.
thanks. Miss XXXXXX YYYYYYYY Reply in My E-mail:(XXXXXXXXXXX@YYYYYYY.ZZZ)

Example six

Dear Sir/Madam
I'm the C.E.O of XXXXX Textiles. We'd like to offer you additional earnings $2000 – $8000 per month. It's easy and will not take a lot of time. No costs, No Investments, Work Part Time or Full Time. Up to $2000 Part Time and $8000 Full Time. Work from Home with a Business Opportunity that no job could ever offer. Use your own computer to make money and make a CAREER as your own boss. I would like to know if you are interested. Work will consist of receiving of the payments from our clients in USA and Canada.
All you would be doing is receiving these payments that would come to you via the mail system in your country, have them cashed and remit the rest to me. I would be willing to pay you 10% of whatever payment you process. These payments would come in different forms.
We are always facing serious difficulties when it comes to selling our products to Americans; they are always offering to pay with Different Modes, which are difficult for me to cash here in the UK. Because of a hold of almost three weeks that would be placed on them before they clears the banks here in the UK. Unfortunately we can't open the bank accounts in all the countries we work with and because of that we seek for a representative/bookkeeper in USA and Canada.
Respond only if you will like to work from home part-time/full time and get paid weekly without leaving or it affecting your present job. (PAY IS GOOD)If interested please reply with the information below to Email: XXXXXX@XXXXXX.com
EMPLOYMENT APPLICATION FORM: FULL NAME..... ADDRESS (P.O Box Not Accepted)..... CITY.....STATE....ZIPCODE.... PHONE ..... CELL PHONE..... AGE.....SEX..... PRESENT OCCUPATION ..... RECENT BANK.....
XXXXXXX XXXXXXXX ARTS AND CRAFTS 99-98 XXXXXX STREET XXXXXXXXXX

LONDON,WG2B 6TD +44-999-999-9999
Best Regards, Mr. XXXXX XXXXX

The fraudsters will then send fake checks or postal money orders, in the hopes of getting the victims to cash those fake money instruments and then getting real money from the victims.
These scams are also use as phishing tools, because many times the fraudsters are able to get the victims full name, address, social security, bank account number, etc, etc, which in ends up being identity fraud.

Dating scams

Main article: Romance scam
Online dating scams and fraud are almost as old as Internet dating itself. Often called a Sweetheart Swindle this is often a long, drawn out process in which the con artist develops a relationship, and eventually convinces the victim to send money. The scammer often meets the victim in chat rooms or via online dating sites. Their object is not to get into their hearts, but get into their wallets. They will try to earn someone's affections and trust so that they can persuade him/her to send money. The requests for money can either be a one time event or repeated over an extended period of time. The details of the scammers' stories will vary with each case. The scenario commonly revolves around a tragedy having befallen the scammer, and he/she desperately needs money. After spending time communicating and building a relationship with the victim, the scammer will ask for help in the form of money. Most online dating services have a hard time dealing with scammers, outside of issuing warnings to their users to be alert for anyone you've never met asking for money.
Some potential indicators you may be dealing with a dating scam:
The online sweetie says, "I love you" almost immediately.
The person asks for money, to cash a check or money order.
The person claims to be a U.S. citizen who is abroad, well off, or a person of importance.
The person claims to be a contractor and needs help with a business deal.
The person claims to need money for a parent's "operation in the hospital".
The person will have an attractive photo posted on the website, but won't be willing to send you any other photos. Most likely, that is not a real photo of the scammer.

Click fraud

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

International modem dialing

Customers of dial-up Internet Service Providers, such as AOL, use a modem to dial a local connection number. Some web sites, normally containing adult content, use international dialing to trick consumers into paying to view content on their web site. Often these sites purport to be free and advertise that no credit card is needed. They

then prompt the user to download a "viewer" or "dialer" to allow them to view the content. Once the program is downloaded it disconnects the computer from the Internet and proceeds to dial an international long distance or premium rate number, charging anything up to US$7-8 per minute. An international block is recommended to prevent this, but in the U.S. and Canada, calls to the Caribbean (except Haiti) can be dialed with a "1" and a three-digit area code, so such numbers, as well as "10-10 dial-round" phone company prefixes, can circumvent an international block. One example is www4.bux.to

Internet marketing and retail fraud

This is a fast-growing area of internet fraud perpetrated by dishonest internet marketing and retail sites. A variety of products and services are involved. The customer is tricked by a legitimate-looking site and effective marketing into giving their credit card information and CVV number, or sending cash by other means, in exchange for what they believe to be the goods or services. The goods never arrive, turn out to be fake, or are products worth less than those advertised.

Where a credit card is involved, the perpetrators may also aim to use the customer's credit card information to obtain cash or to make purchases of their own. A common example of this type of fraud are pornographic websites that advertise free access. Upon further inspection, however, a credit card is required "for age verification purposes only". The scammers then use your credit card information to make large charges to the credit card.

In cases involving fake or worthless goods, many are health products, related to health fraud. These products might advertise anything from a quick way to lose weight to a cure for a serious disease, and may:

promise a lot, claiming they can "do it all"

claim to be a "scientific breakthrough", featuring fake doctors or scientists making claims for the product, with technical jargon that only experts in the field know is used falsely

feature a long list of "personal testimonials", with no way to check if they are true or fake.

Once your credit card information is given to these types of scam companies, they usually will charge you no matter what type of cancellation you attempt to go through. This can often be overcome by contacting the credit card company. Credit and consumer protection laws in many countries hold the credit card company liable to refund their customers' money for goods or services purchased with the card but not delivered. The loss is then suffered by the card company, but ultimately passed on to customers in higher interest and fees.

Internet ticket fraud

A variation of internet marketing fraud is offering tickets to sought-after events such as concerts, shows and sports events. The tickets turn out to be fake or are simply never delivered. The proliferation of online ticket agencies and the existence of experienced and dishonest ticket touts has fuelled this kind of fraud in recent years. Many such scams are run by British ticket touts, though they may base their operations in other countries.

The company Euroteam is a well established ticket scam. Norwegian based they force customers to confirm that they are buying tickets for a company in order to dilute consumer protection laws. They promise to deliver tickets often confirming

their delivery up until minutes before an event is due to start.
A prime example was the global Beijing Olympic Games ticket fraud run by US-registered Exclusive Leisure and Hospitality, sold through a professionally-designed website, www.beijingticketing.com with the name "Beijing 2008 Ticketing". On 4 August it was reported that more than $50 million worth of fake tickets had been sold through the website. On 6 August it was reported that the person behind the scam, which was wholly based outside China, was a British ticket tout, Terrance Shepherd.

Internet Marketing SEO Fraud

This type of fraud involves a supposed internet marketing specialist presenting a prospective client with detailed graphs and charts that indicate that his web site receives (x) thousands of hits per month. The specialist emphasizes that payment for his services will increase web traffic, in return increase costumers. The marketer then proceeds to not provide the proposed services.

Phishing

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

Email Spoofing

Main article: Spoofing attack
The sender information shown in e-mails (the "From" field) can be spoofed easily, though nowadays many domains have the Sender Policy Framework implemented, which helps prevent the e-mail spoofing. This technique is commonly used by

Spammers to hide the origin of their e-mails and leads to problems such as misdirected bounces (i.e. e-mail spam backscatter).

Pharming

Main article: Pharming

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

If the web site receiving the traffic is a fake web site, such as a copy of a bank's website, it can be used to "phish" or steal a computer user's passwords, PIN or account number. Note that this is only possible when the original site was not SSL protected, or when the user is ignoring warnings about invalid server certificates. For example, in January 2005, the domain name for a large New York ISP, Panix, was hijacked to a site in Australia. In 2004 a German teenager hijacked the eBay.de domain name.

Secure e-mail provider Hushmail was also caught by this attack on 24th of April 2005 when the attacker rang up the domain registrar and gained enough information to redirect users to a defaced webpage.

Anti-pharming technologies are now available.

Auction and retail schemes online

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

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

Another variation of fraud is for a seller to ship an item with USPS delivery confirmation (but not require signature) to an incorrect address that is within the buyer's zip code. The item shipped is usually an empty envelope with no return address and no recipient name. That successfully triggers the delivery confirmation receipt so the seller can claim the package has been delivered. Standard USPS Delivery Confirmation only tracks to the zip code level, not to the specific address.

Paypal Fraud

This is new form of fraud where a buyer (a scammer) will target eBay auctions which are "Collection in person" and will have a fake address or storage address with P.O Box (as ebay/paypal now allows un-confirmed address and these transactions are not covered by seller protection.) What these people will do is buy an item from the

seller and intend to collect it in person. This person will collect the item and will claim back, stating he hasn't received the item. Paypal has user policy that IF they don't have a tracking number they will grant the money back to the scammer (Paypal does not take video evidence, signature proof or any other proof as valid collection.)
It is strongly suggested if you are selling items with collection in person that you do cash transactions by handing the item and collecting cash to avoid the scheme.

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

Avoiding Internet investment scams
The US Security Exchange Commission have enumerated guideline on how to avoid internet investment scams. The summary are as follows:
The Internet allows individuals or companies to communicate with a large audience without spending a lot of time, effort, or money. Anyone can reach tens of thousands of people by building an Internet web site, posting a message on an online bulletin board, entering a discussion in a live "chat" room, or sending mass e-mails.
If you want to invest wisely and steer clear of frauds, you must get the facts.
The types of investment fraud seen online mirror the frauds perpetrated over the phone or through the mail. Consider all offers with skepticism.
Do not use your credit card number and cvv number to buy products from online lesser known merchants.