Online Shopping

FORENSIC ACCOUNTING CLASS

FALL SEMESTER 2007

Owens Community College
Perrysburg, Ohio

Instructor: Ronald W. Coon, Sr., CPA, DABFA

Vickie Ames

Amanmyrat Gurdov

Sara Mandraken

Mike Reibe

David Shaffer

Troyce Wilson

INDEX

Appendix

DISCLAIMER

Any businesses, trade names, service marks, trademarks, intellectual property, logos and symbols used in this paper are for ***reference examples only***. Neither this class nor the Instructor, nor the Owens Community College endorses these businesses, trade names, service marks, trademarks, intellectual property, logos and symbols. The student class also does not represent the preference of one business, trade names, service marks, trademarks, intellectual property, logos and symbols over another.

INTRODUCTION

The weather! The traffic!! The long lines!!! That store doesn't have what I want!!!! Why isn't the store open when I need it to be????? Isn't there a solution?

Yes, there is a solution. Online shopping! How convenient is it really? How economical is it? How safe is it? This report is going to try to answer those questions. Many consumers are using online shopping everyday. This gives you the comfort of browsing for items without the hassle of increased traffic; pressures from sales associates and long checkout lines. However, there are some downsides to online shopping, as you risk your personal information getting out and possibly leading to identify theft. There is also the risk of not receiving your item in a timely and acceptable manner or of not receiving the correct item.

The following stories give you an idea as to what can happen with the various scams that are used in cyber space.

Scenario #1

Lynne runs a bed and breakfast in South Australia. Lynne received a booking request from Indonesia via her website from a travel agency in Kuta, Bali. They wanted to book a two-week stay for two couples, their Japanese clients. After several emails to organize details and cost the travel agent was not concerned with dates available or the cost, agreeing to the first price offered by Lynne. The travel agent from Bali even agreed to pay the full amount in advance with their client's credit card; however they did inquire as to what there was to see in the area, but did not appear very interested in any details.

Lynne suggested that the couples pay via PayPal, but the travel agent claimed they couldn't use it, and instead sent the couple's credit card detail via email. When Lynne tried to process the booking, the bank declined the credit card transactions.

Lynne said the most suspicious factor was that the supposed travel agent wanted the Japanese clients to pay us the total amount, and have us pass on the commission to the agent.

The scammers had used credit card information from Japanese tourists who had been traveling in Bali. They were hoping that Lynne would send the 'commission' to them following their fake booking. Ultimately, Lynne did not lose money to the scam, but there are plenty of small businesses around that may have.

The bright point to this story is that Lynne used some common sense and business savvy to run the card first before to make sure that is valid before releasing any of the cash to the scammers.

Scenario #2

Nicole was browsing the internet one day, using her home computer. A pop-up appeared on her screen telling her that she had won a holiday to the Bahamas, but in order to retrieve her prize she would have to call the number listed within 3 minutes to claim the prize. Nicole immediately called the number. A female voice with an American accent answered the call and told Nicole in an excited voice that she had won the holiday.

The woman who answered the phone spoke very quickly and Nicole was quite excited about the prospect of a holiday. When she asked Nicole is she accepted the holiday, she immediately said "yes".

The woman mentioned some figures that didn't seem to have any connection to the holiday prize, and asked Nicole for her credit card details. It wasn't until she asked for these details that Nicole began to suspect that she had not 'won' the entire holiday. After the woman had taken Nicole's credit card details, she told Nicole that she was 'locked in' to buying the holiday.

Nicole panicked when she heard the term 'locked in' as she and her husband are both students. Once she realized the holiday had been charged to her credit card, Nicole asked to withdraw but the woman refused. Eventually Nicole did request to speak with a manager who also refused to let her out of the holiday and was forced to listen to a recording with the company's terms and conditions and confirm that she understood and agreed to them. She was threatened with the company charging her an additional $1,000.00 is she did not follow through with this.

Nicole immediately called her bank and cancelled her credit card. The bank said they would do their best to recover the money. Nicole's husband spent several hours on the internet trying to locate and contact the company. Eventually he did make contact via phone and the person was apologetic and promised a full refund, however the next day when they contacted Nicole again, they gave her a false telephone number. The bank was able to recover their money, however this scam caused Nicole and her husband a lot of time, hassle and worry.

Nicole remembered the remedies that were available to her, since this transaction was with a credit card. As a consumer, you are afforded certain rights when the card is used on the transaction. In most cases (98%) "If it is too good to be true, then it possibly is."

In this report, we intend to inform you of scams to be aware of if you use online shopping and what you can do to prevent yourself from being a victim. We will provide you with the information as to what to look for so you can feel safe shopping on-line.

A NEW AGE

Unfortunately the number of people in situations like Nicole is growing, as more and more people are using the Internet for things like research, surfing and shopping. The popularity of on-line shopping especially is growing. On-line shopping doesn't require you to leave your house, it allows you to quickly compare prices without spending the difference on gas and it opens a greater variety of choices. With on-line shopping, you can shop any time you feel like it, you're not limited to when a store is open.

There are multiple types of on-line shopping. Many brick and mortar stores, like Target and Circuit City, have on-line stores as well. This allows the public to buy from somewhere they trust, without the hassle of holiday crowds or a long drive to the store. Consumers can also buy anything that the store carries, not just what is in stock at their local store.

Other stores, like Amazon.com, only exist on-line. Some of these stores have been in business long enough to become just as trusted as stores like Borders. They offer the same conveniences as the other stores, but often can provide lower prices because they do not have to pay for many locations and other overhead costs brick and mortar stops incur. Like Target.com, shoppers can purchase from the website and have it shipped to the recipient without the hassle of having to pack it up and ship it themselves.

Of all the other sites that host auctions, E-bay is one of the most well known sites. These sites provide a place to both buy and sell. These sites are one of the best

ways to find things like out-of-print books and antiques. They also are a great place to find “almost new” things for a good price. For example, a new computer game may cost $49.95 at a retail store, but a person who played it once and decided they didn’t like it could auction it off at a much lower price.

Craigslist is a collection of on-line sites that perform multiple purposes. The web site is mostly divided by city. Detroit listings are on different pages than Albuquerque listings, for example. Craigslist has pages for job openings, personals, selling and giving away things Also, it has discussion pages and a place to share local news such as church rummage sales or volunteer events.

CAUTION: THE WARNING SIGNS

There are many types of scams that people need to be aware of. They range from lottery scams that promise great financial winnings, to scams resulting in credit card and identity theft, where the individual's personal information is compromised. Once this happens, unfortunately the victim's identity probably has been stolen.

The overall objective of this section is to introduce the schemes, give practical examples, and explain how the fraud takes place. It will also show what typical information is sent from the scammer to entice the victim and finally, a look at who scammers really are.

Online Shopping Scams

Online shopping has made it easier to find the merchandise we want that the local shopping plazas don't have. In fact, online shopping is oftentimes more efficient than in-store shopping and the quantities of styles and items available are much larger than what can be found in traditional stores. There are plenty of legitimate companies online, but there are also fraudulent sellers out to cheat consumers. Setting up a fancy webpage or posing as a reputable seller, is not difficult to do on the internet. For example, sending offers, extending credit lines, and shopping sprees by e-mail are easy and inexpensive. Dishonest sellers may even misrepresent what they are offering, take your payment and never provide the merchandise or resolve the problem when you make a complaint. One way to make sure that you are dealing with a reputable business is to look for one of the web assurance logos on their website.

Lottery Scam

The Lottery scam begins with an e-mail transmitted as spam to a lot of unsuspecting victims. The victim unknowingly opens this e-mail because more often than not, the subject line is enticing. This e-mail is from someone *you don't know*, claiming you have won a large amount of money in a lottery you have never heard of. This e-mail looks so official; it's no wonder why the victims are duped into this scam. They promise to supply you all the details to collect your winnings after you pay something. The scammer will usually ask recipients to wire money from small fees to larger payments of thousand of dollars to cover such things as taxes; release fees; filing fees; and fiduciary fees.

This all sounds legitimate to the victim, since the fatal assumption is that there are normally fees to cover the movement of monies internationally. This reason alone, allows the scam to succeed. This scam is basically a random fishing expedition. If you respond in any way to the email, the scammers will send further messages or even contact you by phone in an attempt to draw you deeper and deeper into the scam. Also, you may be asked to provide banking details, a large amount of personal information, and copies of your driver's license and passport. Moreover, if you comply with these requests, the scammers will have enough information to steal your identity.

Online Auction Scams

It is possible to buy almost anything over the internet these days. Unfortunately, scammers can use the anonymous nature of the internet to rip off unsuspecting

shoppers. Scammers can pretend to be selling a product, often very cheaply, just so they can steal your credit card or bank account details. Similarly, they may take your money but send you a faulty or worthless product instead of what you thought you were ordering or even nothing at all.

Most online auction sites put a lot of effort into spotting scammers, which is why scammers will often try to get people to make a deal outside the auction site. They may claim that the winner of an auction that you were bidding in has pulled out, and then offer the item for sale to you. Once they have your money, you will never hear from them again and the auction site will not be able to help you.

Another common trick is for an online auction to be rigged by the scammers. If you are selling a product, the scammer can enter a low bid followed by a very high bid under another name. Just before the auction closes, the high bid will be withdrawn and the scammer's low bid will win. If you are buying a product, the scammer can arrange for dummy bidders to boost the price up. Auction sites do not allow this practice either, but it is very hard for them to police.

Counterfeit Check Scams

If you received a letter or e-mail claiming that you were an entitled to a huge payment would you know how to handle this situation? What if you were an unsuspecting consumer selling items in a classified ad or online at auction sites and a buyer wanted to pay for an item with a check? This scam is initiated in response to a legitimate activity that you are pursuing. Once the scammer is in touch with you, they

often chat via email or phone, talking about the item or service you have for sale. They appear friendly, sincere, and aboveboard. Also, they don't want you to send any money in advance, only after you have their money deposited in your account. They work hard to win your trust, but appearing trustworthy is the con artist's primary tool in getting you to accept the scheme as genuine.

In either case a check is received as payment for the goods or amount that you are allegedly entitled to. In most cases, the scammers would issue a certified check to ease any suspicions of the victim. Most of the time, the scammers will issue the "certified check" for more than the amount required. Once this "certified check" is received, a note is usually attached to it requesting that you cash the check and wire the difference back to them, citing one of a number of believable reasons why the amount was incorrect..

The biggest reason this scam draws numerous people in, is because the scammer appears to have sent you what appears to be the equivalent of real money, usually in the form of a cashiers check drawn on a U.S. bank, a postal money order, or certified check. Then you are requested to wire or express part or all of that money to the scammer or some third party, immediately. The predator relies on the victim's belief that real cashier's checks, certified checks and postal money orders can be trusted more than personal checks. In some cases the counterfeit checks or money orders that the scammers send are so real looking that they can even fool a bank teller, and very, very tough to identify as fake.

Over Payment Scams

Similar to the counterfeit check scam, check overpayment scams target consumers selling cars or other valuable items through classified ads or online auction sites. Unsuspecting sellers get stuck when scammers pass off bogus cashier's checks, corporate checks, or personal checks. The scam artist replies to a classified ad or auction posting, offers to pay for the item with a check, and then comes up with a reason for writing the check for more than the purchase price. The scammer asks the seller to wire back the difference after depositing the check. The seller does it, and later, when the scammer's check bounces, the seller is left liable for the entire amount and without the item they were selling in the first place.

Phishing Scams

Phishing is a scam in which the attacker sends an email purporting to be from a valid financial or eCommerce provider. The email often uses fear tactics in an effort to entice the intended victim into visiting a fraudulent website. An example of this is claiming the recipient's bank account is frozen until information is updated. Once on the website, which generally looks and feels much like the valid eCommerce site, the victim is instructed to login to their account and enter sensitive financial information such as their bank PIN number, their Social Security number, mother's maiden name, etc. This information is then surreptitiously sent to the attacker who then uses it to engage in credit card, bank fraud and/or outright identity theft. Here are a couple examples of these Phishing type schemes:

Social Security Scams

Claiming to be from the Social Security Administration, the scammers tell recipients about the 3.3 percent cost-of-living bump in benefits for 2007 (or which ever year is applicable), with the following instructions: "We now need you to update your personal information. If this is not completed by November 11, 2006 (or some date before the next year), we will be forced to suspend your account indefinitely." Would-be victims are then directed to a website that looks like the Social Security Administration's official site. Once directed to the phony website, they are asked to register for a password and to confirm their identity by providing personal information such as their Social Security number, bank account information and credit card information. This scam is particularly effective at targeting senior citizens who rely on Social Security as their main form of income.

The Social Security COLA Phishing scam will join the annual parade of faux government agency e-mail assaults, which generally start during tax season.

Payment Processing Scams

Scammers disguise their intentions under legitimate payment companies that operate for the protection of consumers. They copy the letterhead or trade marks used by finance companies. They then send an email that appears to be from Pay Pal, e-bay, Visa, Master Card, or any financial intuition which states that your account has been compromised. If you click on a link it will take you to a copycat site that looks identical to Pay Pal, e-bay, Master Card, or Visa. They will ask you to enter personal

information such as your Social Security number and bank account numbers. Many unsuspecting people have lost their life savings through being fooled by this trick. Once it is in the hands of the cyber criminal, your whole life becomes a nightmare when you attempt to straighten out the mess. This translates into horrendous debt, or worse. They can use your personal information to perpetuate a fraud in your name.

Online Credit Repair Scams

The email promises that negative information on your credit report with credit bureaus can be erased for an upfront fee. It is illegal and impossible to remove negative information from a credit report when the information is true. If the information is false you can call the credit bureau directly and have the information removed for free

Other Types of Scams

Usually during the holidays, various other types of scams show up to the unsuspecting victim. These include everything from what looks like free money to charitable solicitations that will really tug at your heart strings. Here are some of the other types that could show up unexpectedly and put a real damper on things if you give in.

Loan Scams

A loan scam occurs when a business is offered an unsecured business loan by telephone, Internet, or mail. While application fees are common, excessive fees such as processing or first month's fees due before approval, should be a red flag. These

scams are aimed at getting your money quickly and disappearing or rejecting your application altogether, leaving you with no loan, less money and a lot of questions.

Generally, talking to your own bank for a loan should be your first choice. It's a good bet that if your own bank isn't willing to give you a loan, no other reputable lending institution would be willing either. If it sounds too good to be true, it probably is and could wind up costing you hundreds or thousands of dollars.

Charity Frauds

Spam e-mail is sent to many users describing an occurrence of a great disaster that has made the news, usually with either real or fabricated people's stories calculated to make you empathize. Hurricane Katrina, wildfires in California and tsunamis in Thailand all come to mind. Starving children in Africa has always been a common choice with these scam artists. Actually you could choose any country and add starving children and this scam is complete. Recently, there have been scams that used simulated Internal Revenue Service letterhead/markings. All of these scams have one thing in common, and that is, to tugging at your heartstrings. Welcome to the Charity Fraud! These messages try to take advantage of your generosity and kindness, but they will not be used for the purpose you believe. Their primary function is to collect monies from kind and generous people all under the guise of being a real charity. The scammer's goal is to try and make the e-mail and website appear as legitimate as possible creating this phony storefront. Once the victim responds to the plea, the scammer has retrieved some very valuable information from the victim. Bank account

number and credit/debit card information is enough information to obtain not only the original donation, but other unsolicited donations as well.

Not only do these scams cost people money, they also divert much needed donations away from legitimate charities and causes. Luckily these types of scams are not that common. However, you should always be on your guard and use a little bit of common sense when choosing to donate to one of these charitable e-mail requests.

Home Based Jobs

Americans have flocked to websites in search of better or higher paying jobs, but have fallen victim to opportunities that do not exist. The various online recruiting sites such as Career Builder.com, HotJobs.com, and Monster.com have grown from job-posting boards into Web sites hosting millions of résumés and thousands of available jobs. Unfortunately, crooks have also discovered this lucrative field of online recruiting, and they've been busily devising new schemes to exploit job seekers. One of the most prevalent scams is a cyber-twist on an old con; "The fraudulent job-placement scheme."

Job hunters who have publicly posted their résumés receive spam e-mail touting phony employment or work-at-home business opportunities. The object is to get the victim to pay a big fee, sometimes upwards of thousands of dollars, for job-placement assistance or to start a home business. However, these hyped job openings, often touted as government positions, are really nonexistent. These jobs actually serve as the bait to lure the victim into the scam. Most of these sites will require an up front payment before they can "process your application." That is usually the first indicator

that you are walking into a scam. Another indicator is that the scammers are requiring the job applicant to submit to a pre-employment background check in order to be hired. They required the applicant to provide sensitive personal data, which sometimes includes checking-account numbers and/or social security numbers. A real background check does not require you to provide any of that type of information. With this information the thieves can use this personal information to create bogus credit cards, take out loans, or drain checking accounts. In other words, steal your identity!

Most legitimate sites will examine you based upon your posted resume and if you qualify, they will send a copy of their fee structure and contract. You should be aware of sites that advertise government jobs, because most all of the government jobs can be viewed free in classified ads or online job boards. There is a requirement that they be posted in a public forum to be viewed. All of these postings for federal jobs require you to go to www.usajobs.gov for application procedures. That is the only website authorized for federal governmental positions.

Travel Offer Scams

An unsuspecting individual receives a postcard, telephone call, e-mail or fax offering you an all-inclusive vacation at a luxury resort. The price is very low and looks great, but you are often hit with hidden fees and taxes. You can have trouble getting the dates you want to travel and then be forced to pay an upgrade fee, and some of the luxury hotels turn out to be anything but. Some of these trips offer the hotel at a low price, but not airfare. A lot of consumers have complained that they bought their plane tickets only to find out the hotel they wanted wasn't available, or the dates they wanted

for the hotels were sold out. If you buy the airfare, and learn the hotel isn't available for when you wanted to travel, you might have a hard time getting your money back for the flights. . If you can't get your money back you might be able to pay a fee to change the flights or else you'll be forced to pay fees to get a hotel for when you want to travel.

Investment & Real Estate Scams

Some investment seminars may try and convince you to follow high risk investment strategies, such as borrowing huge sums of money to buy property. Others promote investments that involve lending money on for no security or with other risky terms. While investment advice can be legitimate and beneficial, it is important to look carefully at what an investment scheme or seminar is offering. Attending an expensive seminar or investing in the wrong kind of scheme can be costly mistakes.

You could be invited to an investment seminar in a number of ways. You might receive a letter drop in the mail, see an ad in a newspaper or magazine, or hear about it through word of mouth. The seminar may promise that a motivational speaker, an investment expert or even a self-made millionaire, will give you advice on investing.

The seminars and real estate investment schemes make money by charging you attendance fees, by selling you over-priced reports or books and by selling property and investments without letting you get independent advice. They often make misleading or deceptive claims or pressure you to buy into investments that will end up losing you money.

The investments that the seminars offer are often over-valued and you may have to pay fees and commissions that the promoters did not tell you about beforehand. The seminar promoters might offer rent guarantees or discounts for buying the plan, but these may not deliver the benefits they promise when the total cost of the deal is taken into account.

Some seminars or schemes may even fly you to the property location to view the property. They will try to pressure you into committing to the deal without giving you time to obtain independent information or advice. This tactic can incite more trust, since you have seen the property. It feels more “open” and thus safer.

Nigerian Scams

The most common form of the advance fee con is the African or Nigerian money version. The scam will start with you receiving a message from someone you've never heard of from somewhere exotic in Africa, Eastern Europe or perhaps Asia. This person claims to control or knows about some secret bank account that belongs to a former dictator, dead family member, disappeared rich person, etc. In order to access these funds, they claim to need you to supply them with your account information for various reasons. In return for this little service, you'll supposedly get a hefty slice of the total. If you follow up and express interest, you can expect to receive warm appreciation, official looking bank documents showing the deposits and the coming transfer to you. This is where the scam happens, you will need to send a payment as proof of your bona fides and to cover processing fees or bribes to officials, or you will need to supply your own banking information in detail. You'll never see the money you

invest, nor will your account swell by the expected millions. Appendix A has a sample of a Nigerian Letter and what to look for to spot its phoniness.

Iraq Soldier Advance Scam

An increasingly common tactic being used by advance-fee scammers is to pretend to be a US soldier based in Iraq who has found a stash of hidden loot. For example, a fictitious soldier, and his comrades have chanced upon a fortune in cash apparently hidden by Saddam Hussein. But, claims the email, the soldiers need your help to move this money out of Iraq so that they can invest it, and of course, they are willing to offer you a generous percentage of all this lovely cash in exchange for your help. This scam seems to sounds like a great opportunity. You could become a millionaire overnight just for helping out a bunch of patriotic soldiers who surely deserve a reward for the extreme hardship and danger they face every day.

The substantial amount of cash is just a figment of some slimy scammer's imagination who is certainly not a soldier based in Iraq. Like thousands of similar variations, the email is designed to tempt the gullible into agreeing to participate in this enticing, once-in-a-lifetime opportunity. Even if it were real, it is illegal both under US law and the UCMJ (Uniform Code of Military Justice) to remove any such treasure found in foreign countries.

Once our hapless victim agrees to proceed, the scammers will begin sending him requests for upfront payments. These payments, the scammer will claim, are entirely necessary if the deal is to be successful and they cannot, under any circumstances, be

deducted from the lump sum. These payments are needed to pay bribes, insurance, legal expenses, delivery costs, or any other fanciful excuse that he can come up with. The scammer will continue to extract further payments from the victim until they have no more funds or finally realize that they are being conned.

Scam email cover stories about hordes of cash found by soldiers in Iraq may seem believable to some potential victims because such finds have actually occurred and have been widely reported in the media. In fact, some versions of the scam include links to genuine articles about such finds and even use the names of real soldiers in an attempt to add credibility to the scammer's spurious claims. In many articles, the media neglects to report on what happens to the find. This omission seems to lend credibility to the scam since it does not prove it wrong. Unfortunately, Nigerian scams like this continue to claim victims all around the world.

Soldier's Death Scams

Scammers are now targeting families of soldiers killed in Iraq by claiming to be connected to the Homeland Security Department. Both of the common scams are online pleas for help and money, fraudulently linking the scammers to the bureau. In one scheme, an e-mail is sent to families of U.S. soldiers killed in Iraq which includes a link to the bureau's website. The e-mail claims to seek to recover money from a friend of the slain soldier.

In a similar spam e-mail, the scammer identifies himself as being sent by a federal agent trying to track down funds looted from the Iraqi Central Bank by Saddam Hussein's son. The e-mail also links to the bureau Web site and asks for confirmation

of the recipient's address. The scammer's letter states that there is a very important and confidential matter that they urgently wish to discuss with you. The bogus e-mails resemble the so-called "Nigerian letter" discussed above.

Online dating scams

Most dating sites are full of these scams, and many don't bother to get rid of them because the scammers' profiles look good. The scammers use model photos and have elaborate profiles that attract more members to them. The victim signs up to an internet dating site, such as Singlesnet.com, Match.com or Yahoo Personals. They create a profile, look around the data base for singles in their area to meet and hopefully make a romantic connection with and come across a scammer's profile.

Once the victim expresses interest, the scammer sends a pre-made letter that looks legitimate. However, the letter gives the unsuspecting victim an alternative e-mail address to correspond with them. Once the victim contacts the scammer outside of the dating site, they will slowly establish a phony trust or friendship with the victim. The scammer may exchange emails with the victim for days or weeks. They may even talk to the victim on the phone until a decision is made to meet.

The scammer claims he cannot afford to travel to where the victim lives, but offers to meet somewhere in the middle and requests money to help pay for this. After the victim sends the money, they never hear from the scammer again or receive ongoing excuses to delay the trip. Another angle the scammer will use is that they have a sick child or relative, or are stuck in another country and they need your money to

help. A professional scammer is very good at making you feel sorry for them. You may feel inclined to help them and send them money.

809 Area Code

You receive an email, letter, or some other communication which seeks to convince you to call a number in the 809 area code. The message is always urgent (that's a common theme of virtually all scams - they have to happen NOW) and appears important or critical. You may receive a spam email which says something like, "You have 24 hours to settle your outstanding debt before it is sent to collections. Call me now at 809-xxx-xxxx to preserve your credit." Call the number and you will be billed as much as $25 per minute! Some people receive a postcard, which states, "You have won! Call 809-xxx-xxxx to get your prize." Call the number and you will get your prize all right - a $150 charge on your phone bill!

There was one case in which someone received an ICQ message saying their relative was in the hospital with a terminal illness. The poor person called the "809" number only to be put on hold for a very long time - over an hour – and then was hung up on. He called over and over, frantic and distraught - and got a phone bill of over a thousand dollars!

The 809 area code is similar in concept to 900 numbers. You get charged either per call or by the minute. The problem is that the 809 area code is in a foreign country, like the Dominican Republic in the Caribbean and thus is not covered by United States law.

In the United States, all 900 numbers must state in their advertisements and at the start of the call the cost of the call. You also have a small period of time, usually the first minute, to hang up without being charged. The 809 area code has no such restrictions. Because you made the call voluntarily, it's very difficult to get the phone company to reverse the charges. In fact, in many cases you will find yourself arguing with a foreign phone company, which states that you made the call and they did nothing wrong and thus you need to pay.

Definitions

Below are definitions of some computer lingo and the various types of viruses:

Cracker

Crackers are often mistakenly called "hackers." Crackers are the "bad guys" who seek to "crack" or gain unauthorized access to computers, typically to do malicious things (e.g. to steal credit card information or crash the computer.) Crackers might do this by writing a virus, worm or Trojan horse. Alternatively, they may just exploit weaknesses in the computer's operating system in order to gain entry. Many crackers will install a "backdoor" which allows the cracker to "remote control" your computer over the internet. This allows them to distribute child porn or perform a denial of service attack against somebody else. Most crackers aren't particularly smart and merely take advantage of well-known, existing security flaws or the gullibility of the typical internet user.

Hacker

When used properly, this term refers to an elite breed of "good guys" who are talented computer programmers. They enjoy solving challenging problems or exploring the capabilities of computers. Like a carpenter wielding an axe to make furniture, the hacker does good things with his skills. True hackers subscribe to a code of ethics and look down upon the illegal and immoral activity of crackers (defined above). When the press uses "hackers" to describe virus authors or computer criminals who commit theft or vandalism, it is not only incorrect but also insulting to true hackers.

Psychology of a scammer

There have been many debates on why online scams succeed. Scammers target people of all backgrounds, ages and income levels across the world. There is no one group of people or demographic who are more likely to become victims of a scam. If you think you are too clever to fall for a scam, you may take risks that scammers can take advantage of. Scammers have succeeded because of two things. First, a scam looks like the real thing. It appears to meet your needs or desires. Second, the scammers manipulate you by enticing you to produce the response they want. Psychological tricks are used in scams, as well as exploiting peoples' belief that everyone is honest and sincere. While intellectually people realize these people are out there, we rarely believe that they are the people we deal with. Scammers often use psychological triggers to get an automatic response from you without you realizing it. Greed is the ultimate vehicle that the scammers use to entice the victim and is utilized

most often. The victim can always fight back by following a simple rule: “If it is too good to be true, then it probably is.”

Viruses

A virus is a program that propagates itself by infecting other programs on the same computer and usually sends itself to other computers by infecting e-mails the victim sends. Most viruses can do serious damage, such as erasing your files or your whole hard drive. Some viruses have been known to totally lock up and shut down your computer. Other viruses may just do silly/annoying things like pop up a window that says "Ha ha you are infected!" or other similar phrases. There are some viruses that are functional and open certain security doors to allow access to the individual computer. True viruses cannot spread to a new computer without some form of human assistance. Trading files is the normal way of spreading these viruses; however, it has been known that even opening up e-mail can spring a virus in your computer. The best protection is using a service that provides some form of file scan before it is opened. Below are some examples of these types of viruses:

Worm

The worm is also a program that propagates itself. Unlike the virus, a worm can spread itself automatically over a network from one computer to the next. Worms are not clever or evil, they just take advantage of automatic file sending and receiving features found on many computers.

Trojan horse

This is a very general term, referring to programs that appear desirable, but actually contain something harmful. The harmful contents could be something simple, for example you may download what looks like a free game, but when you run it, it erases every file in that directory. The Trojan's contents could also be a virus or worm, which then spread the damage.

Remote Access Trojan

Abbreviated as RATs, a Remote Access Trojan is one of seven major types of Trojan horse designed to provide the attacker with complete control of the victim's system. Attackers usually hide these Trojan horses in games and other small programs that unsuspecting users then run on their PCs.

Data Seeking Trojan

This type of a Trojan horse is designed to provide the attacker with sensitive data such as passwords, credit card information, log files, e-mail address or IM contact lists. These Trojans can look for specific pre-defined data (e.g., just credit card information or passwords), or they could install a key logger and send all recorded keystrokes back to the attacker.

Destructive Trojan Horse

A type of Trojan horse designed to destroy and delete files, it is more like a virus than any other Trojan. Unfortunately it can often go undetected by antivirus software.

Proxy Trojan Horse

A type of Trojan horse designed to use the victim's computer as a proxy server. This gives the attacker the opportunity to do everything from your computer, including the possibility of conducting credit card fraud and other illegal activities, or even to use your system to launch malicious attacks against other networks.

FTP Trojan

A type of Trojan horse designed to open port 21 (the port for FTP transfer) and lets the attacker connect to your computer using File Transfer Protocol (FTP).

Security Software Disabler Trojan

A type of Trojan horse designed to stop or kill security programs such as an antivirus program or firewall without the user knowing. This Trojan type is normally combined with another type of Trojan as a payload.

DoS Attack Trojans

This is short for denial-of-service attack. What it does is to attack a network and bring that network down by flooding it with useless traffic. Many DoS attacks, such as the *Ping of Death* and *Teardrop* attacks, exploit limitations in the TCP/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like viruses, crackers are constantly dreaming up new DoS attacks.

POSSIBLE SOLUTIONS

There are many ways for you to prevent or protect yourself from fraud. When purchasing items online, there are some precautions that a customer needs to take. One of the biggest things a consumer needs to know is whom they are making the transaction with and what they are making that transaction for. Most businesses that offer online purchasing have terms and conditions listed before you purchase an item. As a consumer, it is recommended that you read through those terms to help yourself understand how the process of purchasing an item works if something were to go wrong, either with the shipping or damaging of an item. Most items purchased online have to be delivered, rather than picked up. The buyer needs to know how long the delivery will take and what happens if the product purchased never shows up. Also, the consumer needs to know what they are all paying for in the transaction taking place. For example, does that digital camera come with the case pictured with it? Furthermore when paying online by credit or debit card, make sure you check the company's security policy. This will ensure the safety of the financial and personal information that they are presenting. . If you were to use a debit card, it is wise to change the account numbers on your card after several uses or utilize a virtual card service such as what PayPal offers. A consumer should take this precaution because no matter the security of the sites, the risk of your information being stolen rises with each online transaction.

When looking for items online to purchase, there are some other things consumers need to look out for. If a product looks too good to be true, then most of the

time it probably is. For instance if a price is unbelievably low, than the consumer should look into the business to make sure it is not a scam or that there is nothing wrong with the product. Once the buyer has agreed to make a purchase, they should print out the agreement, which would include any emails or conversation regarding the transaction. This will help create evidence if something were to go wrong with the sale. These are just a few of the steps a consumer can take when purchasing an item online.

A popular type of online shopping is online auctions. Many scams can take place on these sites when purchasing an item. As a buyer, look at the seller's rating. Most auction sites have a rating system on both sellers and buyers. Make sure the seller does not have a bad rating and if they do, see why by checking comments if they are available. Additionally, complete the sale on the auction site and not through a private transaction because if the sale is not completed on the site and something were to go wrong, the site does not protect the buyer. Furthermore, look at the online auction's site's information to make sure the site itself is legitimate.

When a consumer is shopping online, it is recommended that they pay by credit card. The Fair Credit Billing Act protects consumers when they purchase items by credit or charge cards. This act allows the company to be investigated if a consumer is reports unauthorized charges.

Any time someone is shopping online, consumers should never give their credit card information out to just anyone. Be careful on who the information is given to by checking out the website information. Additionally, credit card or personal information should not be sent by email or instant messaging. Doing this would help prevent money being stolen from you.

Credit card information can be stolen online, even if the consumer is not sending it in an email your information can be obtained using web "cookies". Cookies are an informational data packet stored on home computers that were sent from a website. These cookies are needed to produce websites that work functionally. The cookies help store memory, so if a person needs to go back to the site later, the information is still there. Also, cookies can be used to store preferences on computers for individuals.

Cookies can be stolen a few different ways when being sent back and forth between servers. They can be stolen a few different ways. One method is called session hijacking. A third party steals the cookies and reads them using packet sniffers, which is a computer program designed to read cookies. So be careful how much you use your credit card online.

There is computer software that can be used to help prevent hackers from stealing your financial and credit information, anti-virus software. This software also prevents viruses from infecting your computer. Anti-virus software can be used to build a firewall to protect your computer system. A firewall is a guard to keep out computer hackers. This software should be updated regularly to keep up with the changing viruses. There is computer software that can be used to help prevent crackers from stealing your financial and credit information. This type of software is called anti-virus software. This software also prevents viruses from coming into your computer. Anti-virus software can be used to build a firewall to protect your computer system. A firewall is a guard to keep out computer crackers. Most available software offer updates anywhere between every day and once a week.

One of the biggest parts of security a consumer needs to take is using common sense. Using common sense can prevent some of the biggest scandals. Some of the biggest scandals can be prevented this way. If something looks distorted or sounds “too good to be true”, then it probably is not a good situation. Refer to the appendix for an example of a letter that offers something that seems good, but is a scam. After the letter, there are some points on what to look for in the letter that shows it to be a scam.

Lastly when on an online shopping site, look for the site’s certifications. The certification will help determine how safe the site is. There are many different types of certifications to look for. Looking for these may help prevent and protect you against online fraud.

HOW TO RECOGNIZE A SAFE SITE

We have mentioned frauds and scams and covered some aspects of preventing them. Now, we come to one of the main aspects of online shopping, web assurance seal services/certification. Web Assurance Seal is an online service that rates the trustworthiness of e-stores. Depending on an Assurance Seal, consumers completing transactions with unfamiliar e-stores can see the trustworthiness of the site. Usually, Web Assurance Seal Services are categorized into 3 groups or dimensions. They represent security, privacy and business integrity of the e-store. We are going to cover the certification process of these businesses.

There are 3 types of certifications:

1. Knowledge Based Certifications
2. Organizational Based Certifications
3. Technology/Product Based Certifications

Knowledge Based Certification – certifying an individual knowledge and skills. For instance, Cisco identifies these individuals as Cisco Certified Security Professional (CCSP), Cisco IPS Specialist, Cisco VPN Specialist. Consumers might also come across the seals such as Certified Internet Web, Comp TIA Security+, MCSE: Security, EC-Council, etc.; these are also knowledge base certifications.

Organizational Based Certifications – certifying an organization that has reached certain standards. Some Organizational Based Certifications are NIST, CICA, CESG, ASIS, CPP, etc.

Technology/Product Based Certification – certifying that a technology/product or system has been accredited at a certain standard. This is the most common type of certification. For example, TRUSTe, Visa, *Verified by Visa*, VeriSign, Webtrust, Systrust, etc. The whole idea of the certifications is to provide assurance to customers about the business' principles. That is, the disclosure and follow-up with its promises. The current Federal Trade Commission (FTC) online privacy standard is based on the Fair Information Practice Principles. These principles must be met before the approval of the seals or certifications. They are:

Notice: Data collectors must disclose their information practices before collecting personal information from consumers;

Choice: Consumers must be given options with respect to (1) whether and (2) how personal information collected from them may be used for purposes beyond those for which the information was provided;

Access: Consumers should be able to view and contest the accuracy and completeness of data collected about them; and

Security: Data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use.

Websites with high standards of privacy practices can join and benefit from seal approval programs without making large changes in privacy policies. Websites with lower standards would be required to make significant changes in privacy policies in order to join and benefit from seal approval programs. Privacy seals differ from security seals, because privacy seal grantors do not review a sites' technology in detail, instead examines the business processes and use of personal information. Security seal

grantors examine the measures that website takes to safeguard the personal information. And then, we have business integrity seals or certifications. Business integrity grantors mostly deal with customer service, examining FAQ section, complaints, comments, queries, refund policy, company contact information, etc.

The strategic design of such seal programs is a key ingredient of their effectiveness. For example, consider the two types of monitoring costs borne by a firm that sponsors and administers a seal program. First, the sponsoring firm must ensure that all members meet the specified requirements to obtain the seal. Second, the sponsoring firm that runs the program must ensure that all members continue to abide by its policies over time. The greater the requirements (i.e., the more rigorous the program), the higher the costs per member (both initial approval costs and ongoing monitoring costs).

A key feature of Internet seals of approval programs is that companies that agree to abide by the seal of approval standards (and pay a registration fee) are authorized to place “privacy seal of approval” logos on their Web sites. And they require each licensee Web site to post a seal logo that acts as a hyperlink to the seal’s site to act as an authentication procedure for visitors to the licensee site. Each licensee site was examined to determine if it displayed a seal logo or words promoting participation in the seal program, and whether either of these was hyperlinked to the appropriate seal site. The location of the seal logo(s) or other seal information on the licensee Web sites was also determined. The majority of licensees displayed their privacy seal of approval information on both the home and privacy pages of their Web sites. Some companies

displayed privacy seal information on only a privacy policy page, while another displayed only on the home page.

You can find more information from following websites.

Visa www.visa.com

SysTrust, WebTrust www.aicpa.org

BBBOnline www.bbbonline.org

TRUSTe www.truste.org

VeriSign www.verisign.com

Bizrate www.bizrate.com

TRUSTe, that protects the privacy of personal information usage and has about 1500 clients. BBBOnine follows with about 700 clients. The most popular security seals

are *VeriSign*, WebTrust, while BizRate.com, BBBOnline Reliability Program seals are popular for business integrity ratings.

In conclusion, we see that investigation of company type and/or size isn't enough. We, online consumers, must pay close attention to the Assurance Seals or Certifications that rate the security, privacy and business integrity of the websites. These Assurance Seal Services are essential in determining the trustworthiness of the e-store and play a big role in avoiding frauds, scams and identity theft.

APPENDIX A

Dear XXXXX,

My name is Mrs. Elizabeth Justin. a branch manager and also the personal accounting officer to Late Engineer Johnson Smith, a national of your country, who was an oil merchant/contractor with the federal government of Nigeria. On Saturday 4th may 2002 he had an accident via the ill-fated eas airline crash in Kano. All occupants of the plane unfortunately lost there lives. Since then I have made several enquiries to your embassy to locate any of his extended relatives, this has proved unsuccessful.

You may visit the following websites to read more about the incident.

Http://news.bbc.co.uk/1/hi/world/africa/1968616.stm

After these several unsuccessful attempts, I decided to track his last name over the internet, to locate any member of his family hence I contacted you. I have contacted you to assist in repatriating this money and property left behind by our customer who has a sum of US$ 11,500,000 (Eleven Million Five Hundred Thousand, United States Dollars) left with our bank here in Nigeria before they get confiscated or declared unserviceable by the bank as the banking guidelines stipulates that if such money remained unclaimed for over a period of 5 years and 9 months it will be confisticated that is why I am requesting for you to stand as a next of kin of late Mr. Johnson , because you have the same surname and same country, We are going to have this deal together with his personal lawyer who also has the whole legal documents including the death certificate and police report of his death.

The lawyer to Late Engineer Johnson, have gone ahead to prepare an attestation note in your name, as the rightful beneficiary to the fund, which already have been endorsed and certified by the United States Consul General Ambassador Donald McConnell, the fund will be paid to you forthwith, as the beneficiary (if only you heed to this request and work all along with me into it's fruition).in addition to the aforesaid, you will find as Attached in this e-mail, photos of the property and photo of the United States Consul General, Ambassador Donald McConnell, when he endorsed the attestation documents at the bank which will enable payment of the fund to be made to you, as the beneficiary.

Furthermore, be informed that your readiness and unrelenting effort to carry out this matter, count because I've made every arrangement to facilitate it's fruition, but need you to finalize it. More so, I've opted to share the inheritance unvaryingly, between the three of us. Let me hear from you so that the lawyer will get in contact with you for more information, remember I am still working in the bank so I will not like my identity been reviewed before the bank as the lawyer will be dealing with you direct.

Please respond only to this emails address for security reasons, remember that I am still working in the bank so do respond to this email address:

mary_jones@scamletter.com

Awaiting your response.

Mrs. Mary Jones.

THE GIVE-AWAYS ON THIS LETTER

Color-coded indications to give you a heads up on these letters:

The first and last name combination tends to change with the first name suddenly becoming the last name.

The dollar amounts are to even and why are they in US monies and not the native currency with a stated exchange rate?

Note that there is very little time to respond

Why did the Lawyer leave this much money lying around? If anything, he should be sued for malpractice, for not properly setting up the late Mr. Johnson's estate.

Also, note the numerous spelling and grammatical errors.

APPENDIX B

RECOVERY TIPS

If you believe that you have been a victim of identity theft, there are four steps that need to be completed. These can be completed in any order. However, all of these need to be done as soon as possible to set a timetable, and, ultimately, to prevent any further problems. You should keep a log of all conversations, mailings, and meetings that have to do with your identity theft recovery. This is in case you will need to reference them in the future.

1. Contact your local law enforcement. You will need to file a police report. Try to bring as much information as you can when filing, including any letters from creditors and if possible fraudulent statements to verify your case. You may also need to complete an ID theft affidavit before coming, which was developed by the Federal Trade Commission This form will formally list all known fraudulent accounts. This affidavit may also be required by any of the companies involved.

Ohio has also implemented the PASSPORT program for ID theft victims. This program issues a special card to ID theft victims, which can be used to confirm their identity when necessary. Local law enforcement will contact all other state authorities by placing the victim in the computer, which may help prevent future crimes from occurring.

2. Contact the credit bureaus. You will need to put a fraud alert on your credit report. This will monitor activity on your report and let you know when someone uses your identity. However, this may not prevent any crimes, because the person may have all your information and may pass through any extra verification procedures. Some states allow for a credit freeze, which stops any company from using your credit report, and that way no one can open accounts in your name. This can be effective in large cases, but it may take time to unfreeze, and it may become increasingly difficult to obtain credit for a while.

You are only required to contact one credit bureau; that one will then contact the other two. However, you may want to contact all three to be on the safe side. You should request a credit report and look it over to make sure you document all fraudulent activity. Once a fraud alert is on your credit report, you are entitled by law to receive a free report. It is always a good idea to follow up and verify that the alert has been placed on the remaining two bureaus.

3. **Close any fraudulent accounts**. Contact all of your current creditors by telephone and in writing to notify them of your circumstances. Ask them if they will accept the ID affidavit, if not ask them for their form. See if you can close your accounts, or possibly change account numbers. Review all your recent statements to make sure you have documented all fraudulent activity. Please see the prevention tips on how to keep track of your creditor's information so you will have it when you need it.

4. **File a complaint with the Federal Trade Commission (FTC).** This is important as your case now becomes a federal case and the FTC may contact authorities in and out of your state regarding your case. You can do this by calling the FTC at 800-ID-THEFT (800-438-4338), or fill out the form at www.consumer.gov/idtheft.

Here is a list of Credit Bureaus you will need to contact:

CREDIT BUREAU	TO REPORT CONSUMER FRAUD
Equifax Credit Information Services PO Box 7402741 Atlanta GA 30374-0241 www.equifax.com	Call 800-525-6285 and write to Equifax
Experian PO Box 2002 Allen, TX 75013 www.experian.com	Call 888-397-3742
TransUnion P.O. Box 2000 Chester, PA 19022 www.transunion.com	Call 800-680-7289 and write to Fraud Victim Asst. Dept P.O. Box 6790 Fullerton, CA 92834-6790

APPENDIX C

PROTECTING YOURSELF AGAINST ID THEFT

- Be careful about the information you give out over the phone or on the Internet unless you are *sure* you know whom you are dealing with. If someone calls you, do not assume they are who they say they are. Insist on calling back on a number you know is legitimate.

- Remember that Web sites can be faked. What may look like a legitimate online storefront or contest may simply be a scam to trick you into revealing personal information.

- Take a good hard look at what you are carrying around in your wallet or purse. Carry only the identification information and the number of credit and debit cards that you will actually need. Leave your Social Security card – and anything that bears that number – in a secure place. Your medical insurance card may have your social security number. Make a copy of the card, black out the number on the copy, and carry the copy.

- Make a photocopy of the front and back of everything in your wallet or purse. Put the copy in a safe place so you will have the account numbers and contact numbers in the event you need to cancel credit cards.

- Do not have your SSN or DL# printed on your checks.

- Make sure checks (used and unused), credit cards, bank records, and other personal information is carefully secured in your home or office, particularly if other people, whether workers or roommates, will be around.

- Guard your mail. If your mailbox is left unattended during the day while you are not at home, consider installing a locked mailbox, a mail slot, or using a Post Office Box.

- Hold onto your purse, your wallet, and your checkbook. Do not leave them unattended. If you discover a checkbook, credit card, or personal information missing, take appropriate action to notify your financial institutions.

- If your deposit account information ends up in the hands of the wrong party, consider closing your account and opening a new one with a new account number.

- Shred documents with sensitive/confidential information before throwing them away.

- Secure your trash. Be careful what you throw away. Statements from your doctor, checks on closed accounts, expired charge cards or IDs are treasures to thieves. . Dumpster divers can piece together little bits of information to get what they need to steal your identity.

- If you do not use pre-screened offers for credit, opt out of receiving them. Call 1-888-5-OPTOUT

- Talk to the financial institutions and brokerage firms where you have accounts about placing passwords on them.

- Choose passwords for online financial services wisely. Avoid anything easily guessed or learned via research, such as mother's maiden name, kids' names, and pets' names.

- Take your receipt with you when you leave the ATM.

- Ask about information security and data storage procedures of the companies you do business with, including your doctor's office, dentist's office, and anywhere else that has your Social Security number.

- Give your SSN only when absolutely necessary.

- Know your billing and statement cycles. If something is late, find out why.

- Check your banking, brokerage, and credit card statements immediately after receipt in order to spot bogus charges.

- Cancel all unused credit accounts.

- Be wary of promotional scams, “You are a winner” letters, and requests for help from strangers in foreign countries who promise you riches.

- Be sure that you receive your check orders in a timely manner.

- Obtain a copy of your credit report once a year and take action if there is information about transactions or accounts you did not initiate.

Sources:

www.helium.com

www.scamwatch.gov.au

http://antivirus.about.com/od/emailscams/ss/phishing.htm

http://www.irchelp.org/irchelp/security/trojanterms.html

http://www.webopedia.com/TERM/T/Trojan_horse.html

http://www.dcu.org/streetwise/march2005.html

http://www.chathamjournal.com/weekly/living/consumer/counterfeit-check-scams-70709.shtml

http://blog.washingtonpost.com/thecheckout/2006/11/scammers_who_keep_up_with_the.html

http://www.wbtv.com/news/onyourside/6591832.html

http://www.consumersunion.org/pub/core_other_issues/000134.html

http://www.associatedcontent.com/article/133641/top_online_shopping_sites.html

http://www.aces.edu/pubs/docs/U/UNP-0037/UNP-0037.pdf?PHPSESSID=ae3e2dddf1ea74963e68612cb6129fc7

http://www.lbry.com/articles/424/1/Scams-and-Frauds:-809-Area-Code

http://www.wvrecord.com/arguments/192619-could-you-spot-a-counterfeit-check-scam