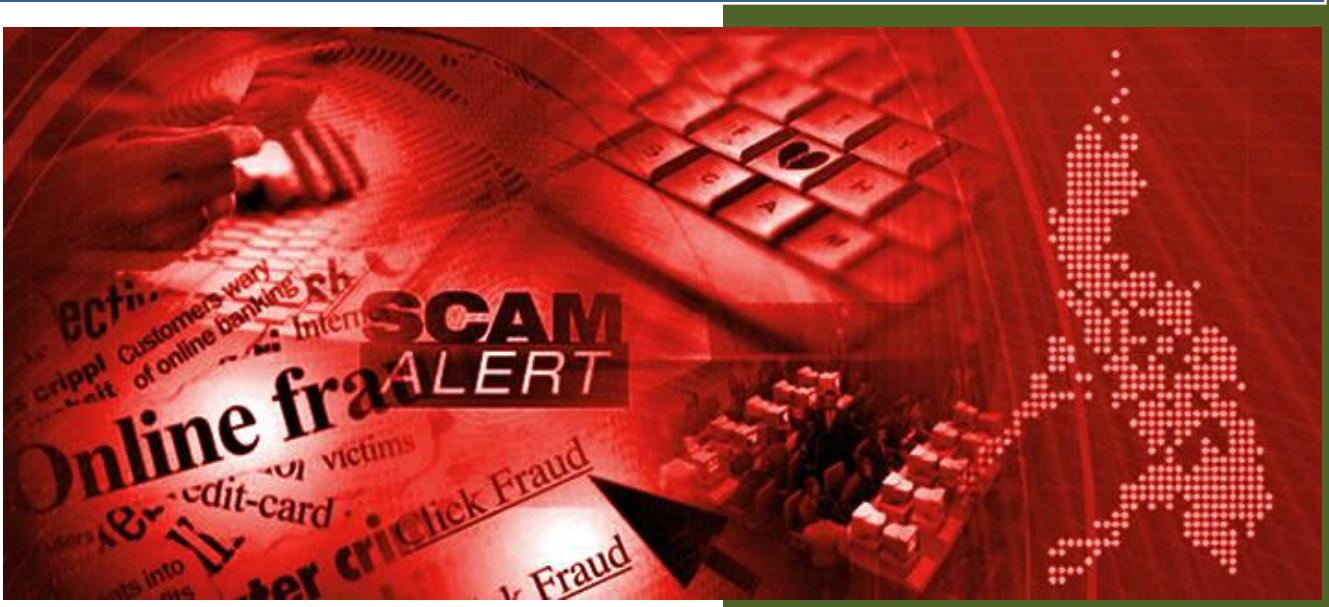
COMMON TYPES OF INTERNET FRAUD SCAMS



www.acg.pnp.gov.ph

COMMON TYPES OF INTERNET FRAUD SCAMS

INTRODUCTION:

The Internet is a useful way to reach a mass audience without spending a lot of time or money. Crime in which the perpetrator develops a scheme using one or more elements of the Internet to deprive a person of property or any interest, estate, or right by a false representation of a matter of fact, whether providing misleading information or by concealment of information.

As increasing numbers of businesses and consumers rely on the Internet and other forms of electronic communication to conduct transactions illegal activity using the very same media is similarly on the rise. Fraudulent schemes conducted via the Internet are generally difficult to trace and prosecute, and they cost individuals and businesses millions of dollars each year. From computer viruses to Web site hacking and Financial Fraud, Internet crime became a larger concern than ever in the 1990s and early 2000s. In one sense, this situation was less a measure of growing pains than of the increasing importance of the Internet in daily life. More users surfing the Web, greater business reliance upon E-Mail, and the tremendous upsurge in electronic commerce have raised financial stakes.

The use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them is currently on the rise. For example by stealing personal information, that can lead to identity theft. A very common form of Internet fraud is the distribution of rogue security software. Internet services can be used to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme. Internet fraud can occur in chat rooms, email, message boards, or on websites.

The Internet offers a global marketplace for consumers and businesses. But crooks also recognize the potentials of cyberspace. The same scams that have been conducted by mail and phone can now be found on the World Wide Web and in email, and new cyber scams are emerging. It's sometimes hard to tell the difference between reputable online sellers and criminals who use the Internet to rob people. You can protect yourself by learning how to recognize the danger signs or warning signs of fraud. If you are a victim or attempted victim of Internet fraud, it's important to report the scam quickly so that law enforcement agencies can shut the fraudulent operations down.

The Philippines continues to face the challenge of effectively addressing the problem of illegal cyber activity and cybercrime victimization, a challenge it shares among developing countries in South East Asia and in other parts of the world. Internet Fraud in the Philippines is currently on the rise, Filipinos and Foreigners alike are not safe on both sides of the fence whether as a suspect or victim. Businesses from micro to multi-nationals are also affected and to put it bluntly everyone will be affected.

TYPES OF INTERNET FRAUD SCAMS

A. BOILER ROOM

In business, the term boiler room refers to an outbound call center selling questionable investments by telephone. It typically refers to a room where salesmen work using unfair, dishonest sales tactics, sometimes selling foreign currency stocks, private placements or committing outright stock fraud. The term carries a negative connotation, and is often used to imply high-pressure sales tactics and, sometimes, poor working conditions.

A boiler room usually has an undisclosed relationship with the company being promoted or undisclosed profit from the sale of the house stock they are promoting. The managers of the boiler room usually have close ties to the same owners of the company whose stock is being promoted. After the sales force of the boiler room sells their clients on the idea of the Initial Public Offering (IPO), they are not allowed to sell the shares that the customer invested. This is because there is no real "market" for the shares, so any shares sold before buyers are attracted would create a large loss in the price of the stock, due to it being thinly traded with no public support. Once the insider investors are in place, a boiler room promotes via telephone calls to brokerage clients or spam email these thinly traded stocks where, there is no actual market.

The brokers of the boiler room actually create a market by attracting buyers, whose demand for the stock drives up the price; this gives the owners of the company enough volume to sell their shares at a profit, a form of pump and dump operation where the original investors profit at the expense of the investors taken in by the boiler room operation.

Protect yourself from Boiler Room

1. If a stockbroker calls out of nowhere with an offer that seems too good to be true, be warned, it probably is.
2. Fraudsters are usually well spoken and knowledgeable. They are also persistent. They might call their victim several times with offers of research, discounts on stocks in small overseas companies, or shares in a firm that is about to float or already at float.
3. Another thing to watch out for is callers are increasingly threatening investors with a police action if refusal ensues.

B. ROMANCE SCAM

Romance scams try to lower your defenses by appealing to your romantic or compassionate side of things. They play on emotional triggers to get you to provide money, gifts and personal details. Scammers target victims by creating fake profiles on legitimate internet dating services. Once in contact with a scammer, they will express strong emotions for you in a relatively short period of time and will suggest you move the relationship away from the website, to phone, email or instant

messaging. Scammers often claim to be working abroad. They will go to great lengths to gain your interest and trust, such as sharing personal information and even sending you gifts. Scammers may take months, to build what seems like the romance of a lifetime and may even pretend to book flights to visit you, but never actually come. Once they have gained your trust they will ask you either indirectly or directly for money, gifts, banking and credit card details. They will pretend to need these for a variety of reasons.

For example, they may claim to be in the depths of despair due to financial hardship or an ill family member. In other cases, the scammer might start off by sending you flowers or other small gifts then will tell you about a large amount of money they need to transfer out of their country or that they want to share with you. They will then ask for your banking details or money to cover administrative fees or taxes to free up the money.

Alternatively scammers may claim to have fallen ill or been involved in a serious accident, then ask for money to pay medical bills or travel expenses to visit. In some instances you may even be contacted by someone claiming to be their doctor. Regardless of how you are scammed, you could end up losing a lot of hard earned money.

Protect yourself from Romance Scam

1. Always consider the possibility that the approach may be a scam. Try to remove the emotion from your decision no matter how caring or persistent they seem.
2. Talk to an independent friend or relative before you send money. Think twice before sending money to someone you have only recently met online or haven't met in person.
3. Never give credit card or online account details to anyone by email.
4. Be very careful about how much personal information you share on social networking sites. Scammers can use your information and pictures to create a fake identity or to target you with a scam.
5. If you agree to meet in person, tell family and friends where you are going especially overseas travel.
6. Where possible, avoid any arrangement with a stranger that asks for immediate payment by money order, wire transfer or international funds transfer. It is rare to recover money that is sent this way.
7. If you think you have provided your account details to a scammer, contact your bank or financial institution immediately.

C. LOTTERY SCAM

An email, letter or text message from a lottery institution arrives from out of nowhere. It will advise you that you have won a lot of money or fantastic prizes—in a lottery or competition that you did not enter. Lottery scams will often use the names of legitimate personnel, so that even if you do some superficial research, the scam will seem real. The email, letter or text message you received about your winnings will ask you to respond quickly or risk missing out a once in a lifetime opportunity. The scammers do this to try and stop you thinking about the surprise too much in

any case you start to suspect to be a scam. You could also be urged to keep your winnings private or confidential, to maintain security and stop other people from getting your prize by mistake. Scammers do this to prevent you from seeking further information or advice from independent sources.

You will usually be asked to pay some fees to release your winnings. Scammers will often say these fees are for insurance costs, government taxes, bank fees, courier charges etc. The scammers make money by continually collecting these fees from you and stalling the payment of your winnings. Some scammers may also be asked to provide personal details to prove that you are the correct winner and to give your bank account details so the prize can be sent to you. Scammers will use these details to try to misuse your identity and steal any money you have in your bank account.

Protect yourself from Lottery Scam

1. Do not send any money or pay any fee to claim a prize or lottery winnings.
2. Do not open suspicious or unsolicited emails.
3. Never reply to a spam email.
4. Never call a telephone number that you see in a spam email.
5. Never respond to text messages which say you had won a competition that you did not enter.
6. Do not click any links in a spam email or open any files attached to them.
7. If it looks too good to be true then be skeptical.
8. If you receive an email, letter or text message telling you that you won a lottery, do not respond. Do not write back and do not send any money or personal details.
9. Providing personal details such as bank account will make you vulnerable to having a stolen identity. You may have your bank account cleaned out or a loan taken in your name. Responding to emails through Internet links might also threaten your computer security through the use of spywares.
10. If the lottery is anything other than a registered lottery just say no, be very wary of lottery that ask you to send money or personal details in there favor.

D. BANKING AND ONLINE ACCOUNT SCAM

d.1 CARD SKIMMING

Card skimming is the illegal copying of information from the magnetic strip of a credit or Automated Teller Machine (ATM) card. The scammers try to steal your details so they can access your accounts. Once scammers have skimmed your card, they can create a fake or cloned card with your details on it. The scammer is then able to run up charges on your account.

Protect yourself from Card Skimming

1. Keep your credit card and ATM cards safe. Do not share your personal identity number (PIN) with anyone. Do not keep any written copy of your PIN with the card.

2. Check your bank account and credit card statements when you get them. If you see a transaction you cannot explain, report it to your bank.
3. Choose passwords that would be difficult to guess.
4. If you are using an ATM, take the time to check that there is nothing suspicious or extra ordinary about the machine.
5. .Ask yourself if you trust the person who you are handing your card over to. If a shop personnel looks like they are going to take your card out of your sight, ask if it is really necessary.
6. If an ATM looks suspicious, do not use it and alert the ATM owner.
7. If you are in a shop and the personnel wants to swipe your card out of your sight, or in a second machine, you should ask for your card back right away.

d.2 PHISHING

The word phishing comes from the analogy that scammers are using email lures to fish for passwords and financial data from the sea of Internet users. Phishing, also called brand spoofing is the creation of email messages and Web pages that are replicas of existing and legitimate sites. These Web sites and emails are used to trick users into submitting personal, financial, or password data. These emails often ask for information such as credit card numbers, bank account information, social insurance numbers, and passwords that will be used to commit fraud.

The goal of criminals using brand spoofing is to lead consumers to believe that a request for information is coming from a legitimate company, but in reality it is a malicious attempt to collect customer information for the purpose of committing fraud.

Protect yourself from Phishing

1. Protect your computer with anti-virus software, spyware filters, email filters and firewall programs.
2. You can verify a website's authenticity by looking for "https:" at the beginning of the internet address.
3. Contact the bank immediately and report your suspicions.
4. Do not reply to any email that requests your personal information.
5. Look for misspelled words.

d.3 EMAIL SPOOFING

Email spoofing is the creation of email messages with a forged sender address something which is simple to do because the core protocols do no authentication. Spam and phishing emails typically use such spoofing to mislead the recipient about the origin of the message. The word spoof means falsified. A spoofed email is when the sender purposely alters parts of the email to masquerade as though it was authored by someone else.

Commonly, the sender's name, address and body of the message are formatted to appear from a legitimate source, as though the email came from a bank or a newspaper or legitimate institution on the Web. Sometimes, the scammer will

make the email appear to come from a private citizen somewhere. Dishonest users will alter different sections of an email so as to disguise the sender as being someone else.

Protect yourself from Email Spoofing

1. Consider what personal information you post on social networking sites. Scammers use publicly available information to identify potential victims.
2. Check if a website has a digital certificate.
3. Install and regularly update antivirus, antispyware and firewall software.
4. Never click on links provided in emails or open attachments from strangers. An email with an attachment that arrives unexpectedly could contain malware.
5. Never provide your personal, business, credit card or account details online unless you have verified the website authentication.
6. Ensure your postal mail is delivered to a secured mailbox.
7. Shred all business documents before you dispose of them.

E. NIGERIAN SCAMS

Background

The Nigerian 419 scam is a form of advance fee fraud or money transfer request similar to the Spanish Prisoner scam dating back to the late 19th century. In that con, businessmen were contacted by an individual allegedly trying to smuggle someone connected to a wealthy family out of prison in Spain. In exchange for assistance, the scammer promised to share money with the victim in exchange for a small amount of money to bribe prison guards. One variant of the scam may date back to the 18th or 19th centuries, as a very similar letter, entitled, "The Letter from Jerusalem" is seen in the memoirs of Eugène François Vidocq, a former French criminal and private investigator. Another variant of the scam, dating back to circa 1830, appears very similar to what is passed via email today: "'Sir, you will doubtlessly be astonished to be receiving a letter from a person unknown to you, who is about to ask a favor from you ... and goes on to talk of a casket containing 16,000 francs in gold and the diamonds of a late marchioness."

The modern 419 scam became popular during the 1980s during the corrupt "Second Republic" governed by President Shehu Shagari. There are many variants of the letters sent. One of these, sent via postal mail, was addressed to a woman's husband and inquired about his health and a long, unexpected silence. It then asked what to do with profits from a $24.6 million investment, and ended with a telephone number. Other official looking letters were sent from a writer who said that he was a director of the state owned Nigerian National Petroleum Corporation. He said that he wanted to transfer $20 million to the recipient's bank account money that was budgeted but was never spent. In exchange for transferring the funds out of Nigeria, the recipient would get to keep 30% of the total amount. To start the process, the scammer asked for a few sheets of the company's letterhead, bank account numbers, and other personal information. Yet other variants have involved mention of a Nigerian Prince or other member of a royal family seeking to transfer large sums of money out of the country. The spread of e-mail and email harvesting software significantly lowered the cost of sending scam letters by using the Internet. While

Nigeria is most often the nation referred to in these scams, they may originate in other nations as well. For example, in 2006, 61% of Internet criminals were traced to locations in the United States, while 16% were traced to the United Kingdom and 6% to locations in Nigeria. Other nations known to have a high incidence of advance fee fraud include Côte d'Ivoire, Togo, South Africa, the Netherlands and Spain.

e.1 NIGERIAN 419 SCAMS

Nigeria may have been singled out is because of the comical, almost ludicrous nature of the promise of West African riches from a Nigerian Prince. According to Cormac Herley, a researcher for Microsoft, by sending an email that repels all but the most gullible, the scammer gets the most promising marks to select. Nevertheless, Nigeria has earned a reputation as being at the center of email scammers, and the number, "419", refers to the article of the Nigerian Criminal Code (part of Chapter 38: "Obtaining property by Cheating") dealing with fraud. In Nigeria, young men would use computers in internet cafes to send mass emails promising potential victims for riches or romance, and to trawl for replies. They refer to their targets as *maghas* scammer slang that developed from a Yoruba word meaning "fool". Many also have accomplices in the United States and abroad that move in to finish the deal once the initial contact has been made.

The scheme begins once a consumer receives a letter concerning the request for urgent business transaction usually the transfer of millions of dollars, being sent out to consumers via mail, email and fax. These letters are commonly referred to as *Nigerian Letter Scams or West African Fraud Letters*. For instance, the writers of these letters will commonly claim to be a Doctor or a corporate entity with a major corporation of Nigeria. There will also be some mention of government involvement. Typically, after receiving a letter a consumer would respond either by phone, fax, or email. The response would be a request for further information on the requirements and procedure for the transaction. Once contact is established, the writer of the letter will normally ask for an upfront processing fee and in some cases arrange for a meeting to discuss the transfer of funds. Most letters come with a breakdown of the percentage of money each party involved will receive once the transaction is final. For instance, many letters received offer the following breakdown, 30% for the account holder, 60% for me and my partners and 10% to be used in offsetting taxes and all local & foreign expenses.

While the scam is not limited to Nigeria, the nation has become associated with this fraud and it has earned a reputation for being a center of email scam crimes. In the Philippines, the Department of Foreign Affairs (DFA) warns Overseas Filipino Workers (OFWs) to watch for the scam from Nigerian syndicates sending emails to unsuspecting victims about employment, monetary gains or other too good to be true offers.

Protect yourself from Nigerian 419 Scam

1. Remember there are no get rich quick schemes the only people who make money are the scammers.
2. Do not let anyone pressure you into making decisions about money or investments.

3. Do not open suspicious or unsolicited emails.
4. Never reply to a spam email.
5. Never send your personal, credit card or online account details through email.

e.2 CHECK OVERPAYMENT SCAM

If you are selling something over the internet or through the classifieds, you may be targeted by a check overpayment scam. You might receive an offer from a potential buyer often quite generous and accept it. The scammer then sends you a check, but the check is for more money rather than the agreed price. The scammer will invent an excuse for the overpayment. For example, the scammer might tell you that the extra money is meant to cover the fees. The scammer might just say that it was a mistake they made when they wrote the check.

The scammer will then ask you to refund the excess amount usually through an online banking transfer or wire transfer such as Western Union. The scammer is hoping that you will do this before you discover that their check has bounced. You will have lost the money you paid into their account, and if you have already sent the item you were selling, you will lose this as well. At the very least, the scammer will have wasted your time and prevented you from accepting any legitimate offers.

Protect yourself from Check overpayment Scam

1. Use your common sense.
2. Know who you are dealing with, independently confirm your buyer's name, street address, and telephone number.
3. Never accept a check for more than your selling price
4. Make sure that checks have been cleared by your bank before transferring or wiring any refunds or overpayments back to the sender

e.3 INHERITANCE SCAM

An inheritance scam is when a scammer contacts you out of nowhere to tell you that you've been left, or are entitled to claim, a large inheritance from a distant relative or wealthy benefactor who has died overseas. The scammer will pose as a lawyer, banker or other foreign official and will advise that the deceased left no other beneficiaries. Some scammers will provide a made up name for your supposed relative. Others will use publicly available family history websites and gather the names of genuine deceased relatives to make the scam seem more credibly convincing.

Some inheritance scams do not refer to family members but rather to a wealthy person who has supposedly died without a last will and testament. The scammer may use news articles about a deceased person, for example following a highly publicized disaster, and claim that without an appointed benefactor you are legally able to inherit the funds. They may alternatively claim that you have been chosen as a lucky beneficiary. The size of the supposed inheritance can be very large, sometimes in millions and often quoted in foreign currency. You will be told that your supposed inheritance is difficult to access due to government and bank restrictions or taxes in the country, and that you will need to pay money and provide

personal details to claim it. The stories told by the scammer can be quite elaborate and they will go to greater heights rather than normal to convince you that a fortune awaits. This includes sending you a large number of seemingly legitimate legal documents to sign, such as power of attorney documents. In some cases the recipient is invited overseas to examine documents and the money. The scammer will often organize an elaborate charade, complete with a safe full of money for anyone who takes up the offer.

Protect yourself from Inheritance Scam

1. Beware of tragic deaths and persons looking for your assistance in moving large amounts of money and to fulfill the role of trustee or heir.
2. Legitimate estates and claims do not solicit trustees or heirs in this manner and do not promise to carry out the exercise 'through the back door'.
3. If someone promises you 20% of a fortune for doing little else than provide banking details, it is too good to be true, and it probably is not.

e.4 EMERGENCY OR "GRANDPARENT" SCAM

Emergency Scam or sometimes referred to as the Grandparent Scam has been around for years. In the typical scenario, a grandparent receives a phone call from a con artist claiming to be one of his or her grandchildren. The caller goes on to say that they are in some kind of trouble and need money immediately. Typically they claim being in a car accident, trouble returning from a foreign country or they need money for bail.

Victims don't verify the story until after the money has been sent as the caller specifically asks that they do not want other relatives to know what has happened by asking “Can you please help me? I'm in jail or in the hospital or in some type of financial need. But don't tell Dad. He would kill me if he found out, please send the money ASAP. I'm scared" Wanting to help their grandchild the victim sends money by a money transfer company such as Money Gram or Western Union. Variations on the scam exist such as an old neighbor, a friend of the family etc. but predominantly the emergency scam is directed toward the Grandparents.

Protect yourself from Emergency Scam or Grandparent Scam

1. If you get a call or email from someone else claiming to know you and asking for help, Check and Validate first.
2. Ask some questions that would be hard for an imposter to answer correctly the name of the person’s pet, for example, or the date of their mother’s birthday.
3. Contact the person who they claim to be. If you cannot reach the person, contact someone else, a friend or relative of the person.
4. Don’t send money unless you’re sure it’s the real person you know.

WORD OF CAUTION

Internet fraud is a form of white-collar crime whose growth may be as rapid and diverse as the growth of the Internet itself. It is apparent that the growth of Internet

fraud to date is outpacing our understanding of the problem. With the prevalent spread of internet scamming these days, it constantly gets more difficult to tell which really mean business and which are not. Professional scammers are getting sharper at refining their schemes as fast as their traps are being discovered. Many scams originate overseas or take place over the internet, making them very difficult to track down and prosecute. If you lose money to a scam, it is unlikely that you will be able to recover your loss. There is no one group of people who are more likely to become a victim 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. We've all heard the timeless admonition "If it sounds too good to be true, it probably is"—great advice, but the trick is figuring out when "good" becomes "too good." There's no bright line. Investment fraudsters make their living by making sure the deals they tout appear both good and true. They're masters of persuasion, tailoring their pitches to match the psychological profiles of their targets. They look for your Achilles heel by asking seemingly benign questions about your health, family, political views, hobbies, or prior employers. Fraudsters or con artists are excellent intuitive psychologists. Just like magicians they understand enough about how the mind works to exploit its vulnerabilities. Scams target people of all backgrounds, ages and income levels.

Why good people do bad things? No single academic discipline or methodology is likely to yield all the answers we would seek from this kind of presentation. In all transactions either on or offline, the greatest weapon of a fraudster or con artist is getting your trust and confidence by trickery through deception. For all of us the tools to fight such misgivings will be skepticism and awareness in all levels.

REFERENCES:

1. Tom Zeller Jr (April 26, 2005). "A Common Currency for Online Fraud: Forgers of U.S. Postal Money Orders Grow". New York Times.
2. ^ Mass Marketing Fraud: The U.S Department of Justice
3. ^ http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-agreement-strengthen-consumer
4. ^ http://www.urbandictionary.com/define.php?term=catfish
5. ^ http://www.irs.gov/pub/irs-pdf/p526.pdf
6. ^ Jamie Doward (2008-03-09). "How boom in rogue ticket websites fleeces Britons". *The Observer* (London). Retrieved 9 March 2008.
7. ^ "USOC and IOC file lawsuit against fraudulent ticket seller". *Sports City*. Retrieved 1 August 2008.
8. ^ Jacquelin Magnay (4 August 2008). "Ticket swindle leaves trail of losers". *The Sydney Morning Herald*.
9. ^ Kelly Burke (6 August 2008). "British fraud ran Beijing ticket scam". *The Sydney Morning Herald*.
10. ^ [a] [b] [c] "Internet Fraud". Federal Bureau of Investigation.

11. http://scamwatch.gov.au
12. www.antifraudcentre-centreantifraude.ca/english/home.html
13. beforeyouinvest.ca/2010/11/new-website-canadian-anti-fraud-centre/
14. www.actionfraud.police.uk/report_fraud
15. www.fbi.gov › Scams & Safety › Common Fraud Schemes
16. www.usa.gov › Citizens
17. www.afp.gov.au › Policing › Cybercrime
18. businessweek.com
19. www.fraud.org/learn/internet-fraud
20. www.scamwarners.com/
21. www.pcworld.com/article/119941/article.html
22. www.onguardonline.gov/topics/avoid-scams
23. www.fraud.org/
24. legal-dictionary.thefreedictionary.com/fraud
25. www.consumerfraudreporting.org

For more information, visit the

PNP ACG websites:

www.acg.pnp.gov.ph

CONTACT US:

PNP ACG Cyber Operations Center

Contact Numbers:

Hotline: (02) 414-1550

Fax: (02) 414-2199

Email: pnp.anticybercrimegroup@gmail.com