Fraud Prevention from the Internet

Best Practices for General User

In 2012, fraud on the Internet cost 30.8 billion yuan Chinese consumers and 63 million online customers were victims of fraud[1]. Fraud is the obtainment of an unauthorised benefit by using unethical means. Everyone can become a victim of these kinds of attacks. Online frauds are scams committed through the Internet. This paper will focus on the ways to prevent online scams and the measures to take in case of suspected fraud.

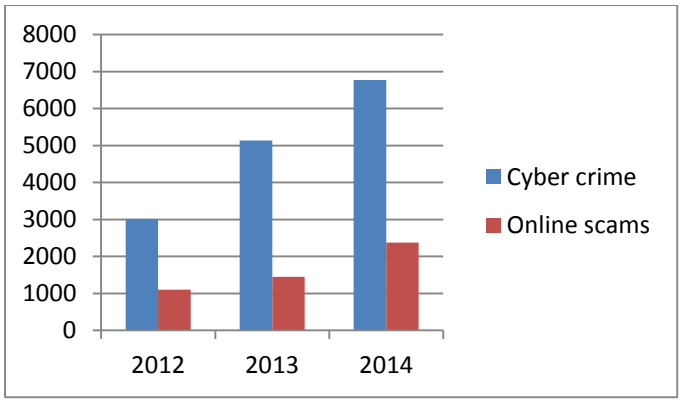

Figure 1 - Evolution of Online scams in Hong Kong[2]

Online Scams

There are different kinds of fraud but they all have the same purpose: to steal as much money as possible from victims. With the Internet, scams don't stop at border anymore and thus online scams become worldwide. A list of the most well-known online scams is presented[3].

- **Con artist fraud**

"Con" means Confidence because the scammer will gain people's confidence to steal even more money. Online, con artists try to steal credit card and bank account number, the most famous fraud belonging to this category is the Nigerian "419" scams. The victim is contacted by e-mail and asked for assistance. The caller declares that he has millions of dollar hidden somewhere but he cannot access them without paying some fees. The victim has to provide money to allow him to pay these costs and in exchange, is assured that he will receive a huge return on investment. Once the money has been sent, the scammer will ask for more until the victim refuses. At the same time, personal information such as copy of passport, social security numbers will be collected. They will also send counterfeit documents to ensure victims of their good faith. The more money is given, the harder it is to stop giving. In fact, the victim thinks that he will eventually get his money back if he gives a little bit more money to the fraud. These e-mails are generally written in upper case letters.

Internet fraud organization of undergraduates in Nigeria[4]

In Nigeria, "yahoo boys" has become a huge community. This nickname refers to undergraduates specialised in cyber criminality and is a nod to their use of yahoo email accounts. Now, students concentrate even more on making money by scams than on their studies. They use electronic mail, instant messaging and chat to carry out fraudulent activities but also voodoo which is supposed to make money come faster. Youths promise fortune to their victims in exchange of a financial support. They collect money from people through disguising and impersonating. Given the severity of corruption in the country, they are able to transfer money across different accounts without difficulties.

- **Identity fraud**

An innocent person can be sued for an act that has been committed in his name. With the Internet, thieves can steal data by using chat room or by com-

promising a computer to collect passwords, usernames and bank account information. Moreover, as a lot of personal information is collected and stored via browsing the Internet, websites have become an easy target of accessing personal information without the owner permission. Phishing e-mail and spam can also lead to stealing of private data. Generally, the victim will be redirected to a fake website which requires update or validation of his personal information. The mail may also state that ignoring the message will lead to devastating consequences or losses. It may take months before the victim realised the scam.

- **Auction fraud**

It is one of the most common online frauds. It can happen over a period of several days but it is always linked to an item purchased. It can be related to issues such as non-delivery, counterfeit good, additional fees… Money transfer is usually done via wire transfer and victim has very little chance of getting his money back.

Sometimes the scammer asks the victim to use a third party service to complete the payment. An illegitimate website will disguise as a legitimate one that conducts the payment. As soon as the transfer is done (that is after the victim sent the goods or the money), the scammer will cut off contact.

In recent days, many offers for one dollar iPhone 6 appear. The associated link will redirect victims to bogus websites, or subscribe users to a premium SMS service that charges them each of the incoming message sent by the scammer.

- **Sweepstakes**

Victims receive an e-mail notifying them that they have won a prize but they have to pay an administrative fee to redeem it. However, they didn't even participate in the online lottery. This "free" prize can end up costing hundreds of dollars. Some lotteries also send invitation to victims offering a "free" try. If they accept once, they will get more and more invites continuously.

- **Online pharmacy fraud**

It is illegal to buy drugs online without prescription. Moreover prescription doesn't prevent victim from falling victim to online pharmacy fraud. The effectiveness of the delivered product is questionable, they may be counterfeit, mislabelled, adulterated, or contaminated. Other crimes committed by online pharmacies include forging of doctor's note or membership fee scam which may even lead to identity theft.

- **Fake diploma**

Degree fraud has become a serious issue. A website in China sold degrees certificates from tens of UK universities and thousands of fake diplomas are in circulation. Bogus websites look like legitimate ones. Some applicants can be scammed of thousands of dollars to get a worthless unrecognised diploma. In Pakistan, the software company Axact has earned millions of dollars by selling fake degrees online; its chief executive is under arrest.

Figure 2 - Fake diploma

- **Dating scams**

Scammers create fake profile on dating sites or social network. They generally present themselves as people in search of their soul mate and try their best to gather victim's information and preference. They will feign affection for their victim within a short period of time (can be in 24 hours). They request the use of another means of communication, for instance instant messaging or phone, instead of the dating website. Once the relationship is established, they will

gain their victim's trust by sending presents or sharing fake personal information, it is then that they ask for financial assistance.

Phone scam[5]

Phone scam is not an online scam but it has become a real threat in Hong Kong over the past few months.

Since the beginning of the year, 200 people have been victims of phone scam. It is 50 times more than last year.

The scammer calls victims as a courier company staff and inform them that a package under their name has been confiscated. Then he transfers the call to an accomplice who pretends to be a mainland Chinese official. The victim has to connect to a fake law enforcement website on which he finds an arrest warrant in his name. Victims can be asked to transfer money or pay cash in person to prove their innocence. Otherwise, victims will be asked to stop all forms of communication and go into hiding. Their family will be contacted and asked for ransoms alleging that the victim has been kidnapped.

80% of the victims are professionals between 20 and 50 and the loss has escalated to HK$27 million. In July, there were on average 5 phone scams per day.

Prevention

Frauds cannot happen without victims' participation, if they refuse to be part of it, the scammer will not be able to do anything. Unfortunately, they can be really persuasive. If it is too good to be true it probably is!

- **Online fraud alert**

Online fraud alerts sent you notification in case of unexpected account activity[6]. This will enable victims to react quickly, such as contacting their bank instantly. The electronic warning can be in the form of e-mail or a text message. People set their parameters to decide in which cases they should be notified. This option is free but additional alerts can be added for a few dollars.

- **Preventive Measures**

Conceal personal information
Personal information should not be given to unknown entities as it may lead to identity theft. To prevent hacking, people should not use the same password for all their accounts. In that case, even if an ill-intentioned person discovers one of the passwords he will not be able to access all sensitive data. (See Newsletter 7 for more information on password management)

Use low credit limit credit card
To reduce the potential loss that may stem from online shopping scam, a low credit limit card is more preferred. In this way, the victim will not suffer from a huge loss from a credit card fraud.

Take time to research before investment
In the face of a promising investment opportunity, preliminary research should be carried out regarding the investment company and the market. An inducement to buy now or within 3 hours is a sign of a scam. If someone presents a proposal of becoming rich quickly it must be a scam. Very few people will take their time only to help others become a millionaire. People should always be sceptical about the motives. Moreover, cash advance loans should be avoided, not to mention loans should not be provided to unmet person.

Verify the recipient identity
Before any money or personal data is transmitted to an entity or a person, the identity of the recipient should be verified. For entity, a quick research on the Internet can provide basic information such as its history and background. In the case of people, Facebook or Twitter profile can be checked. Also, information exchanged in the previous correspondences should be consistent. Somebody who is supposed to live in Florida and claims that he is living in Boston city should be suspected. Inconsistent details are a good way to unmask scammers.

Download only from trusted websites

Malwares can be installed on a computer via free software download and steal personal data. Download should always be done from trusted websites.

Avoid clicking e-mail link

In the case of receiving an e-mail that ask for re-entering of personal data, user should not click the link provided in the e-mail but visit the official website. Similarly, user should not click any link in an e-mail sent by an unknown source. A company will never ask you to give them again personal data such as password, credit card number, and social number. (See Newsletter 9 for more information on phishing scam)


From: Comcast [billing@comcast.net]
To:
Cc:
Subject: Billing update

comcast

Dear Customer,

In a bid to serve you better, we are currently updating our billing systems. Due to this update, we require all Comcast customers to update their billing information on file.

Failure to update your billing information may result in service suspension.

You will be required to provide a valid credit or debit card to complete this process. Please ensure you enter in your card information accurately.

We sincerely regret any inconvenience.

Please click here to proceed

Thank you for choosing Comcast!

Figure 3 - Phishing mail from Comcast

Current Event[7]

A man lost 2,000 USD in an online purchase. The deal was to pay 200 USD for shipping, 1,000 USD when the package was shipped and the rest upon receipt of the good. The seller wanted to use a local delivery company and sent the victim a tracking number and a URL. According to the website, the package quickly arrived London, thus the man sent the following 1,000 USD. The supplier demanded him to pay the balance right away or at least 800 USD more because of an audit issue. The man followed suit. Then he asked for another 600 USD under a new pretext. The man never received its package.

Lesson learnt

Always check an unknown shipper before accepting any goods from it.

In case of delayed delivery excuse and request for additional payment, it is very likely that it is a scam. Thus more money mustn't be sent before the final delivery.

Immediate Actions In Case Of Fraud

In case of fraud, reporting it is crucial. This can prevent the theft from stealing others.

Firstly, all the evidences must be collected and all details should be recorded. For instance, messages of unknown debts, credit card statement of unmade purchase.

Then, authorities have to be contacted. Victims can lodge complaints online via the Hong Kong police force website[8]. The police might ask for related documents mentioned above.

In case of card fraud, the victim might be contacted by a creditor or a merchant about unknown charges. The bank that issued the card should be notified im-

mediately. The speed of reaction is pivotal. All corrupted accounts should be cancelled as well as all new ones opened by the thief[9].

In case of a romance scam, it is important not to take revenge on the scammer or block them. A romance scam peer counsellor delivers one-on-one assistance and guidance to help victims. First-hand experience can be shared online, as databases of scammers are created and building up. Sharing educates people about scam which is the best way to reduce the number of fraud victims. Scammers mustn't know that they are listed in the database, otherwise they will change their identity and be harder to detect.

Conclusion

Online fraud is the most widespread form of cybercrime. Everyone can be victim of fraud one day. The best way to prevent falling prey to online frauds is to avoid them. If it is not possible, it has to be reported instantly.

References

1. "Alipay and Cybersource expand their fraud prevention partnership" 5 December 2013 Web. 23 June 2015
2. "Computer related crime" February 2015 Web. 13 August 2015
3. "How to detect online scam" 21 June 2015 Web. 22 June 2015
4. "Social Organization of Internet Fraud among University Undergraduates in Nigeria"O. Tade & I. Aliyu, University of Ibadan, Nigeria, December 2011, pdf 22 June 2015
5. "Police government telephone deception" August 2015 Web. 13 August 2015
6. "How online fraud alert works" 21 June 2015. Web. 22 June 2015
7. "Five online scams horror stories you need to read" 28 September 2015 Web. 22 June 2015
8. http://www.police.gov.hk/ppp_en/02_er_room/
9. "How con artist works?" 21 June 2015 Web. 22 June 2015

Copyright Statement