DEV SANSKRITI
VISHWAVIDYALAYA

DEV SANSKRITI VISHWAVIDYALAYA

SESSION 2018-21

Assignment 2
Of
E-Commerce

Submitted To:
Dr. Rajeshwari Trivedi
Assistant Professor

Submitted By:
Aniket Kumar
BCA (5th Sem.)

Department of Computer Science,
DSVV, Haridwar

Some common frauds related to E-commerce and cyber security

1. Identity Theft

Jack clicked on the link which took him through to a legitimate looking website. He entered his bank account details and, as he thought, straightened out his account. In fact his problems were just beginning. Unwittingly, he had provided the fraudsters with enough information for them to steal his identity. “A nightmare began” Jack says. The fraudsters had soon withdrawn over £1,000 from Jack’s bank account. Luckily Jack checked his bank statement online regularly and noticed the withdrawal quickly. He notified the bank and soon realised that he had become the victim of a phishing scam.

“The bank was great, very helpful. I had to report the details of the scam and they then refunded the money to me. I had to change the password on my account and they updated my account details. They also advised me that I was at risk of identity theft and that I should report it to one of the main credit agencies such as Experian”.

2. £17 million stolen – biggest UK credit card fraud

In the mid 2000s, a gang of international fraudsters managed to steal the details of over 32,000 credit cards. They used this information to create clone credit cards and scam at least £17million over a period of several years.

The gang members lived a life of luxury on the money: purchasing English mansions, Spanish villas, and a portfolio of other London properties; enjoying first class travel and five-star holidays; and spending a small fortune on designer clothes and shoes.

The scam was masterminded by Russian and eastern European criminals operating out of London with a sophisticated money laundering system, shifting money from the UK to Poland to Estonia, Russia, the United States and the Virgin Islands.

3. The biggest credit card scam ever - $200 million

America likes to do things big, and their credit card scams are no exception. The biggest card fraud to date was committed by a gang of eighteen criminals from New York, who managed to steal $200 million before being stopped. The story wouldn't be out place in a Hollywood movie, with the fraudsters using their ill-gotten gains to live the high life: buying luxury cars; holidays; and millions of dollars worth of gold.

A three-step scam

This scam was more elaborate than the simple card cloning techniques used in the British and Australian frauds. Instead the American fraudsters created thousands of false identities with addresses across the US and in eight countries around the world.

- The card fraudsters created all the information and documents needed to make false profiles with America's major credit agencies.Black market businesses were employed to provide fake credit histories for these false profiles.
- With perfect credit scores for their fake identities they would apply for large loans and credit cards with high limits.
- The money from these cards was spent in a network of sham companies and businesses in on the scam, which laundered the cash.Tens of millions of dollars were wired overseas to Pakistan, India, the United Arab Emirates, Canada, Romania, China and Japan.

The FBI shut the scam down in 2013 and 18 people were jailed on charges of defrauding both banks and the United States. The longest sentence handed down was 30 years.

4. Debit card clone case

One of the victim was Christopher Richards, who have described his case as:
I had an event like that about 5 years ago where the card had never left my hands, other than in a deep pocket in my trousers.
I had drawn some money that morning from an ATM, and later in the afternoon made some purchases.
The following morning, I had a telephone call from the Fraud Department of my bank to tell my that my current account had been suspended following suspicious, inconsistent activity.
The ATM transaction had been recorded and then a few hours later another transaction took place in Holland, and this other transaction that I had done later in the afternoon. Their computing security system has picked up the fact that there was no way I could have been from my home town in the UK, to Holland and then back to London to make this purchase in the time frame that this other withdrawl had been made.
I was refunded the money under the Bank Guarantee Scheme that operates in the UK, but my account was subject to in depth audits and also all entries monitored manually for the following 18 months. The situation never occurred again, and we still don’t know how that card was cloned or where.

5. Phishing

Most phishing scams are found on social networks or delivered via email to multiple users. Those who are unwise enough hand over their personal information, such as account IDs and passwords, can then fall victim to identity theft.

The first known instance of phishing was recorded on January 2, 1996. It was contained within the Windows application known as AOHell, a multifaceted program frequently used for stealing AOL passwords. Today, phishing emails often purport to be from the tech support branch of companies such as Microsoft and Apple.

6. Credit Card Fraud

A real incident told by Kannan Devrajan who saved himself from the credit card fraudsters. He shared his experience with a credit card fraudster who tried to get his credit card details through a telephone call. He talked to him as if he were dumb. Here is how the conversation went.

He: Good morning Sir! I am calling from XYZ bank. You are using our bank's credit card for a while and you have accumulated a huge reward points which you can encash.
Me: Good morning. Thanks. What do you mean by reward points? How did it get accumulated to my card?
He: Sir, whenever you purchase something using your credit card, reward points will be added. Now I called you to help you in encashing the reward points. Your card is Visa card, right?
Me: Sure, please let me know the procedure. Yes, it is Visa.
(I think all Visa cards start with a common digit and he told the first digit to act smart)
He: Please take your credit card and there is a sixteen digit number printed on the front side of the card. Please read those numbers.
Me: But banks always advice me not to share my card details to anyone.
He: Sir, you are right, but it is only for sensitive data live netbanking password, mother's maiden name and date of birth. (Acted smart again)
(I took a pen and paper, and wrote a sixteen digit number. I read the same numbers to him)
He: Sir, there is a expiry date mentioned at the bottom of your card. Can you see?
(I gave him a random month and year)
He: Your card is having your name as "Kannan D", correct?
Me: No, it is not.

He: That could be some system problem. How is your name printed and how you want the name on the card? I will update my database and send you a new card soon.
Me: Ok, it is “D Kannan”.
He: Sir, just turn back your card. You will see a three digit number. Tell me that number.
(I gave him.)
He: Sir, please hold on. I will send you a one time password by SMS. It will help me to encash your reward points.
(He tried to use my credit card details online while I was on hold. But I knew that the details would not work.)
He: Sir, can you tell me your card number again?
(I read what was written on the paper. He believed as the number I had told him before matched with this one)
Me: When will the encashed amount get credited to my account?
He: Sir, the server seems to be slow now. I am checking. Please hold on.
Me: YOU IDIOT. EVEN IF YOU TRY FOR THE WHOLE DAY, THE CARD DETAILS WILL NOT WORK. YOU CAN START BEGGING RATHER THAN STEALING. GET LOST. I GAVE YOUR NUMBER TO CYBER CRIME DEPARTMENT. YOU WILL BE CAUGHT.
I disconnected the call.

7. Nishant Patar as a victim of SBI credit card fraud

The experience of Nishant Patar in his words:

I had applied for SBI Simply Click Credit Card at 22/04/2019 at SBI Credit Card Site.

My application was pre-approved. They had told me that I am qualified for there card. After that they had send me there executive to collect all documents.

SBI Simply Click Credit Card application No : 2211201029532.

In few days they had verified and confirmed all my document and approved my credit card application and told me that they will sent me my credit card.

But 1 week ago, something weird happen, I got message at my phone that I have submit my 2nd new application for SBI BPCL Credit Card. I was shocked that I never applied for 2nd Credit Card at SBI Bank. SBI BPCL Credit Card application No : 2211906004096.

From that day to still today, I am getting call from SBI bank regard of verification and some time even aggressive call regard of this application.

SBI Bank refuse to take my complain at there branch. While none of there customer care number is working for complain. Worst every time I get called from there executive, they will blame me for application.

I am tired of SBI bank and there fraud business tactics on customers like us. This fraud had commited by there main branch employee. Shame on you SBI Bank.

I had sent complaint against them in RBI and Consumercourt.

8. The Nigerian 419

The aforementioned Nigerian prince scam is the most notorious of all phishing scams. It’s made its way into pop culture like no other internet scam, being referenced on TV shows and in the worst kind of internet memes from the mid-2000s that used the Impact font, and which we thought were funny for some reason.

Officially dubbed 'Nigerian 419', this scam traces back all the way to the 19th century, when it was said that a 'Spanish prisoner' needed money. This morphed into a postal scam in the late 1970s and early 1980s, during the nefarious years of the Second Nigerian Republic.

In the late 1990s the now-ubiquitous Nigerian prince started asking email recipients to transfer funds to their bank, in return for which they'd be rewarded with a far greater sum of money at an unspecified date in the future. The exact nature of the scam varies, but the results are consistent: over $1.5 billion has been lost around the world to a scam that we now make a mockery of.

9. Guaranteed loan/credit card

This is a scam that shamelessly preys on poor people, which makes it particularly unpleasant. It takes the form of an email or on-site advert that tells you that you’ve been pre-approved for a credit card or a loan that you haven’t applied for, in an effort to trick you into handing over bank details or other personal information.

Since there’s no way a genuine financial institution would hand you a credit card without taking a look at your credit history, if you get one of these you can safely assume it’s fake news.

10. Phishing Scams in the name of Corona Virus

This is perhaps the biggest scam out there right now because phishing emails can come in many different forms. Most commonly, hackers are pretending to be health officials or national authorities offering advice about staying safe during the Corona outbreak. The reality is that they are trying to trick unsuspecting individuals into downloading harmful malware or providing sensitive, personal information.

Some of these phishing emails look really sophisticated, with one in particular being a fake email sent from the World Health Organisation (WHO), offering tips on how to avoid falling ill with the virus. Once the email user clicks on the link provided, they are redirected to a site that steals their personal information. The problem is, with so many people being genuinely worried about their health and hoping to stop the spread, many don't suspect that these types of emails could be a scam.

The best way to avoid falling victim to these types of phishing emails is to look for suspicious email addresses or lots of spelling mistakes. And even if the email looks pretty legitimate, it might still be worth going direct to the sender's website instead. For example, going direct to the World Health Organisation website for advice means you can avoid clicking any links from the email. That way you can find the information you need and reduce the risk of falling victim to a cybercrime.

Secondly, if an email asks for money or bitcoin donations to help tackle Coronavirus, don't make any transfers. Again, if you wish to help by donating money or services, go directly to the websites of charities or health organisations to see how you can help.

References:

[1]. The 10 most common Cyber Security Scams uncovered – Tech Radar

[2]. What are credit card frauds? - Quora

[3]. Coronavirus Cybersecurity: Scams To Watch Out For – Security Boulevard

[4]. Credit card fraud: the biggest card frauds in history - Uswitch