Unmasking Cyber Shadows

a case study by Sandesh Subedi

Abstract

With the swift enlargement of technology and means, especially in the computational universe, immense convenience and comfort have been experienced by users. However, the process includes not only total relief but also plenty of drawbacks and a term, 'Computer Crime'. In general, computer crime is a deed of invading one's exclusive data for distinctive multiple purposes (i.e., financial loss, reputation harm, unbalancing organizations, terror acts, and many more). Identity theft, identity fraud, and phishing are also computer crimes that have been creating devastating riddles for consumers in this advanced period. These computer crimes are inevitable as knowledgeable handlers create new and diverse methods (from alluring users towards some interesting or tempting advertisements to making them drop at least a tiny bit of information about themselves). These faults can occur in one or two ways, but hackers or crackers have hundreds of possible paths for conducting these activities. With the inclusion of some captivating real-life incidents and advice from victimized people and computer experts, this case exploration assists in defending personal information in every possible way. Furthermore, encouragement to everyone must be given so that vigorous step is taken to minimize these crimes and clients can operate devices safely and eradicate negative thoughts about computers and their applications.

Identity Theft

Identity theft refers to the loss or mishandling of any particular data. It is illustrated as an unauthorized utilization of someone else's exclusive data to impersonate or commend cheating. Identity theft has been a progressively growing problem, not only in some exceptional places but universally. The fabrication of new mechanisms for conducting actions like stealing or any illegal purpose by hackers and crackers has failed to eradicate challenges for consumers. The foremost information that the exploration provides is that being careless, even on very inferior information about any individual or an organization, can guide that respective user to their identity insecurity. Consequently, a client should be pretty intelligent and fully prepared to guard his data from every obstacle at any particular time.

Types and Solutions

There are numerous and diverse types of identity theft. Some of them are:

- Drivers License Identity Theft
- Tax identity theft
- Biometric identity theft

Identity theft has been exhibiting devastating outcomes for billions of users around different corners of the world. Reports from ‘ABC News claim that citizens of the United States squander about 25 billion USD every year and are still in ascending order. Moreover, how enthusiastic is it to know that 1 in every 16 people is a victim of identity theft in the present situation? A new consumer is introduced to this field every 2 seconds, and more than 100 people have already been victimized when we are reading this sentence.

Even very minor information (that is, name, address, date of birth, or medical records) can also be used to mishandle anyone’s identity. A real-life example of a bus boy named Abraham Abdullah can be studied, who used web-enabled mobile phones and virtual voice mail services to access phone calls and messages. The busboy accustomed himself to the statistics of more than 200 celebrities, and it was alleged that he used the basic information of those people from library books and social media. Decisively, he was arrested in 2001 and sanctioned according to the law.

Given the positive behavior that motivates them, a client should positively motivate themselves and get ready to overcome every blunder. What this evaluation counsels is that identity theft is almost inevitable for every person, but there are more or less solutions to deal with it. It is a very clear message from this analysis that no personal information should be shared on any unlicensed sites or pages. Likewise, every operator should use strong and updated passwords and firewalls to keep the documents safe. It is also essential to check and control periodical data regularly.

IDENTITY FRAUD

Introduction

As per the former learning, ‘Identity Theft’ means losing or getting personal or organizational information mishandled. Correspondingly, ‘Identity Fraud’ concerns the misuse of those stolen materials to commit actual evil actions or to accomplish aid or welfare. This illegitimate act has been creating some of the most catastrophic consequences in the computing sector in this contemporary period.

Since this can be deceived by any user, every consumer must be inclined to defend his data and statistics in every possible way. This can be pretty hazardous, as fraudsters can access client documents for law-breaking activities but leave the original location so that the actual owner of the data will be responsible.

Types and Solutions:

In today's modern era, a large amount of identity fraud is being observed. Some of the major issues are:

- Credit or debit card fraud
- Online shopping fraud
- Loan-Stacking Frauds
- Terrorism acts commend

The act of identity fraud has been creating detrimental and negative impressions about computing and its application to operators' intellects. Deceivers or tricksters can employ private information for various distinctive reasons, like creating fake bank and exclusive accounts, applying for passports, selling identities, or misdeeds related to currency or terrorism. Credit card

fraud is one of the most familiar examples of identity fraud, where a fake user will purchase goods unjustifiably or create fake criminal records.

A real-life example of US citizen Jack can be examined to be more clear about this case. Jack was a severe victim of identity fraud, where his bank account was misused to buy a car worth $80,000 and an apartment with all utilities. He encountered thousands of difficulties because of that and got past that case, luckily. Currently, he advises every client to monitor credits and practice on authorized websites.

Furthermore, the case of Dora from Italy seems to be both an appealing and a scary example of identity fraud, where tricksters misapplied her wallet and personal information within it. What happened later was a nightmare when they established illegal business companies and hampered her medical reports. This not only took her about 3 years to prove herself innocent but also made her a patient of mental illness.

Any rational handler should use protection techniques and stay ahead of crackers using multiple distinctive modes. Because identity fraud can occur at any time, a consumer should be aware of unsolicited calls or emails. Moreover, one should be concerned about sharing any of their data only with licensed websites or webpages.

PHISHING

Introduction:

Phishing primarily relates to scams. This is the activity where an attacker steals or tends to steal client data using diverse modes. Hackers or crackers disguise themselves as faithful and ethical beings, especially in online communication. This has been creating indirect impressions among computing operators that it’s unsafe to perform any sort of activity on the internet.

Fraudsters or phishing experts have usually skillfully trained themselves and investigated any particular person's data to fool them in easier or more relevant ways. From the financial loss of any individual to the possibility of getting a virus implanted in an organization's device, phishing can guide anyone to severe loss.

Types and Solutions:

The fake existence of any website and its misbranding are what make phishing attempts successful and deceive people into disclosing their information, such as credit cards, usernames, and licenses. There are several ways in which people have been phishing users. Some of them are:

- Algorithm-based phishing (using algorithms to crack data)
- Email phishing (sending fake emails to fool people)
- Domain spoofing (inventing useless and incorrect domains)

In addition, phishing has been classified into various forms. They are:

- Vishing (Voice+Phishing): Phishing using voice messages or phone calls.
- Smishing (SMS+Phishing): Phishing using text messages or emails.
- Search Engine Phishing: Phishing using bogus webpages
- Spear Phishing: Carefully designed email to target one particular person and victimize the consumer.
- Whaling targets big names in the information chain of any fully grown organization to capture vital information.

An instance an incident at one of the essential universities in Toronto can be taken as an example of phishing. What happened was that fraudsters cracked the data of the professor at that university through an advertisement and got access to his information. But what happened

afterward was more scary, as those crackers sent emails to plenty of students through the professor's email and made them log into fake websites. This victimized them mischievously, as they lost pretty much all of their welfare and, more importantly, their medical and personal data.

Phishing might be a never-ending trouble, especially for online communicators, but every consumer should be aware of the possible damages and hampers on their own. From avoiding replying to unknown emails and phone calls to using third-party software (e.g., SysCloud), a device and one’s stats or data can be kept secure.

Conclusion

Deducing the case and with plenty of exploration on these indispensable topics, demonstrates how crucial and elementary these topics are to anyone new to the computing universe. This duty task granted the theme the opportunity to learn about computing crimes, how these crimes operate, how they affect individuals and organizations daily, and enormous modes to defend consumers' devices and information from diverse unauthorized websites, phone calls, or emails. Nevertheless, the real-life problems and instances studied in the case motivate clients to be super careful and aware of their data and to get rid of obstacles or tensions related to identity theft, identity fraud, phishing, or any other related issues.