 doi:10.20944/preprints202102.0082.v1

REVIEW

Online Identity Theft, Security Issues, and Reputational Damage

Sopna A/P Sinnathamby Sehgar [1,2,*], Zuriati Ahmad Zukarnain [1,*]

[1] Faculty of Computer Science and Information Technology, University Putra Malaysia, Seri Kembangan 43400, Malaysia
[2] Department of Information Security, Faculty of Computer Science and Information Technology, University Putra Malaysia, Seri Kembangan 43400, Malaysia
* Correspondence: gs58191@student.upm.edu.my (S.S.S); zuriati@upm.edu.my (Z.A.Z.)

Abstract: Online identity-based theft is known to be one of the most serious and growing threats to victims, such as individuals and organizations, over the last 10 years due to the enormous economic damage these crimes have caused. The availability of personal information on the Internet has increased the chances of this cyber-crime. Online identity theft crime is the result of a combination of cyber-crimes on the one hand and lack of awareness and training of users on the other hand to protect personal data on the other. Education and awareness, which also contributes to early detection, is the strongest tool for consumers to safeguard themselves from online identity fraud. This paper provides a comprehensive explanation of online identity theft, the various approaches that thieves use to attack individuals and organizations and the types of fraud involved in this cyber-crime. The aim of this research is to evaluate the need for a reformulation of the concept of identity theft in order to be compatible with the evolution of behaviors and fraud.

Keywords: identity theft; cyber-crime; identity fraud; types; techniques

1. Introduction

The growth of the Internet has changed drastically the trend by introducing a new variant called cyberspace identity theft. Cyberspace is a digital and networked work environment that people join while using the Internet. Online users 'surf' cyberspace to exchange information, to interact, to entertain, to buy and sell goods and services, to access and use public and private transport, to share their interests and to make financial transactions across a wide range of industries, both nationally and internationally.

This confidential information is misused for a number of reasons, such as opening a new account, gaining influence over the victim's credit account, gaining government benefits and repealing the law through the use of a false identity. Sadly, identity fraud techniques are concealed from the victim and people typically know when they refuse new loans or credit cards, disproved jobs, or when a debt collector asks for a debt that the victim has not caused. Victims often pay billions of dollars annually to compensate for the consequences of identity fraud and misuse of personal data.

Private information is important and plays a key role in the relationship of many organizations. Developing information technology offers positive advantages for enhancing these relationships, but sadly cyber-crimes are also on the rise. Information as the core of the organization is an important part of the information system, and therefore protection of the information system should be highlighted strongly, because our daily lives are more dependent on computer systems.

Online identity theft is a fast-growing cyber-crime in the world. Proper care must be taken by the organization and the individual to protect their privacy and it is also their duty to take steps to avoid any violation of the data breach. 2020 is the year in which credit card fraud is by far the most common type of online identity theft occurring in 41.8% of all identity theft cases as shown in Figure1.1. [1]

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 February 2021 doi:10.20944/preprints202102.0082.v1

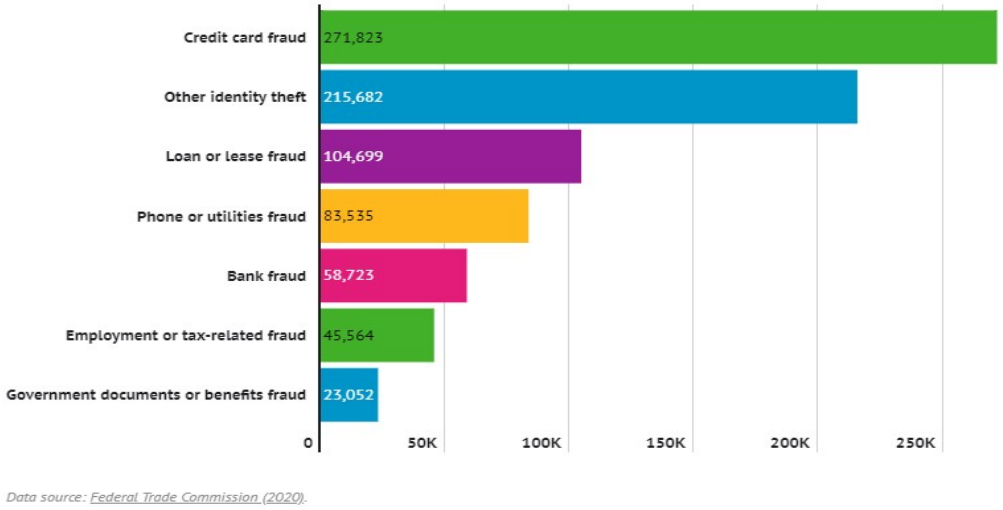

Figure 1.1 Most common types of identity theft in 2020

The **objective** of this research is to acquaint readers with the types of identity theft methods, the various techniques used by fraudsters to attack individuals and organizations, and prevention techniques for individuals and organizations.

2. Identify Theft

Identity theft is the stealing of someone else's personal or financial identity to either gain something like money or to ruin someone's reputation.[2] Some online identity theft schemes include email phishing attempts to lure victims into revealing personal information (e.g., passwords, addresses) and stealing driver's license, credit card, and checking account numbers by hacking into private websites.[3] It also includes unique biometric data (fingerprints, retina scans, facial geometry, iris images, and other unique physical representations), patient identification numbers, and medical records.

The United States recognized identity theft as a crime in 1998, with passage of the Identity Theft and Assumption Deterrence Act (ITADA). Under the ITADA, "identity theft" is defined as the knowing transfer, possession, or usage of any name or number that identifies another person, with the intent of committing or aiding or abetting a crime. The ITADA definition encompasses the three types of identity theft that exist today. At one end of the spectrum, it includes a person's stealing multiple pieces of information about someone and assuming the other's transactional identity, opening ID cards and numerous accounts in the person's name and representing oneself as the other person. This is often referred to as 'new account' theft. At the other end of the spectrum, identity theft includes the more traditional existing-account fraud, where information is stolen about some existing financial account and used to make transactions or access the account's funds. This is known as "existing account" theft. A third type of identity theft is "synthetic" identity theft, which occurs when an identity thief combines stolen information with fictional information to create a new, fake identity. [4]

Other than that, the use of a false identity can be very unintentional, for example, when we fill out the forms with a false name and a date of birth only to be able to subscribe to a discussion site or register to use the application. But user should also 'consider not only the viewpoint of the liar but also the perspective of the deceived. Should the person learn that user has been deceived, user is likely to feel betrayed, resentful, manipulated, suspicious of others who would deal with user in future, and mistrustful of the environment in which the deception occurred.

In a legal context, the use of a false identity can have implications in terms of a violation of the contract that ties the customer to the business, but the most important problems lie elsewhere. If the user does not defend themselves against the anonymity of a pseudonym, but wishes to borrow the identity of a true person, then false identity becomes identity theft.

 doi:10.20944/preprints202102.0082.v1

3. Types of Online Identity Theft

Online identity theft is not a stand-alone crime, it leads to the commission of other crimes. The Identity Theft Resource Centre, which advises government agencies, educates the public and assists consumers as well as victims of identity theft, points out that such theft is not limited to financial crimes. The Centre, which also provides consulting services to legislators, law enforcement agencies and corporations, classifies online identity theft in six categories. Therefore, some researchers define identity theft as a precursor to identity fraud. The following are among the most common types of online identity theft.

3.1 Financial Identity Theft

This includes using information from another person to gain some advantages, such as goods, services and credit, or to access a bank account. It can take one of two forms; the true identity of the name, or the takeover of the account. In the former case, the thief uses the stolen personal details to open a new credit card account that allows him access to the credit card or a check-in account that enables him to receive cheques in the name of the victim. In the above scenario, the attacker has access to the accounts that the victim has already opened by using the stolen personal information of the victim. Worst of all, it can take months or years for victims to rectify the impact of financial identity theft which may result in high debt volumes and low credit scores.

3.2 Medical Identity Theft

In the case of medical identity theft, the fraudster, without the awareness and consent of the victim, uses the name of the victim, sometimes in addition to other pieces of information concerning. For example, insurance, obtaining medical benefits involving products or services, or falsely securing reimbursements for medical goods or services allegedly enjoyed. Action by the fraudster can lead to a manipulation of the victim's medical record with potentially fatal consequences when wrongful medical decisions are taken with respect to the victim. One of the potential consequences of medical fraud is misleading health care providers, which can put the life of a patient at risk. Statistics shows that around 500,000 Americans have been victims of medical fraud.

3.3 Criminal Identity Theft

In this instance, the fraudster falsely claims to be the victim of a crime apprehended by the police. The victim can only know what has happened when called to court to face criminal charges arising out of the offender's action. In such circumstances, victims are often unaware that crimes have been committed on their behalf and that they are likely to be held responsible for any illegal activity committed on their behalf. A victim would only be aware of what happened when he was called to appear before the judge, applied for a renewal of a driving license, stopped by the police for a traffic offence, or found that his license had been suspended or blacklisted. Job opportunities may also be lost because of a fraudulent criminal act.

3.4 Synthetic Identity Theft

This theft is uncommon from other online identity thefts, fraudster combines all the people's details obtained and creates a new identity. A real social security number can be paired with a name and date of birth that are different from the actual owner of the social security number. It is more difficult to trace the crimes committed with the help of this method of identity theft. This is because they are typically not directly represented in the victim's record, such as victims credit report. Instead, they can appear as brand-new reports, or as an auxiliary part of the victim's current credit report. When this identity is used, all victims are affected.

3.5 Tax Identity Theft

Tax return identity theft is the act of filing a return using a stolen identity and taking the victim’s refund. It is the third largest theft of federal funds, after medical and federal unemployment insurance, the fraudster may commit tax fraud resulting in delayed or stolen refunds. Meanwhile, a swiped refund may seem like a worst-case scenario, a fraudster may even use the stolen identity of a person to get an employment, an act of much greater effect. When an identity fraudster uses people’s SSN for employment, all the income they earn under people’s identity must be reported.

 doi:10.20944/preprints202102.0082.v1

In other words, if the victim goes to file their taxes and the earned income numbers don't fit, the IRS would mark the victims back as suspicious. This can have serious financial implications if taxes on unclaimed profits are levied which can lead to prolonged stress with a request to audit the taxes. Victims of fraudulent tax return identity theft can face stressful barriers to recovery from stolen tax returns and identity theft.

3.6 Child Identity Theft

Child identity theft is usually committed by a relative who will take out loans and credit cards in the child's name. As children have no reason to check or monitor their credit reports, they will usually remain unaware of the fraudulent activity until they come of age and require loans. This type of fraud can take years to sort out and could stop you from being able to buy a house or car. It's also likely to increase the interest rates on any loans you might be offered. One research showed that as many as 10.2% of the 40,000 children surveyed were victims of identity theft. As kids, victims of this kind of identity theft can only find out what happens much later in their lives, meaning that the crime can continue for a long period of time.

3.7 Review on Types of Identity Theft

The above review demonstrates the various forms that online identity theft could involve. Two main categories were identified. One is the actual identity theft name. In this case, the thieves steal the personal details of their victims, which is used fraudulently to gain financial, medical and other benefits, by impersonating the victims. The other one is the takeover of identity fraud, which entails hacking over existing accounts belonging to victims. This is generally achieved by intercepting the communications of the victims relating to financial transactions by illegally transferring their addresses to those of the fraudsters.

Some of the major ones include criminal identity theft, financial identity theft, medical identity theft, and synthetic identity theft. The problems relate not only to financial losses, but also to the medical risks to which innocent victims are exposed due to distortions in their medical records. In addition, victims can be prosecuted and convicted for crimes they have not committed or refused jobs and credit facilities until they have cleared their names, usually after lengthy ordeals and expenses.

The study also shows that it is quite a challenge to detect some forms of identity theft, particularly synthetic identity theft. This makes it more difficult for law enforcement agencies to identify a fraud, the consequence of which will, in many situations, be borne by borrowers who have falsely given credit to thieves. Another notable point is that children are equally vulnerable to identity theft. The fact that children's social security numbers do not normally have any details makes fraudster to have a good target for make use of the data.

As a result, children can be faced later in life with criminal records that they know nothing about. Basically, online identify theft is the starting point of many other types of cyber-crimes. Thus, it may involve several stages, perpetrated at different times and places, as well as through different techniques. Correspondingly, the next section of this research paper discusses some of the methods used by online identity theft.

4. Techniques of Identity Theft

Fraudster is using many techniques to commit identity theft. These methods have been categorized into three types in this research paper. The categories listed are:

a) Physical Theft: examples of this are dumpster diving, mail theft, skimming, change of address, reshipping, government records, identity consolidation.

b) Technology-Based: examples of this are phishing, pharming, DNS Cache Poisoning, wardriving, spyware, malware and viruses.

c) Social engineering: examples of this are pre-texting, contests and surveys, obtaining credit reports, bogus employment schemes.

 doi:10.20944/preprints202102.0082.v1

4.1 Hacking

Identity thieves can also hack into computer systems, networks and databases to extract large quantities of personal information. Hackers may sell all the stolen information or directly benefit from private information. For example, in 2009, a computer hacker, Gonzalez, 28, stole more than 135 million credit and debit card numbers in chain stores like 7-Eleven, and obtained $1.6 million in cash (Meek, 2009). Hacking involves the unlawful access to a computer system (Australian Institute of Criminology, 2005) and is among the oldest computer related crimes, which has become a serious and widespread phenomenon. Apart from famous targets like NASA, the United States Air Force, the Pentagon, Yahoo, Google and eBay, (CIPPIC, 2007) offenders increasingly target the computer systems of regular users to obtain identity related information or aim for systems that host large databases for the same purpose.

4.2 Phishing

By using this technique, fraudsters impersonate real organizations and send out false text messages, e-mails (spoofing) or phone calls in the names of such organizations in order to persuade victims to reveal personal details. Users can be threatened with significant consequences if the information is not given by the user. The link will redirect victims to a site that looks just like the official bank or credit card site, but is actually a fictional site designed to persuade victims to reveal their personal details. (Jakobson, 2013) For example, the criminals may set up a fake website in the name of an established travel agency, and deceive unsuspecting victims to reveal their credit card details in order to buy tickets. Based on existing literature, phishing is the most prominent online identity theft strategy that has been shown to be effective in many cases.

4.3 Wardriving

Wardriving consists of physically searching for wireless networks with vulnerabilities from a moving vehicle and mapping the wireless access points. Wardrivers will use hardware and software to find WiFi signals in a particular area. They may intend to only find a single network or every network within an area. Once networks are located, wardrivers will record the locations of vulnerable networks and may submit the information to third-party websites and apps to create digital maps. For example, in 2003, Salecedo the American hacker and his partner were sentenced to nine years in prison because of unauthorized access to Lowe's Companies wireless connection and stealing credit card account numbers (Justice, 2004).

There are three primary reasons wardrivers look for unsecured WiFi. The first is to steal personal and banking information. The second is to use victims' network for criminal activity that victim, as the owner of the network, would be liable for. The final reason is to find the security flaws of a network.

4.4 Fake Employment Schemes

Another identity theft technique is the issuance of fake job advertisements where bogus employers post jobs on their websites and ask job seekers to submit a resume or an application form to obtain personal information. (CIPPIC, 2007) In this way, identity fraudster deceives victims into submitting resumes containing their personal information such as full names, qualifications, phone numbers, email addresses, and account numbers.

4.5 Use of Malware

The most dangerous form of identity theft involves cybercrime, the use of malware such as keystroke logging programs or other forms of spyware. It targets communications between users and their computers with a purpose to obtaining personal information to interfere with Wi-Fi signals. According to the 2012 Verizon Data Breach Investigative Report, malware has led to 69% of data breaches. An example of identity-stealing malware is a malicious block of code called MEDJACK, designed specifically to attack medical devices. Security researchers have found new versions of this malicious code designed to hack hospital equipment such as x-ray machines and MRI scanners. The malware releases a sophisticated zero-day attack that allows cyber criminals to steal patient data from devices, including the PII used by thieves to commit identity theft. The number of malicious smartphone applications used for identity theft is also on the rise. Research has recently seen sophisticated Android apps designed to secretly steal your credit card data and other

 doi:10.20944/preprints202102.0082.v1

confidential information. Victims are unlikely to know about the malware until they hear about the unauthorized use of their identities.

4.6 Preying on Social Networking Sites

Social networking sites have become hot spots for cyber-criminals to commit identity theft. Users may not be aware of how much information they give to identity fraudsters unknowingly through their social networking accounts, such as Facebook, Instagram and other social networking, in order to obtain personal information revealed by users. Seemingly harmless personal information concerning their full names, partners, pets, mother's name, schools they went to or birth dates, provide excellent clues for cybercriminals to figure out their passwords. Even sharing their experiences of using online banking, provides cyber criminals with details about the types of banking users or the types of accounts users have. When all these apparently innocuous pieces of information are put together, cyber criminals may use social engineering techniques or phishing to steal identities. In certain cases, identity fraudsters are pretentiously acquainted with users just to trick them into disclosing their personal details such as bank account numbers, credit card numbers and home addresses.

4.7 Review on Techniques of Identity Theft

It can be seen from the study that various techniques and modes of operation are used by fraudsters to gain access to the personal information of others. These tactics increasingly represent a higher degree of complexity and experience, and criminals have a number of reasons to do so, but above all pursue some financial benefit and hide their wrongdoings. Alternatively, identity theft can be as easy as sifting through the garbage of an organization or the individual to find discarded documents containing sensitive personal details. A major feature of online identity theft strategies is the high degree of anonymity that criminals can afford, making it an immensely common mode of operation and offering very lucrative returns. Identity thieves are continually exploring new techniques and as the conventional method of committing fraud becomes more complicated and less lucrative, it is expected that criminals will turn to new ways of online identity theft. This provides more publicity for individuals and a real obstacle for law enforcement officials and legislators.

5. Prevention Techniques for Individuals and Organizations

Fraudsters use a variety of techniques and approaches to obtain personal information. In essence, on the basis of the situation, fraudsters choose their methods of attacking their targets. For example, identity theft methods for stealing information from organizations are different from individuals.

5.1 Prevention Techniques for Individuals

a) **Limit the information posted on the Internet**

Be stingy in revealing amount of personal information on the Internet such as your full name, birth date, address or credit card number. The same goes for online shopping and the platform needs you to have some details to process your order. Don't provide more details than is needed to process your order, such as a leisure lifestyle or your annual profits. If this information falls into the wrong hands, the identity theft is going to be incredibly simple.

b) Install anti-virus and anti-spyware software and keep them updated with the latest security patches

Viruses and spyware have become so powerful in the hands of cyber criminals that they can hack computer networks and steal data. Having a proper updated version of antivirus and antispyware is not enough; users must also ensure that their device is updated regularly with the new security patches available. Users should link to the respective vendor websites for the most recent security updates.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 February 2021 doi:10.20944/preprints202102.0082.v1

c) Conduct online transactions only at secure websites

Safe Socket Layer (SSL) authentication should be provided for any websites that require users to provide login details, personal identity information or financial information. SSL offers an authentication system, such as digital certificates, which encrypts all transactions between computer users and remote websites to prevent hackers from reading data. Make sure that these websites follow the correct SSL procedures by verifying the correct type of the SSL website address (using 'https://...') and the existence of a closed padlock icon as seen in the picture below.

Picture 1: SSL Websites

d) Implement a strong password and keep it safe

When creating a social networking password or an internet banking, make sure the user uses a good, strong password. One way to build a nice, strong password is to use a phrase with a combination of alphabets, numbers, uppercase letters, lowercase letters and symbols. Get a phrase that the user can remember, and use the first letter of each word as their password, and then convert it to the letters that you can remember. The password should be long enough, for example 8 or more characters.

e) Be careful with what you download or when opening email attachments

Think more carefully before downloading a "free" game or gadget from unknown sources or opening an email attachment from someone you don't recognize. These downloaded or attached files may contain malicious codes to steal your personal information. Do this only when your trusted anti-virus software is running. Always scan downloaded items or files with an updated version of your anti-virus program before installing or running them on your computer. You can also download a powerful online virus and URL scanner from the internet that analyses suspicious files and URLs for viruses, worms, trojans and all sorts of malware that can be detected by the anti-virus software.

5.2 Prevention Techniques for Organizations

Since businesses and organizations have identity and private information in their databases, it is important to have a strategic plan to protect key information. In the first step, in order to provide an efficient and stable system, organizations such as financial or governmental organizations must ensure that their security systems can identify red flags. The security of the websites is more important than ever. Cyber criminals are actively searching for improperly secured websites to attack, although many consumers say that website protection is a top priority when they choose to buy online or access social networking. As a consequence, stable servers and the network infrastructure that supports them are important. The implications of a breach of security are considerable: loss of revenues, damage to reputation, legal liability and loss of consumer trust.

 doi:10.20944/preprints202102.0082.v1

a) Implement appropriate security management practices and controls when maintaining and operating a secure web server.

Appropriate management practices are important for the operation and maintenance of a secure web server. Security practices include the identification of your company's information system assets and the development, documentation and implementation of policies, and guidelines to help ensure the confidentiality, integrity and availability of information system resources.

b) Ensure that only appropriate content is published on organization's website.

Business websites are also one of the first places cyber criminals are looking for useful information. However, many companies do not have a web publishing mechanism or policy that determines what kind of information to publish freely, what information to publish with limited access, and what information should not be published in any publicly available repository. Some generally accepted examples of what should not be published or at least should be carefully examined and reviewed before being published on a public website include:

- Classified or confidential details on the company.
- Sensitive information relating to your business' security.
- Medical records.
- A business' detailed physical and information security safeguards.
- Details about a business' network and information system infrastructure -- for example, address ranges, naming conventions and access numbers.
- Detailed plans, maps, diagrams, aerial photographs and architectural drawings of business buildings, properties or installations.
- Any sensitive information about individuals that might be subject to federal, state or, in some instances, international privacy laws.

c) Secure and encrypt organizations Wi-Fi

Organizations can choose to operate a Wireless Local Area Network (WLAN) for the benefit of customers, guests and visitors. Well then, it is critical that such a WLAN be kept separate from the main company network such that traffic from the public network cannot cross the internal networks of the company at any point in time. Internal, non-public WLAN access should be limited as much as possible to specific devices and specific users while meeting the business needs of the organization. All users should be issued unique credential with the current expiry dates to be used when accessing the internal WLAN.

d) Develop strong password policies in organizations

Oftentimes, two-factor authentication methods, which require two types of evidence that you are who you claim to be, are safer than using just static passwords for authentication. One common example is a personal security token that displays changing passcodes to be used in conjunction with an established password. Consequently, two-factor systems could not always be feasible or realistic for an organization. Password policies should allow employees to use the strongest possible passwords without creating a need or temptation to reuse or write down passwords. This means passwords that are random, complex and long (at least 10 characters), that are changed on a regular basis, and that are carefully guarded by those who know them.

e) Train employees to recognize social engineering

Social engineering, also known as "pretexting," is used by many offenders, both online and offline, to trick innocent people into giving away their personal information and/or installing malicious software on their computers, devices or networks. Social engineering is effective because fraudsters are trying their best to make their work appear respectable and often even beneficial, making it easier to trick users. Several offline social engineering takes place over the telephone, but it also happens online, too. Information obtained from social

networks or shared on websites may be sufficient to establish a compelling trick for employees. Teaching people, the risks involved in sharing personal or company information on the Internet will allow you and your employees to avoid personal and organizational losses. Many criminals use social engineering techniques to get people to voluntarily install malicious computer applications such as fake antivirus, believing they are doing something to help make them safer. The presence of pop-ups with unusual security alerts and asking for credit card or personal details is the most obvious way to detect a fake antivirus infection.

6. Conclusions

As a fast-growing social issue, online identity theft is a major crime that is on the rise across the globe, threatening individuals and organizations so that understanding relevant issues and concentrating on information protection are required to find constructive steps and overcome the problem. Thieves, fraudsters and criminals use a variety of techniques to gain personal information. The variety of techniques used to obtain personal information and the amount of profit reflect the level of motivation, expertise and commitment of fraudsters. Facts indicate that offenders modify their tactics on the basis of their motive; thus, the cost of identity theft to individuals is different from that of organizations. In addition, the advent of emerging technologies and the lack of people's knowledge of how to protect their personal information are motivating fraudsters. Thus, it is important to increase people's awareness of how to protect themselves in online networks through media education. In terms of public education costs, it should be acknowledged that governments and other big businesses should consider costs as investment rather than expenditure to keep a community safe. In addition, companies that obtain personal information from individuals in their databases, such as banks, financial services and retail stores, are more vulnerable than most small businesses or corporations. Hence it is important for these organizations to have efficient strategies, policies and actions to protect them against theft of mass identity. Strong defensive strategies should combine security knowledge, training, technical control and an effective strategy for handling information.

Author Contributions: Authors contributed equally to this work. Present a primer addressing to some of the problems, solutions, and challenges in Online Identity Theft specifically in individuals and organizations. The author focuses on their problem areas, proposed methods, and techniques considered. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding. This research is self-funded by the authors since it is part of the requirement for Research Method subject in University Putra Malaysia for postgraduate students.

Acknowledgments: We thank the anonymous reviewers for their valuable comments and suggestions, which helped us to improve the content, organization, and presentation of this paper.

Conflicts of Interest: The authors declare no conflict of interest

References

1. Stacey L. Schreft, “Risks of Identity Theft: Can the Market Protect the Payment System?”, A review IEEE Access, July 2019.
2. S. Smadi, N. Aslam and L. Zhang, "Detection of online phishing email using dynamic evolving neural network based on reinforcement learning", Decis. Support Syst., vol. 107, pp. 88-102, Mar. 2018.
3. Asif Karim, Sami Azam and Krishnan Kannoorpatti “Efficient Clustering of Emails into Spam and Ham: The Foundational Study of a Comprehensive Unsupervised Framework”, A review IEEE Access, vol. 8, 17 August 2020.
4. Tariq Rahim Soomro “Identity Theft and Social Media”, A review ResearchGate, February 2018.
5. M. E. Elhamahmy and Tarek S. Sobh, “Preventing Information Leakage Caused by War Driving Attacks in Wi-Fi Networks”, IEEE Technology, May 2011.
6. Milne, G. R., Rohm, A. J., & Bahl, S. (2004). “Consumers' protection of online privacy and identity”, Journal of Consumer Affairs, 38, 217–232.
7. LaRoche, P. and Zincir-Heywood, A.N., “Genetic Programming Based Wi-Fi Data Link Layer Attack Detection”, “In Proceedings of the 4th Annual Communication Networks and Services Research Conference (CNSR 2006)”, IEEE Press, May 24–25, 2006, pp. 8–15.
8. "Securing Wi-Fi Wireless Networks with Today’s Technologies". Wi-Fi Alliance. Available at: http://www.wi-fi.org/files/wp_4_Securing%20Wireless%20Networks_2-6-03.pdf [Accessed Dec. 2020].
9. Kumari, L., Debbarma, S. and Shyam R., “Security Problems in Campus Network and Its Solutions”, “International Journal of Advanced Engineering & Application”, Vol. 1, Issue 1, pp. 98-101, Jan, 2017.

10. Alexis, Alexei. 2007. "Data Security Breaches Rampant Among Businesses, Survey Shows," Banking Daily, May 15.
11. Robert Sicilianoii, Matt Cullinaiii, Stew Robertsiv, Terri Beckv, Julie Fergersonvi, Paul Bondvii, Susan Grantviii, Mike Cookix, Eva Velasquezx , and Matthew Donahuexi. "Identity Theft: The Aftermath 2016", Identity Theft Resource Center, 2016.
12. Philippe Jougleux. "Identity theft and internet", A review ResearchGate, January 2014.
13. Watson, C., "Online identity crime – a fresh perspective: part one", F.I. 2011, Feb/Mar, 20–22. Part two: F.I. 2011, Apr/May, 20–23.
14. Elseveir, "Preventing Identity Theft by Protecting Your Data", Information Protection, Pages 31-35, 2014.
15. "Cyber Security Planning Guide". Available at: National Institute of Standards and Technology: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf [Accessed Dec. 2020].
16. Solove, J.D., "Identity theft, privacy, and the architecture of vulnerability", 54 Hastings L.J. 1251 2002–2003.
17. Justinas Rastenis, Simona Ramanauskaitė, Justinas Janulevičius, Antanas Čenys, Asta Slotkienė and Kęstutis Pakrijauskas, "E-mail-Based Phishing Attack Taxonomy", MDPI, Appl. Sci., 10(7), 2363; https://doi.org/10.3390/app10072363. Dec 2020.
18. Krombholz, K.; Hobel, H.; Huber, M.; Weippl, E. Advanced social engineering attacks. J. Inf. Secur. Appl. 2015, 22, 113–122. [Google Scholar]
19. Yeboah-Boateng, E.O.; Amanor, P.M. Phishing, SMiShing & Vishing: An assessment of threats against mobile devices. J. Emerg. Trends Comput. Inf. Sci. 2014, 5, 297–307. [Google Scholar]
20. Cybersecurity Threatscape: Q3 2019. Available online: https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2019-q3/?sphrase_id=70070 (accessed on 26 December 2020).
21. Jagatic TN, Johnson NA, Jakobsson M, Menczer F 2005). Social Phishing. Communications of the ACM, 50 (10) December, pp. 94- 100. Available from: Business Source Complete.
22. Wang, W.J., Y. Yuan, and N. Archer, A contextual framework for combating identity theft. Security & Privacy, IEEE, 2006. 4(2): p. 30-38.
23. Shah, M. and R.I. Okeke. A Framework for Internal Identity Theft Prevention in Retail Industry. 2011. IEEE
24. Geeta, D.V., Online identity theft–an Indian perspective. Journal of Financial Crime, 2011. 18(3): p. 235-246.
25. Allison, S.F.H., A.M. Schuck, and K.M. Lersch, Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. Journal of Criminal Justice, 2017. 33(1):19- 29.
26. Bergholz, A., et al., New filtering approaches for phishing email. Journal of computer security, 2010. 18(1): p. 7-35.
27. Adam, M.E., et al., Awareness of Social Engineering Among IIUM Student. World. 1.
28. Atefeh Tajpour, Suhaimi Ibrahim, Mazdak Zamani, "E-Commerce and Identity Theft Issues", IJACT: International Journal of Advancements in Computing Technology. 2013.
29. Yucheol Cho and Sangjin Lee, "Detection and Response of Identity Theft within a Company Utilizing Location Information", IEEE Xplore, 2016.
30. Collins, J.M., Investigating identity theft: A guide for businesses, law enforcement, and victims. 2006: Wiley.