Alsaidi et al., J Forensic Res 2019, 10:4

Journal of Forensic Research

Review Article Open Access

Cybercrime on Transportation Airline

Abrar Alsaidi[1], **Adnan Gutub**[2*] **and Taghreed Alkhodaidi**[2]

[1]*College of Computer and Information Systems, Umm Al-Qura University, Makkah, Saudi Arabia*

[2]*Department of Computer Engineering, Umm Al-Qura University, Makkah, Saudi Arabia*

***Corresponding author:** Adnan Gutub, Professor, Department of Computer Engineering, Umm Al-Qura University, Makkah, Saudi Arabia, Tel: +966 12 527 0000; E-mail: aagutub@uqu.edu.sa

Received date: October 23, 2019; **Accepted date:** November 12, 2019; **Published date:** November 19, 2019

Abstract

With the development of the internet and increasing internet connectivity, cyber security is the most critical topic surrounding the use of internet technology and online transactions. Users may be exposed to a myriad of security problems when using these platforms. Airline companies can also be vulnerable to criminal activities that may lead to loss of passenger's private information, loss of aircraft or destruction of properties by criminals. It is imperative for security professionals to protect users on a large scale and begin to handle existing vulnerabilities in the aviation industry. This paper focuses on the electronic crimes in the aviation industry, in particular, those that may lead to loss of passenger's information and properties and jeopardize airlines business activities or loss of properties such as destruction of planes.

Keywords: Cybercrime; Phishing; Identity theft, Cyber security, Aviation

Introduction

In this information age, governments and business organizations depend on the use of computer systems to provide and manage a set of services such as transportation, water, energy, billing, and revenue collection among others [1]. This growth in the interconnection of services and service providers has enhanced many operational features that have brought many benefits to the people. This however, has opened up avenues for Internet-related criminal activities, which makes consumers vulnerable to them. Cybercrime involves criminals carrying out malicious activities in the cyberspace such as using malware, phishing, spamming and hacking to steal peoples financial information or steal from them using their credentials [2,3]. The transportation system such as airline booking is also vulnerable to these kinds of attacks and requires an objective approach to realize ways of dealing with such threats.

The modern methods of airplane monitoring and control are also top on the list for cybercriminals because of the extensive use of the network to provide a variety of service. The primary pur- pose of cybercriminals is to acquire vital information about flight patterns, routes, and personal passenger information [4]. Access to this kind of information can lead to an array of adverse vulnerabilities such as terrorism, or high jacking of planes while on the air if a stringent system based protective measures are inexistent [5]. The development of defence against these vulnerabilities is an essential and urgent solution for countering cybercrime. To realize this, we present an overview of the most common vulnerabilities in software, and network, and the simultaneous attacks on technologies such as smartphone technology, including prevention strategy.

Types of cybercrime

Cybercrime falls into two categories:

1. Active: if someone uses a computer to commit a crime without authorization.

2. Passive: when one uses a computer to track data traffic and steal information [2].

Tools for cybercrime

Any application on the internet can be a carrier of worms and other malicious programs. Online criminals use chatting platforms to steal users IDs and pass to their contact partner spyware to help them collect more information. The other critical tool is email, which is the fastest and easiest tool to carry viruses that are capable of damaging user data and devices in minutes. Internet downloads such as music, videos, and software may carry threats that allow hackers to modify the downloadable components to suit their objectives [6]. It may be malware or spyware that steals user information or company files and secretly sends it to the hacker, or a virus. A virus can destroy documents by erasing files or essential information on the computer.

Literature Review

The literature provides four classes of cybercrime regarding the relation of the computer to the crime. They are:

The computer as the target: Involves stealing mental property, theft of information gained from digital files such as medical information and personal history [7].

The computer as the instrumentality of the crime: Involves fraudulent use of machine cards (ATM), credit card fraud, financial theft from accounts, and fraud of telecommunications.

Computer is incidental to other crimes: Bookmaking, money laundering, organized crime books.

Crime associated with the prevalence of computers: Forgery, hacking, selling programs in a black market computer, and technological theft. Cyber-trespass: is passing of cyber limit into other computer systems in an extent to causing damage such as hacking and

virus distribution, Cyber-deceptions, Cyber to break of laws and decency, and Cyber-violence [8].

Comparison of cybercrime in transportation

One of the most important services offered via the internet and which may be vulnerable to cybercrime involves the provision of services related to transportation. In all systems of transport, the top peril is the security threat on confidential information. The aviation sector is vulnerable to cyber threats, not only to physical threats, particularly with the use of Bring Your Device (BYOD) in airports, but also manipulation of aircraft security system that may make them subject to danger [9]. Cybercrime demands high skills and knowledge that is better than the level of skills by the average user. Aviation organizations should understand the purpose of crime to take adequate measures to tackle cybercrime. Among of the motives include:

Ticket fraud: Can take place in airport or online by employees of an airline who assists customers. Customers may be vulnerable to attacks on the network when they buy tickets online or in offices. Criminals may be able to dupe customers through fake websites where they still their information or tickets and leave the customers disappointed [9].

Phishing: Is attempting to trick traveler into discovering their private data, their credit card numbers, and details of a bank account by masquerading as airlines or creating trick pages of bank account to obtain sensitive information [8]. A trustworthy airline may verify the process by email, update, validate, or confirm their data, which is most commonly lately because it is quite easy to implement. Hackers do not need direct communication with victims or their phones but only pretend as technical support staff. Usually, there are three steps for attacks; these are orderly:

- Creating a similar website.
- Sending emails with fake sites to fool the users.
- Getting information needed then return users to site.

In the first step, the hacker steals the identity of an organization and generates a similar website. This possible by copying all HTML lines and graphics from that parent website which makes it is tough for users to note the differences [8]. The hacker can then steal user information through the login forms.

Spam: The spam mail is another form of cybercrime. Email messages are distributed regarding products or airlines services that may be fictitious, and the traveler may be vulnerable to financial fraud [3]. More than 53% of email traffic was spam in 2015, despite a gradual drop over recent years according to a Symantec Intelligence Report. Spammers still seek to evolve their tactics and reach many through social engineering attacks.

Hacking: Hacking is one of the most dangerous forms of cybercrime done on a large scale and has an intense focus on community security. Piracy is the unauthorized access to devices and systems. Attacks in the area of transport such as unauthorized access to the airline system may result in disruption or destruction of passenger databases, or access to financial information of the company or passengers. There are two main categories of this type of attack; human-based deception and technology-based deception [4]. On technology-based deception, the user believes a computer when interacting with a real computer system, which may obtain user data by informing the user that an application has a problem to obtain confidential information from the user [8]. Human-based deception, on the other hand, works by taking advantage of the ignorance of the victim.

Card fraud: When a user logs in to an airlines website to book a flight, he/she may encounter one of the previous methods of fraud to steal his credit card numbers.

Identity theft: Is obtaining sensitive information without the knowledge of the customers. Criminals may obtain these from the company's database or by fraudulent methods. In 2012, the UK Fraud Prevention Service protected 150,000 victims of identity theft crimes [10]. Today, Access to and monitoring of electronic and security systems are now growing at a high rate. E-mail and the Internet are the most common forms of communication.

The problem to be solved

This paper addresses the aspect of cybercrime with a specific concern on air transport. There are several benefits brought about by the internet, though it opens up avenues where criminals use it to commit fraud especially in crimes associated with online transactions. Cybercrime and privacy violations have made business incur losses due to fraud committed by cybercriminals. Online net- work platforms accessible using electronic devices like cell phones, tablets, and laptops have allowed access to a vast number of users, some of who are potential hackers [5]. Specifically, wireless routers that are common in airline transport predispose these prospects to vulnerability as hackers can decrypt their security firewalls and thus access stored data in the databases of these companies and their customers using the platform. There is also the threat of losing aircraft and passengers as many airline companies are considering buying the modern aircraft that are believed to have inbuilt, secure systems can be easily modified through changing the IP addresses, login details, and domain names [9].

The requirement that passengers should avail all their information including Identification Documents (IDs) using Bring Your Device (BYOD) is a risky course. The personal ID is a safety standard requirement for identification and trans- actions in various sectors of the economy including processing of bank accounts and credit cards. Hacker's main motive revolves around monetary gain, where they try to have personal access ID through hacking the airline database, resulting in the traveller losing their credit card money.

Hajj and Omrah

The seasons of religion in the Kingdom of Saudi Arabia is one of the most important seasons in which millions of traveller from home and abroad perform Hajj or Umrah. People use various means of transport such as land, sea, or air. The use of aviation service is the largest because of the delegations of Muslims from abroad that arrive at a high rate, forcing them to intensify the number of airlines and the multiplicity of means of booking electronically by the traveller or through the offices responsible for the bookings. As long as the process is carried out through the Internet, completely either by the customers or by the company providing the service, the customers may be vulnerable to cybercrimes.

The Ministry of Hajj and Omrah adopted a preventive role to protect the rights of services provided to pilgrims by mandatory contracts be- tween the offices of pilgrims and companies and transport services. It provides to pilgrims a reliable airline. They also receive the complaints on their unifying phone and are available to all when exposed to any electronic crimes. Ministry of Hajj and Omrah

are linked to the Ministry of Transport, the General Authority of Civil Aviation (GACA) and other government institutions that provide safe services for pilgrims and help them [11]. The airlines are required to provide passenger information properly, or the company may face sanctions.

Solution to cybercrime

Secure cyberspace requires a joint effort from all stakeholders, including governments, technology companies, and individuals in the society. All the countries of the world have established institutions that are responsible for protecting against cybercrime and combating it and raising awareness to the members of society about the extent of their dangerous and fraudulent methods developed continuously by criminals. These institutions have websites available to those who want to communicate with them and submit their complaint against any crime they may have and contain forms for all types of crime to be reported by affected users. Communication and information technology commission in Kingdom of Saudi Arabia protects the rights of individuals from exposure to cybercrime and addresses all communications submitted on their websites and available phones [11].

Increasing aircraft security can also be solved using cybercrime attribution. This is the process of matching cybercrimes with a criminal, asking specific questions, and analysing computer language, computer code, and network activity to create scientific evidence, which establishes the basis of the process of attribution**.** Attribution is a complicated process that is difficult and expensive to use but also very important in detect facts of indicators of compromise, interference, or malicious activity. Attribution is a useful method for solving cybercrimes because, unlike the malicious intruders who exploit technical vulnerabilities, attribution exploits human weaknesses prominent computer code features such as modularity [9]. To carry out basic tasks, malicious intruders often reuse software in their operations. The reused software is loaded directly into the victim computer providing a trail for the attribution investigators because the software has their hallmarks and signatures, which can lead straight to the identity of the intruder. As a result, the method proves to be useful and practical since it has been used by leading cyber security companies such as Fire Eye as shown in their report on Digital quartermasters.

Proposed solution

Cybercrime has become a buzzword in the tech sector as the increase in internet penetration has opened up possibilities for criminals to use the platform to commit fewer crimes. The disappearance of the Malaysian passenger plane MH370 goes back to a technical failure that could have resulted from somebody tampering with the computing system. Therefore, the safety of vehicles and their passengers is of utmost importance by preventing cybercrime.

Some intervention methods such as training pilots, provision of knowledge, and experience of a flight crew can help in overcoming these challenges. The flight companies need to create awareness among their workers by teaching them about contemporary criminal activities and how it can affect them. The workers need to have comprehensive prevention measures and incidence reporting techniques to address these problems. Passengers having problems such as the disappearance of cards and tickets should receive help very quickly.

The companies should also leverage the power of technology to curb insecurity. Multiple layers of security should be deployed around the database and servers of the travel companies, and web- site features used to prevent tampering with the websites by criminals. Weak scripts and features should be removed and anonymous tracking feature installed to capture the activities of any hacker trying to attempt breaking into the company's database.

Additionally, flight companies ought to install security features such as spy cameras and voice recorders in the planes which can be activated to relay real-time images from remote locations. In situations such as plane hijacks, disappearance, or accidents, one can easily see the situation inside the plane to be able to determine measures to take. Working in tandem with security forces in providing security backups is imperative in solving the hitches that come with cyber security.

Comparisons of all in brief

There are many forms of cybercrime which are evident in the aviation transportation sector. They can range from phishing, hacking, spamming and ticket fraud, which can allow criminals to access vital information that can jeopardize the activities of the flight crew and the passengers. Identity theft involves a hacker accessing confidential information from the customers by accessing the company's database and stealing customers and employees information. Apart from card theft and spamming, identity theft can be very detrimental to a company.

On the other hand, spamming and phasing can readily grant hackers access to a company's database through employees accounts. Companies need to prepare employees for social engineering attacks, malware, and spyware, which hackers may use to access the system. These attacks are very dangerous and require employees to be knowledgeable in preventing these crimes. Beefing up security on airplane communication system, having backup and recovery options ready and using security devices to monitor unusual activities in planes can help prevent unwanted occurrences.

Conclusion

With the rapid development of the internet and increasing internet connectivity, the connection of the organizations systems to each other in the same network has helped in the management of services including transportation, adding operational features that benefit the communities. However, with these features appeared what is known as cybercrime, which may damage Internet users and make them vulnerable to attacks and theft of information and fraud and tricks of criminals to achieve their malicious goals by taking advantage of loopholes in the systems. This paper summarizes the crimes on the recipients from the transport service.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

References

1. Fok E (2015) Cyber security challenges: Protecting your transportation management center. ITE Journal Washington, DC, USA.
2. Chang JM (2013) New trends in cybersecurity. IEEE IT Professional 15: 2–3.
3. Fok E (2013) An introduction to cybersecurity issues in modern transportation systems. ITE Journal 3: 19.

4. Eddy N (2018) Personal information is top target of cyber-attacks, new CDW research shows. Tech Talk Blog.
5. Price JC, Forrest JS (2013) Practical aviation security: Predicting and preventing future threats. Butterworth-Heinemann, Elsevier, Amsterdam, Netherlands.
6. Akhgar B, Staniforth A, Bosco F (2014) Cybercrime and cyber terrorism investigator's handbook. Syngress, Elsevier, Waltham, USA.
7. Symantec (2016) Internet security threat report (ISTR). Symantec Corporation, California, USA.
8. Jang-Jaccard J, Nepal S (2014) A survey of emerging threats in cybersecurity. J Comput Syst Sci 80: 973–993.
9. Rid T, Buchanan B (2015) Attributing cyber-attacks. J Strateg Stud 38: 4–37.
10. Brunt M (2018) Britain's most wanted fraudsters revealed. Sky News, UK.
11. GACA (2018) Electronic safety reporting system.