2014

Is Your Online Data Really Private?

Nathan Pitchaikani
Parkland College

Nathan Pitchaikani
Lauren O'Connor
English 102: 001
November 17, 2014

Is Your Online Data Really Private?

Introduction

In the present age everyone depends on technology. At least once per day someone uses a machine to help them accomplish their tasks. For example, imagine not using a cell phone for a whole day. These days, machines contain personal information or data about their owner. In most cases this isn't an issue. However, with technology becoming more advanced day by day, there has become a reason to worry. People are able to illegally enter other people's computers and steal information. Leading to the point that being able to protect one's personal data is crucial. Learning how to safeguard one's own information or data is important and it is also crucial to understand how hackers are able to steal data in order to prevent it.

History of Computer Crime

Data privacy has been an issue in computers since they were developed. To understand the history of computer crime better one should understand what hacking is. Hacking is when someone use a computer to get access to unauthorized data in another system. The authors of *Computer Crime, Investigation, and the Law* state that the first ever major computer hack was in 1981 by Ivan Murphy (38). He hacked into AT&T and changed their internal clocks. Since this was the first ever hacking one might think it was a big deal. A person might wonder how someone would be able to figure out how to hack something so important. Someone is able to hack when he or she understands the internal networking of what they want to hack. In Ivan's case, he realized the pivotal role that the system's clock played and exploited that (38). *Computer Crime, Investigation, and the Law* also explains that in 1986 a

17 year-old named Herbert Zinn hacked AT&T again and stole more than 50 computer programs (39). What makes this case interesting is the fact that he admitted to doing it and the court gave him the first ever sentence requiring jail time. He went on to serve a nine month sentence in jail. As written in the book, in 1988, there was another case in which a Cornell University graduate, Robert Morris, used a worm that spread through over 6,000 computers (41). He clogged networks by overloading traffic. This was done because he was able to exploit the security flawlessly in the UNIX operating systems. Throughout the whole event there was as much as $100 million in damages. The law allowed a maximum of five years in prison and $250,000 in fines. However, Morris was only charged with three year probation, 400 hours of community service and a $10,000 fine. The courts still didn't take computer crime very seriously (41).

Then in 1989, cyber espionage began. The authors of *Computer Crime, Investigation, and the Law* state that there was a group of people who hacked into the government and university systems (42). They stole data and software and began selling it to the Soviet government. Imagine what would happen to a person who did that now? Even though espionage might have been a big deal back then, cyber espionage wasn't taken very seriously. What is interesting is that fact that there might have been more cases of cyber espionage, but this was the first case that was publically known. Chuck Easttom and Det. Jeff Taylor state that in the year of 1989, a person by the name Kevin Mitnick was convicted of stealing software from the Digital Equipment Corporation and stealing long-distance codes from MCI communications. Because of this case, hacking was made a federal crime. Kevin Mitnick is a widely known hacker and has been the inspiration for several books and film characters. Currently Mitnick is an author and a security consultant (43). Lots of good hackers who get in trouble with the law end up making a deal with law enforcement to work with the federal government to make data more secure. The 1980's was the start of computer crimes but in the 1990's computer crime started to involve more privacy leaks.

The 1990's was the start of more issues involving computer crime. According to the book *Computer Crime, Investigation, and the Law,* in 1990 the secret service launched "Operation Sundevil" with the purpose of catching hackers. There were 150 secret service agents along with local law enforcement. During this time, that much man power was considered very powerful. 150 men plus local law enforcement also showed communication between departments as well as the fact that "Operation Sundevil" was being taken very seriously. This group had raids in about 15 states and seized a great deal of computer equipment. Despite all of that, it only led to three arrests (44). Following this, many people thought that this operation was a waste of resources. However, it was the first major federal operation. As the years kept passing, more and more cases appeared. With each case, jail time continued to increase. The courts started to take computer crime a bit more seriously. For example, there was a case in 1994 where a 16 year old boy who lived in the United Kingdom broke into Griffith Air Force Base, NASA, and the Korean Atomic Research Institute according to Church Easttom and Det. Jeff Taylor. This case was very special because it involved more than one country. Scotland Yard investigated this crime, found the perpetrator and arrested him. This was the first time there was international cooperation for a computer crime (45). The book *Computer Crime, Investigation, and the Law* states that there was another case with Kevin Mitnick; he was accused of hacking computers. The FBI was not able to put their full effort into the case because of other cases so external people helped. This was the start of external citizens helping in computer crimes (46). What is interesting is the fact that even after being convicted for a previous crime, Kevin Mitnick still committed more crimes. This shows that the punishment was not severe, because Kevin Mitnick committed another crime. There are more cases involving international hacking of Citibank, the start of child pornography, electronic terrorism, phishing, and massive spam. All of these cases are stilling happening right now. They might have started in the 1990's but the federal government still hasn't found a way to stop cases such as phishing and massive spam permanently. The reason for this is because hackers keep changing their ways of committing these

crimes. Currently the variables factors that are changing is the magnitude of the hack and the fact that there is now more organization between groups of hackers.

In the 21st century, even the government started to use computer crime to their benefit as skillfully as criminals. Criminals get help from other cybercrime criminals and develop a system. For example, if a criminal needs to get out of a country fast, he or she would meet with someone who can give him or her new credentials. Spies often deal with such criminal systems when they feel they can't go to the government. Another example is that the US government has reached the point in which if they need to, they can hack into citizen's computers, phones, or tablets. However, in most cases they would need a warrant for this. Hackers keep trying to steal more and more data making personal data very vulnerable. There are so many different cases in which hackers have stolen client data from companies.

Hacking Cases

There have been so many different cases in which companies have been hacked and personal data has been compromised. Some of these companies are: Adobe, Dropbox, iCloud, Yahoo Mail!, and Adobe's Digital Edition. Adobe without even knowing, broadcasted Adobe Digital Edition user's data online. The digital edition is popular with libraries, because it allows people to borrow e-books for a certain time. The customer's data that was put online was specific to what book people were reading and what page the user was currently on. It makes sense for Adobe to keep track of what users are reading and what page they are on, so the user can start back on that page. However, the fact that there was a security flaw, which resulted in putting this information online is the real issue. Programmers at Adobe should have been skilled enough to realize that they made such a serious mistake. Later in November 2014, there was another issue. Although, this issue was much more serious. Paul Ducklin at Naked Security states that Adobe's initial estimate was that information on nearly 3 million user's

accounts were compromised. Nevertheless, that number quickly increased to 38 million (1). According to Paul Ducklin, “a database of adobe user data has turned up online at a website frequently used by cyber criminals” (qtd. in Welch). The fact that this has happened two times raises the main issue of whether or not the general public can trust Adobe with their personal data. After going further into this issue, it turns out that Adobe was using some questionable encryption techniques. Encryption basically converts the data into another language, this language has a key in which each letter is changed. For example, the letter “a” could be “%23”, there would be different codes for each letter. So this way the hacker won’t be able to understand the user’s data unless he or she has the key. Or to be more specific the decryption key. On the positive side, the company was quick to reset passwords for all the users involved. Adobe made a statement saying that “the hacked accounts included mainly invalid Adobe IDs, inactive IDs, Adobe IDs with invalid encryption passwords, and test account data” (Adobe). It will be important to watch Adobe closely and make sure that there isn’t any personal data on an Adobe account. Another serious issue is the situation with Dropbox and iCloud.

Dropbox and iCloud are both known for their online storage for users. Dropbox was hacked in July 2012. Instead of a hacker directing hacking into the company to get user information, it was one employee that was hacked. Because of this employee the hacker was able to send spam to e-mail addresses used for Dropbox accounts. On top of that, some of the Dropbox user’s accounts were hacked after the email spamming. Because of this issue, Dropbox right way implement a two-step authentication so that users accounts would be more secure. A two-step authentication would include entering your username, password, and answering a security question about the account holder. Additionally, Dropbox, has set up a new page letting users view when they were last online so that users can make sure that nobody else accessed their account. Celebrity’s iCloud accounts where hacked and inappropriate photos were stolen. These photos were put online on illegal websites such as torrent websites. This problem quickly escalated as there were underage photos too. Apple was not able to

prevent the data from spreading online. The pictures spread so fast that even crime task forces were not able to stop it. A similar event took place with Expendables 3, it was available online one month before it even debuted in theaters. The film was in proper high definition quality leading to the fact that it must have been someone who was working on the film who leaked it. Due to the movie being available online the movie didn't really do well in theaters. Having a secure email provider is important as personal information is on most peoples accounts.

One might think that the above cases were bad however the issue with Yahoo Mail is much worse. Yahoo was hacked four times in several months. Dropbox was questioning users, but Yahoo Mail is even worse. Many people have switch to Gmail because of this issue. There were reports from United Kingdom that user's accounts were still compromised after Yahoo supposedly fixed the issue. The author Mike Wheatley stated in his article "*Yahoo Mail Hacked Again – Serious Questions Raised About its Ability to Protect Users"* that "the hackers are believed to be in Russia, and that they employ a method that takes advantage of a cross-site scripting (XSS) vulnerability in Yahoo email service" (Wheatley). Another time during the hacking period Yahoo users complained that their accounts were sending spam to their contacts and their passwords were changed. Yahoo security has failed majorly and Yahoo have a long way to go until they get their customer reassurances back.

It is important that users should not provide a lot of personal information. It is better to just memorize important information instead of keeping it online; where it can be hacked. As technology advances hacking will become more advanced. It is important that people understand how Intellectual property laws will protect their data from other people. And how people can appeal to try and get their property back from the accused hackers.

Intellectual Property

Intellectual property is a really important concept to understand as it relates to a user's data rights. Intellectual property can be thought of as the creations that come from the mind, such as inventions, literary, artistic works, and design. Intellectual property is protected by the law for example patents, copyright, and trademarks. This allows people to receive recognition for their work. It is important that people understand that whatever creation/data they make or discover is their right and nobody else can use it without their say so.

Intellectual value is the value of one's intellectual property. Somebodies intellectual value can be zero (market value). For example, an old painting that a mother made for her daughter. It isn't really worth anything but, the daughter finds it valuable as her mother painted it. On the other hand, the data/content can be worth something and in most cases it is worth more than the market value. In relation to data privacy if someone were to steal someone's content/data, they would not be able to sell it or claim that stolen data as theirs. This is because of the intellectual property laws. This is why major companies like Samsung and Apple are constantly fighting about cellphone designs. Both companies feel that certain parts of their phones are being copied by the other company. Which is why there are so many court battle to see who is correct. In the current age or the age of information literally everything is intellectual property. Some of the most popular examples are programs (software), paintings, and pictures. There are many different ways people can go about selling items with intellectual value and not worry about personal account information being compromised.

There are some safeguards that one can use to protect their data when selling items. People can create a system which manages payments, these are called micro-transactions. Mirco-transactions are where users can buy items by making small payments. For example, mirco-transactions happen when a user wants to buy an online game. To make sure that this works a strong security system is needed. People can use a third person system like Cyber-Cash, which mediates the transactions between browsers and web sites. Another system that can be used is the smart card. Smart card have a memory

chip in them that keeps track of a user's account information. The memory chip looks like the golden chip in SIM cards. These methods will prevent hackers from trying to steal your intellectual property online. There are some cases in which Intellectual property becomes a real life issue.

Intellectual property has many real life cases involving big companies. One of the well-known disputes is Napster. The article "Top 5 Intellectual Property Disputes" by Heleigh Bostwick states that in the case involving the Recording Industry Association of America which sued Napster (a file-sharing site). Napster allowed people to share music files, and people could download music for free (Bostwick). The main issue was the fact that Napster did not own the rights to the music that people were uploading, downloading and sharing. This was a big issue because major artists were losing lots of money. That is because nobody would buy the music albums since they could just download it for free from Napster. In the end the Recording Industry Association of America (RIAA) sued Napster and won which caused Napster to stop allowing users to upload music and terminate their servers. Currently Napster works as a "fee-based music download site and pays licensing fees". This case is important for internet users to understand as music artists hard work goes into making songs, and sites like Napster make it harder for artists to do well. Artists would lose a considerable amount of money because their music will be available online for free on Napster. This is also an issue of intellectual property in which someone else has taken ones data in this case music and is freely giving it to other people. Another famous case is Bratz Dolls vs Barbie. An interesting fact is that a person by the name of Carter Bryant was a designer for Bratz dolls but also working as a consultant for Barbie. Thus started a battle for intellectual property that got really intense because the employee was with both companies. As one can probably tell legal issues involving intellectual property has always been a tough topic.

Intellectual property can easily be redistributed once it is on the internet. This is because anyone can access it. Then they can just download the data or copy it. The same thing happens with piracy online. This is the reason why some people do not like to publish their work online. They are

scared that other people will misuse it. An example of a situation in which other people's data gets misused is when teachers share an online textbook with their students. Usually they do not have the permission to do so. This is how policy comes in to play for colleges. Policy is needed to make sure that no intellectual property laws are broken and the university doesn't get into trouble. When it comes to intellectual property there are certain laws that can be used to protect people's data. There is the Copyright Act of 1976 which discusses eligibility for protection and copyright ownership. The copyright act also has a section about direct infringement which states that "any unauthorized invasion of the exclusive rights of the copyright owner, without permission, constitutes infringement" (*Computer Crime, Investigation, and the Law* 94). Another act that protects people's property is the Digital Millennium Copyright Act which implements two different international copyright treaties and limiting liability for online copyright infringement. Legal issues around intellectual property have always been a debatable area. All in all, legislators and courts are trying to balance the interests of authors and information consumers.

Data collection

A big part of people wanting to collect personal data is so they can sell the data. These people include advertisement companies and people who want to sell to advertisement companies. Personal data is worth a lot of money to companies in advertising, especially email addresses. Email users get a lot of spam email because of this. This happens when one make a new account on a website and he or she clicks "I agree to statement". Sometimes hidden in the "terms of use" is a sentence allowing the company or website to send that person emails. However, normally there is a check box, during the account set-up. Most people don't read everything carefully and just click next without even looking what they are agreeing too. Because of this, people normally receive spam email or junk software.

Personal data is also collected when people search on Google. This is because Google keeps a record of what people like. For example, say a user is on amazon and the user is searching Asus Laptops.

Then later when the user goes onto Gmail to check his or her email he or she will see advertisements related to Asus Laptops. It's important to note that this will only happen if the internet user is not using ad block software, and is using Google Chrome as a browser. This is because ad block software will prevent the user from having any ads. The reason why it affects Gmail is because the internet user is using Google Chrome and they both are connected. The same thing would happen if anyone uses Google maps. Except instead of advertisements, Google will give people suggestions of places that they might have searched before. This is because Google has kept a record/memory of places that the user has searched before.

Social networking can be another hub for data collection as well. For example, Facebook keeps a memory of the information on what users like on their profile. Also, when Facebook users play games on Facebook, the company who owns the game has access to the user's information. This is because when the Facebook user starts the game, there is a pop-up box asking for his or her permission to let that game access his or her Facebook account, which most people don't notice. This becomes the main issue because the only way to play the game is to give the game company access to the user's Facebook account. This can be problematic. The only way to solve this problem is to find the game online through another website which does not ask for any personal information. However, this doesn't solve the problem completely because the user will not be able to connect with his or her Facebook friends, since the user isn't on Facebook. There are many other online sources that collect user's personal data through downloading.

Google Play Store is another source for data collection. Whenever someone download an application, the Play Store will ask for access to personal information such as in-app purchases, identity, contacts/calendar, location, Photos/Media/Files, Wi-Fi connection information, Device ID and call information. This is basically all the data on the cell phone. With all this information a virtual profile can be made. On top of that, not only the phone user data is accessed, but other people as well. This is

because in a person's contact list he or she has other peoples contact information. Also, in that user's camera gallery he or she could have taken photos with their friends. With all this data analysts are able to connect all the dots with this information and figure out new information about friends of the user or the user itself. For example, analysts can figure out what makes that person mad and that the person's dad died when they were at a young age. The government has lots of analysts to figure out enemies' actions before they even happen. This is what the Central Intelligence Agency does in relation to terrorism. Imagine everything someone does on a computer is being monitored, that is what a keylogger is capable of.

Another popular way of data collection is keyloggers. A keylogger stores the keys typed in and saves them. For example, let's say there are two people Jack and Molly. Jack lets Molly log into her Facebook account on his laptop, Jack could have a key logging software running in the background. Once Molly types in letters for her username and password. The keylogger records all the letters typed in and takes screenshots. The keylogging software is hidden in the background so Molly doesn't even know that the keylogger was running. Some of the best keyloggers take screen shots and even organize the keys based on time and webpage that the user is on. This makes it easier for the owner of the software to go through the data and find out the password or username of the victim. Some of the most popular keylogging softwares are Spytech SpyAgent Standard Edition, All in One Keylogger, Elite Keylogger, and SoftActivity Keylogger. This software can be very dangerous in the wrong hands. For instance, at a public library someone can install a key logger in the morning and then uninstall in the night. Most libraries auto uninstall programs that aren't selected by the library tech admin. However, the most safe public internet access points don't let users install programs on the computer for this very reason. All in all, it's important that people understand public computers aren't always safe and it is not smart to log into any personal online accounts on such computers.

Pharming is a popular ways for hackers to collect personal data from people. Pharming is when a user is on a site that looks exactly like the original site, however it isn't. For example, an internet user clicks on a link to the Citibank webpage. The webpage the user is taken to looks just like the normal Citibank webpage, except the URL is very different. An example of a URL would be "www.blahblahblah.com/345af/asdfsa/jtdf", note the URL is very random and there is no HTTPS. The HTTPS is used when the webpage is secure. The link was redirect to a fake page because someone hacked the link reference and redirected to their webpage. The whole point of this is too trick people into thinking that they are on Citibank webpage and hope that the users enter their username and password for their Citibank's account. Normally once the user enters their information the web, the page says an error has occurred, which makes it look like there was a mistake on Citibanks side. After this the hackers make it so their webpage goes straight to the authentic Citibank web page. Hackers utilize this method so it can be hard to know when pharming is happening or not. To make it safer for users, people can get an anti-virus software which will detect Pharming.

Phishing like Pharming is another popular way for hackers to get personal information. Phishing happens when users receive an email asking for personal information. The email may sound like someone in distress. The idea of phishing is to make the email will look like it is sent from an official place, like a bank. Unlike Pharming which, redirects the user to another webpage, Phishing directly asks the user to send a reply with user's account information. The person who sent the email makes the email sound like they need the email user to send their account information to verify that they are that account holder, when in fact the hacker is stealing the email user's information. Anti-virus software can spot phishing too. Most email providers like Gmail also have safeguards which will warn the users when there is suspicious mail.

There was a recent case in which a cyber-gang stole 1.6 million of a woman's life savings in Britain (Liebowitz). Luckily the gang was caught by police. However, it didn't make much of a difference

because the suspects spent the money. The woman had no lifesaving left after the incident became stuck in a tough position. This is a good example of how cybercrimes create real victims. I have personally received more than ten phishing emails. Most of them were sent from someone I did not know so I was able to tell right away. However, I did receive an email from someone who was a family friend. The email said that she and her family were stranded in Europe and someone had stolen all their identification and luggage. The email asked if I could send money over to help her out so she could come home. I was young when this event occurred because of this I called friend's family to make sure that they were okay. It turned out that they were perfectly fine. My friend's email had been hacked. Phishing and Pharming are serious hacking attempts and people should be very aware.

Many times the reason data is hacked is because of an employee. For example, a hacker will try and hack into an employee secure account. The purpose of this is to try and get his or her username and password to access the company's server. A server is a place where data is stored for a group of people. Once the hacker has access to the company server, the hacker can access all of the company's client's personal information. This technique is very popular and relativity new. Some hackers are even good enough to make it look like the employee took the client information, and the hacking never occurred. This is why it is important that companies have many safeguards protecting their clients from their end too. Most companies track what their employees are doing when it comes to using the internet. The main reason for this is because the company wants to make sure that the employee is being efficient and not wasting time. However, the other reason is so that the company's security can keep a watch on their employees to make sure that they are not doing anything to compromise the integrity of the company's clients. Companies who have really important data to protect will sometimes even contract hackers to test their safeguards. The hacker tries to intentionally hack into the company, however with no bad intentions. Whatever weak points the hacker detects, he or she reports to the company so that they can be fixed immediately. Sometimes these hackers are previous convicts.

However, this is important because to correctly check if a company is secure the company needs someone who is really good at hacking. Sometimes data is stolen right under a person nose, cookies steal people's information when they are accessing the internet.

There are a few different types of cookies. Some of them are more harmful than others. Cookies normally enter users machine when they are surfing the internet. Some of the major types of cookies are session, persistent, secure, and flash cookies. Session Cookies are not dangerous, in fact they help users. Session cookies keep track of unfinished tasks. For instance, there is a person called Billy and he is on Ebay. Billy adds two items to his cart but accidentally exit out of the page, subsequently Billy opens up his Ebay account and his items are still in his cart. This is because the session cookie is keeping track of that data. Persistent cookies keep track of how long a user visits a website and how that user came to that webpage in which the cookie came from. Secure cookies are used to store encrypted data. Hackers try to steal this cookie so that they can decrypt the cookie and see what data is in it. An example of what data could be in the cookie is a credit card number. Flash cookies are the new way to follow internet user's movement on the internet. This may be hard to believe but their main goal is not to track the internet user. The cookies job is to provide Flash applications different options, so it can save information to the user's local system. This can be very helpful when anyone wants to play online games, because it helps save the gamers progress. However, there are many debates on whether people want a cookie tracking them even if it is helping them with simple things like saving games. Most cookies help users out with simple tasks that people take for granted. Nevertheless, tracking user's information still is ethically wrong just as spyware is too.

Spyware is also something that users should be aware of. Spyware gets data from the machine that it is targeting. Spyware normally involves some software that is on the target computer. This normally happens without the computer owner knowing. This software records all keystrokes like a keylogger. This means that usernames and passwords are stored. Spyware also records web sites visited.

The difference between Spyware and a keylogger is that Spyware transit the information to a particular internet address. This way the hacker doesn't need to come back to the machine and get the information manually like a keylogger. Depending on how experienced the hacker is he or she can make the internet address belong to someone who is totally unaware of the crime. Spyware is very popular for a few reasons. One being that it's very easy for the hacker to obtain because there are many legal spyware software's in the market. An example, is a software to monitor children's web access. Secondly, spyware is very easy to put on the machine. Hackers attach spyware to free games, music, movies, etc. This way when users download a free game the spyware has a door to the computer. As long as the game is downloaded from the internet there is a path for the stolen information to go to the internet address. Hacking into a website gets more complicated as it involves more steps.

There are many different ways of hacking into someone's system. There are two popular methods of hacking a website. The first one is called SQL injection. SQL is an acronym for Structured Query Language. SQL is used in relation with databases. The whole point of SQL injection is for hackers to enter SQL code directly into the web forms like login fields. This way the hacker can change the needed code to change the password and username requirements. For examples, the hacker can set it up so that the username and password need to be equal to each other. This would let normal users (people with the username and password information) in and it would let someone who typed username: 1 and password: 1. This is because 1=1. SQL injection is a very popular method of hacking but can only work when the certain website has a connection to a database. This is because SQL is only used for databases. The second one is called cross-site scripting also known as XSS. This kind of attack is harder to prevent than SQL injections and is becoming more popular day by day. The hacker uses XSS functions (code) by embedding JavaScript into hyperlinks to manipulate a website. This gives the hacker the power to take control of user's session, web ads, and personal information. The worst case situation would be if a hacker gained access to account information by taking over the whole website.

Foot printing is another hacker technique that takes time but is effective. Some people may say Foot printing is very similar to what detectives do. This is because Foot printing is when a hacker cases out a target. What is means by case out a target is that the hacker will look for vulnerabilities in the user's system. For instance, the hacker will see what operating system and router the user is running. Then the hacker will see if there is any flaws between those two systems, if there is the hacker will exploit it. If there are no flaws then the hacker looks for some other means of entry through some other flaw.

There are two popular techniques for find account passwords directly, they are Brute-force and Dictionary Attack. A brute force attack is when the software the hacker is using tries every single permutation of letters, numbers, and symbols in order to crack the password. This method normally takes a lot of time, but normally works out in the end. The other type of attack is called a Dictionary Attack. This attack is normally the fastest way to crack most passwords. What happens is there is a text file that contains commonly used passwords, one by one the software checks if that word is the password. Sometimes the text file is based specifically on what the person likes. This is because most people choose passwords that relate to them in some way so that they can remember it easier. Some of the application used to do this are L0phtCrack and Brutus. Normally windows has a three try password lock out system, meaning that the hacker can try three passwords and then won't be able to try again for a while. To avoid this hackers install Linux on the computer. The hacker then goes on the Linux account and uses the software to find the hashed password file. This hashed password file is a file which contains the password for the windows operating system. This way is preferred as it takes less time and is much easier for hackers.

Securing Data

Learning how to secure one's personal data is very important. There are many different ways people can go about this. Since there are many different ways hackers can get one's personal data,

there will need to be many techniques to protect one's data. For example, if someone want to access the internet securely, they can use TOR, Virtual Private Network (VPN) to help keep their anonymity protected. TOR is used by government agents who are overseas and need a secure connection to base. On the other hand VPN's are used by the general public. Mainly, company employee's use VPN's when they are working from home. The reason for this is because they need to remotely connect to their company's server, and if a VPN was not used then hackers can steal the data as it is being accessed. An example of a public used VPN is Hotspot Shield. Both of these will help someone access or connect to other networks securely. However, it is important that the internet users secures his or her home network first. There are a few basic things that someone can do to make sure that their network is safe. For example, one can make sure that there is a network security key. Also, he or she can encrypt their data, this won't make it harder for a hacker to get access to their data, but it will make it hard for the hacker to see what exactly the data is. Both of the above methods can be done if the one looks at the documentation for their wireless router. Also, both of these tips will not affect how one uses their network, but it will help protect it.

Some people think that when they delete files from their trash bin, it is gone forever. However, this is certainly not the case. There are softwares anyone can use to recover the data that the user deleted from their trash bin. An example of a software is Recova. Because of this, it is important that one does not sell their hard drive to anyone. For example, there are two people Kaila and Joe. Kaila puts all her important files in the recycle bins and then deletes them from the recycle bin. She then decides to sell her hard drive to Joe. Joe after buying her hard drive used a file recover software and recovered all of Kaila's personal information. Joe then decides to sell Kaila's personal information online. To prevent this outcome there are a few ways to make sure that one's hard drive data is not recoverable. People can smash their hard drives with a hammer so that the internal memory or cache gets broken. Another way is to set their hard drive on fire. Both of these ways make the hard drive not reusable. If

one just want to wipe all the data from their hard drive then they can use an open-source software called Darik's Boot and Nuke. After one has downloaded it, he or she just puts it on a pen drive and boot from that. Then he or she just needs to enter in autonuke at the prompt. Another method is to download the Eraser which is for windows, this will remove data in folders or selected files permanently. For Macs there is a data wiping tool built into the system, just go to Finder and select Secure Empty Trash. Theses ways will make sure that nobody can recover data.

There are many different small things people can do to make hackers jobs harder and make one's data more secure. For instance, people should be careful what applications they download from the Google Play Store. This is because most applications before installation ask for access to contacts, social networking accounts, and email. These then give information about not just one person but other people too. To avoid this people should read what the application needs access to before just installing it carelessly. For cell phones people can install an anti-virus application to make sure there are no virus on their phone. Something else people can do to keep their data more secure is to never keep all of their online accounts connected to one email address. If that email address were to get hacked then all the other online accounts connected to that email would be compromised too. Also, people should not use the same password for all of their online accounts. This is because once a hacker figures out one password for an online account, he technically has access to all of the other user's online accounts. If a person still wants to have only one email account they can add a text message validation to their email account. How this works is that the account owners gives his or her number to their email provider and after anyone tries to log in, the email provider will send the account owner a text message with a validation code. Without that validation code nobody will be able to enter email account. This is called a two-step verification and is popularly used. This technique can be used with a person's bank account too. Whenever anyone wants to withdraw money or even access their account in general, the bank will send them a verification code to make sure that it is the owners account and not some hacker. One can

also get bank alerts on their phone when anyone accesses their account, this way if account owner didn't access their account, and they get an alert, they know that someone else was in their account and can call the bank right away. This will prevent any serious damage to a user's bank account. Lastly, having security questions that are hard for someone else to guess is important. Security questions should not be something that someone can just look up to find the answer to. For example, "What is your mother's name?" is not a good security question as people can find that out very easily with access to the internet.

Email address are used by everyone. Everyone also receives spam email. Most email providers are good with spam collection, and cause of this the spam goes straight into the spam folder. It is important to note that some spam comes with attachments. One should never open these attachments especially if the attachment is an .exe file. An .exe file is an executable file, almost all viruses, worms, and malware start as a .exe and once someone runs it, it activates. Most anti-virus software's scan email attachments to make sure that they are safe before the user opens it. If spam somehow does manage to get into a person's inbox, there should be a button or setting which will mark that email as a spam and make sure that any other mails coming from that email will go straight into spam. Email is a good way to communicate with people however, users must be careful.

Conclusion

It is crucial to understand how hackers are able to steal data through phishing, pharming, and other methods in order to protect one's personal data. Understanding how computer crime has progressed during the time period is important as people can get an idea of where computer crime is going to in the future. Likewise, hacking cases and intellectual property provide pertinent information about how to safeguard your data legally. Both data collection and securing data directly describe how

to avoid and protect personal information. Hackers are dangerous but if awareness is spread about how to protect yourself from hackers, then data privacy will no longer be an issue!

Works Cited

Bostwick, Heleign. "Top 5 Intellectual Property Disputes." *Legalzoom.com.* N.p., July 2009. Web. 11 Nov. 2014

Easttom, Chuck, and Jeff Taylor. *Computer Crime, Investigation, and the Law*. Boston, MA: Course Technology, 2011. Print.

Liebowitz, Matt. "Phishing Gang Steals Victim's Life Savings of $1.6M." *Msnbc.com*. Security News Daily, 19 Mar. 2012. Web. 10 Nov. 2014.

Wheatley, Mike. "Yahoo Mail Hacked Again – Serious Questions Raised About Its Ability to Protect Users." *SiliconANGLE,* N.p., n.d. Web 13 Nov. 2014.