

9

Spyware: An Emerging Threat

Brent A. Atchley and Allen R. Lee

Spyware Overview

The year is 2004, and the United States Government has enacted laws to combat the disgusting distribution of child pornography over the Internet. Susan is a single mom of three, living in Plainsville, USA. She enjoys a normal life, and faces many challenges in raising three kids alone. Susan's two oldest kids, twins Bert and Ernie, are in high school. They have asked their Mom to buy a computer for the family so they will have a better chance at a successful high school career in this technological age. Susan has no use for a computer, but she agrees to buy one because she wants Bert and Ernie to do well in school. Susan works two jobs to support her family, so she is rarely at home.

After a few days of surfing on the web, Bert and Ernie have found something of great interest to them, Internet pornography. "This is great," Bert says to Ernie, "we can download all of the porn we want, and no one will ever know." They have been visiting many porn sites lately and have noticed that the speed of the computer has slowed down considerably. The Internet browser homepage seems to be stuck on an unknown web search site and cannot be changed back to the original homepage. Included on the site are many links to pornography websites. What Bert and Ernie don't realize is that huge amounts of spyware have been covertly installed on their computer from all the sites they have been looking at, and the spyware has secretly placed hundreds of child pornography links on their computer. They don't tell Susan for fear of getting punished and losing their computer. She will never find out anyway. After all, she has never even used a computer.

A few months have now passed since the purchase of the computer, when one morning there is a knock at the door. It is the Federal Bureau of Investigations. They are making accusations that

Susan is in possession of child pornography files on her computer, a federal crime. After a short trial, she is convicted and sentenced to five years in prison. Her life has been ruined, her family and reputation destroyed, all while never touching a computer.

This scenario may be a bit far fetched, but the likelihood of something similar happening to an ordinary citizen is increasing at an incredible rate. Today's generations are witness to an ever changing computing landscape, facing many challenges and threats that must be dealt with in a quick and efficient manner. In this dynamic computing landscape, we have been witness to the emergence of a new technology, broadly termed "spyware." Many politicians in Congress have expressed great concern over spyware, demanding that there be appropriate laws in place to combat this emerging threat. But what are all of these people referring to when they use the term "spyware," and why is the issue so important to so many people? This chapter will provide readers with a general overview of what exactly spyware is, as well the implications that it has on technology, privacy, and business ethics. The chapter will then discuss why spyware is a major threat to financial institutions, and what can be done to combat this threat.

Spyware Uses and Considerations

Many definitions of spyware exist, as well as types of applications that are considered to be included in that family. Spyware can be defined as "any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes" ("What is Spyware?" 2004). Webroot Software Company defines it as "a program that monitors users' computer activities without their knowledge" (Greene 2004). Regardless of the definition used, it is a very broad term that must be broken down into specific categories. For the purposes of this chapter, spyware will be placed into four categories: system monitors, key loggers, trojan horses (including automated phishing), and adware.

Many computer users hold the impression that spyware is merely an annoying inconvenience that is used by businesses for advertising purposes, but truth be told, a good portion of it is used for malevolent purposes. Aside from the fact that it has many implications on individual privacy that will be discussed throughout this chapter, spyware "could be used to commit acts of industrial espionage. If Company A, for example, wants to know what ingredients Company B uses in its rival product and where it sources them from, what is to prevent it (Company A) from using spyware to track the behavior of employees in the supplies department of that organization (Company B)" (Corbelli 2004). The scenario described above could easily occur and will become a major concern to companies who extensively use technology in the workplace. Industrial espionage via Spyware would most likely be accomplished through the use of system monitors. This category of spyware is especially dangerous to companies because it does just what the name suggests, monitors a person's computer. A variety of system monitors are in circulation today. They can range from low risk to the "totally insidious type which can record your screen as a slide show and e-mail the recording to someone else" (SpyCop 2004). There have also been reports that a new type of

spyware, termed video spyware, is starting to turn up in some places. This type takes a continuous video stream of your screen, and sends chunks of that video via e-mail to a specified account. Although firm proof of this claim is lacking, the thought of video spyware should make most computer users very concerned. It would mean that someone who invests the time and effort can see virtually everything that a given person does on their machine, essentially taking away that person's privacy altogether.

The next category of spyware, which is similar to system monitors, is key loggers. Like system monitors, these also record actions you do on your computer, but they do this in a very different way. Key loggers capture information by recording a computer user's keystrokes for later viewing (SpyCop 2004). By doing this, a person monitoring a machine can view everything that has been typed on the computer since the key logger was installed. Key loggers can record user account information, to be used to gain access to restricted areas of the network, and to restricted information on that network. This information could potentially be used to hold a company hostage (Corbelli 2004). Many companies sell key logging and system monitoring software, which can be used by businesses who want to monitor the activities of their employees. However, key logging and system monitoring software packages are mainly used for malevolent purposes.

The third main category of spyware is commonly known as trojan horses. The term trojan horse "comes from the Greek story of the Trojan War, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy" ("What is a Trojan Horse?" 2004). Back door trojans often appear as desirable programs, but without the user's knowledge they deploy remote access tools on the user's machine. This allows hackers to gain access to the computer. Trojans can be deployed in a variety of ways, ranging from delivery by e-mail attachment to being bundled with other software packages (Greene 2004). They are often designed to capture a specific payload when run on a computer. This payload can range from a wide variety of things. For back door trojans, the payload is placing remote access tools on a user's computer. For other types, the payload can range from infecting a computer with a virus, placing a key logger on the system, or retrieving sensitive information such as usernames and passwords.

The fourth category, and perhaps the one that most people think of when using the term "spyware," is called adware. Michael Castelluccio describes how adware first surfaced in the technology age:

One of the first places adware showed up was in shareware that wasn't making very much money for its creators. An ad or two and/or access to information valuable to marketing departments became part of the cost of some of these inexpensive programs (Castelluccio 2004, p. 57).

This meant that companies, who were struggling financially, could bundle ads paid for by other companies with their software. Often, this

was an easy way for the company selling ad space to earn profits, and the information that came from the ads would provide the companies paying for the ads with valuable marketing data.

Many companies today offer their software products in two ways. The first is to offer the software as a “pay” version, which usually contains no adware. Many consumers however do not want to pay for this ad free software, so they choose the other version. This is usually the “ad supported” free version. The company can then give away a free version without losing money, because it is bundled with adware. Many consumers are content to give up some of their online privacy to receive this free software, or they do not really understand the implications of “ad supported” software. The main issue with adware is privacy. A user must decide how much their information (such as browsing habits and online buying habits) is worth. If they are willing to give up some amount of privacy for a free program, one that would cost next to nothing for the ad-free version, they probably do not value their online privacy very highly. Besides privacy issues, one of the main drawbacks to having adware installed on your computer is how the ads affect the system performance of your computer.

Pop-ups and pop-unders consume memory without your permission, and some sites actually plant Web bugs when they send information. So you type in an address, your machine downloads the information from the site, you click off the two or three pop-ups, and you think that's the end of it. Underneath, a Web bug sends the IP address, time and date, and type of browser you are using back to the advertiser for future reference. Some will even look over the cookies stored on your machine and send back information about your browsing habits (Castelluccio 2004, p. 57).

Computer users must be aware of these implications, and decide whether their privacy and computer performance are worth compromising in order to save a few dollars on a piece of software. Some adware is more malevolent than other, such as “browser hijackers,” which take control of your Internet browser. This is the type of spyware that was described in the example with Susan, at the beginning of the chapter. Once the browser is infected, it is often very hard to return it back to a normal state of operation.

Adware is viewed as a great asset for many fledgling companies because it provides valuable consumer market research, without much effort from the company seeking that information. Some proponents of adware say that it is beneficial to the consumer, because products and websites can be tailored to each individual consumer, but is this really beneficial to the consumer? Perhaps a more important question can be “is the use of adware an ethical business practice?” We will try to answer this question in the ethical analysis section towards the end of the chapter. There are many ways spyware can be distributed to computer users around the world:

Spyware is delivered via Web mail and e-mail attachments, shared network folders (with little or no security), misconfigured firewalls, instant-messaging, and peer-to-peer applications. A second

delivery method is more sophisticated and relies on social engineering tactics. These are designed to get the computer user to click on a provided link, open an attachment, or install a free program. The newest delivery method requires no interaction by the computer user except normal Web surfing. Dubbed "drive-by downloading," spyware code is delivered to computer users' machines when they visit an infected Web site or view pop-up ads that contain special active content coding (Germain 2004).

These social engineering tactics are also the method used in phishing scams. Phishing is considered spyware by some people's definitions, and it will therefore be discussed further in the subtopic of this chapter, regarding spyware in relation to financial institutions. Regardless of how spyware is delivered now or in the future, it will be important for businesses and consumers to recognize the ramifications of spyware, as well as new ways of fighting this emerging technological threat.

Spyware's Threat to Financial Institutions: Conflict Resolution

Now that it is known what spyware is, why it is used, what types are in existence, and how it is deployed, the chapter will change focus to why spyware is a threat to financial institutions. For the purpose of this paper, financial institutions refer to any company that deals in financial markets on a regular basis. Examples include businesses such as banks, stock brokerage companies, and insurance companies. In today's technological age, it is rare that one of these financial institutions does not use computers as a daily part of their operations. They use computers to carry out business transactions, provide customers with websites to conduct business through, store sensitive customer information, store company secrets, store sensitive company data, and so on. Due to this heavy dependence on computers to run day to day operations, security is of great concern. Financial institutions must ensure that the property they own does not fall into the wrong hands. Most of these financial institutions have found that use of the Internet is becoming a great financial asset to the company. It provides a new channel to reach potential customers. Without utilizing this important tool, most financial institutions will fall behind in the highly competitive market. Given this important asset, the company must ensure that information stored and transactions completed are done in a secure way. If they do not meet this challenge, they will lose customer confidence, and ultimately, the customers themselves. Spyware's ability to damage a company's reputation and credibility, and in turn lower consumer confidence, is the main reason why spyware is one of the largest threats to financial institutions. This section of the chapter explains why spyware threatens the credibility of financial institutions. It also explains how certain types of spyware exploit weaknesses of online banking. Finally, the section looks at what can be done to combat the threatening effects of spyware, to ensure customer confidence.

Spyware poses a threat to financial institutions because banking information is highly sensitive, and must be secured from unauthorized people. It is a bank's lifeline. If bank customer information is

compromised in anyway, it could severely damage the financial well-being of the company. Although there are many laws in place against defrauding an individual, there are very few in place that prevent people from stealing information such as online banking user accounts through the use of spyware. There are two bills which aide in disciplining individuals that install spyware on your computer that are close to being passed in Congress today. These will be discussed later.

As banking online becomes more and more common, financial institutions become more at risk. It hasn't been until recently that banks started getting actively involved in securing themselves from hackers. The cost of deploying strong security measures are often times too high for small banks to bear, so they employ minimal security to keep costs down. Financial institutions are now realizing the importance of electronic security as we move more and more towards a digital age. Moreover, financial institutions have now changed their tune and are willing to bare the costs of staying secure and keeping up with market standards in order to stay competitive in the marketplace.

Spyware affects financial institutions in many different ways. It affects their most important asset, their customers. As mentioned previously, spyware programs can steal customers' information, and that information can be sold to the highest bidder by the individuals who stole it. When a customer's information is stolen, the customer believes that it is the financial institution's fault for not having the security in place to protect their customers' information. The customers then switch banks, claiming that the institution is not willing to make the necessary changes to be a credible institution and to better serve their customers. Credibility is very important to financial institutions. If it is questioned, lost, or compromised, it will be tough for the institution to regain the confidence of customers or gain confidence from new customers. It is very important for customers to trust and believe who they are banking with. When an individual selects a financial institution, credibility and trust are the two most important factors determining which institution the prospective customer will choose.

Companies realize that more and more people use computers each and every day, and those people are learning that banking online is more convenient than banking at a local institution. Regardless of the lack of security, people continue to bank online because of its convenience. Financial institutions realize that people are starting to use online banking solutions more and more. With this realization, these same institutions started to recognize the cost savings of doing online banking. They realized that it is much more cost efficient to offer banking online and maintain online banking than it is to offer a local physical location. In order for their online site to be successful, they still must maintain that certain level of credibility and trustworthiness. But how does an institution accomplish this? More importantly, what types of spyware attacks can damage an institutions credibility?

The first main threat, which continues to grow at an alarming rate, is that of phishing. This form of infiltration is defined as a social engineering attack, where corporate identity is misrepresented in an attempt to trick individuals into disclosing sensitive information that they would not normally give out if they knew the true identity of the

perpetrators (Salmond 2004, p. 3). This poses an obvious threat because the people that commit these acts are disguising themselves as customer support representatives sending out e-mails looking to help an individual that needs assistance in getting their account back in good standing. This is known more commonly as fraud, but in the electronic sense, it's referred to as phishing. Phishing is a type of spam that targets a specific group. In most situations, people do not realize that they are being phished. They only realize it a couple weeks later when they find that a couple hundred dollars has been stolen from their account. The information is compromised and the user is at risk of further losing highly sensitive information that is essential to their existence. The bank then takes a credibility hit as a result.

As you have seen thus far, online banking is a great asset for financial institutions in today's technological age. You have seen how phishing threatens the well being of financial institutions. The other main way that spyware is a major threat to financial institutions is through the deployment of trojan horses. As explained in the chapter overview, trojan horses are often designed to capture a certain payload by sneaking in programs onto a user's computer. In the case of financial institutions, the payload that is generally targeted is sensitive logon information, such as usernames and passwords. This can range from employee user accounts at financial institutions, to banking customers logging onto their online banking account from home. Trojans try to capture this information in a variety of ways. There are three main ones which threaten financial institutions. The scob trojan operates in a very interesting way that makes it hard to be detected by normal security measures. Most companies employ the use of virus and spyware removal software. However, the scob trojan activates before encryption occurs. This cripples the ability of traditional virus and spyware scanners to block it" (Germain 2004). This can be a scary idea, because the security put in place at financial institutions to stop these threats, does not even recognize them. To gain a better idea of this new threat, we turn to Itzy Sabo, Vice President for Product Management at Finjan Software.

Scob is hidden in an active code vehicle and downloads a key logger. It is a multistage, blended attack. Once the malicious code is slipped into a computer in an infected ActiveX control through the browser, it then contacts another Web site to download the spyware executable. So far, the payload is a key logger program. But security experts are worried that the same Scob mechanism can just as easily contain even more dangerous payloads.

This is a major threat to financial institutions, mainly because it targets people who use online banking. It can retrieve their user logon information, and once inside can transfer funds at their leisure, or gain account numbers and other sensitive account information. One way that financial institutions can combat this threat is to require users of their online banking services to use third party Internet browsers, such as FireFox. FireFox prevents all ActiveX controls from running in a webpage thus preventing threats such as the scob trojan. Preventing

Active X controls from running is a great help, because many Trojans exploit this feature of web browsers.

The web money trojan operates in a similar way as scob. The web money trojan usually hides in a compressed state inside a Windows help file. Once the trojan is unpacked, a GIF file is installed on the user's machine through a pop-up ad brought in by the trojan. The pop-up ad is displayed in the web browser. The .gif file then triggers an executable file. The executable file contains instructions telling the computer to wait for a signal to start running a key logging program, also brought in by the trojan. The signal itself comes from the user's web browsing. When a user goes to a financial institution's website containing the infected code, the signal is sent to the user's computer. Once this signal is sent to the user's computer, the website is actually spoofed from here on out. This means that the site looks exactly like the financial institution's website, but it is actually a copy of site, hosted in an entirely different geographic location. This spoofed website is used to prevent detection by the financial institutions server security measures (Germain 2004). Once the user has inputted their account information into the spoofed website, the account information is compromised, and can be used in the same way as the information obtained by the scob trojan.

The third trojan attack is being termed "automated phishing." This attack uses a trojan named tolger. "Unlike phishing attacks, which come in singly as individual e-mails, once the tolger infects a system it sits invisibly in the background, monitors which Web sites are put on the browser, and if it recognizes one as an online banking site it ambushes the user by capturing keystrokes and snapping screen shots. Periodically, that information is packaged and sent to a remote server controlled by the attacker" (TechWeb 2004).

All of these different types of attacks display how financial institutions are among the greatest risk of being damaged financially by spyware attacks. By having customers who are exploited by spyware attacks, the reputation of the company takes a hit, and the company eventually loses business as a result. One thing that financial institutions must do to ensure their credibility is to create widely distributed campaigns aimed at educating their customers on the risks of spyware. Only by making their customers aware of threats associated with online banking can they make people want to protect themselves against the threat.

The Internet and our computers are quite possibly the greatest tool that we use today, but they are also one of the greatest security threats that we face. Even corporate networks are not safe from spyware. Packages known as enterprise spyware solutions are quickly becoming a popular install for corporations across the world. This is one way in which financial institutions can protect themselves against spyware threats. Financial institutions will need to offer spyware protection to their online banking customers in order to stay competitive. As a matter of fact, Citibank, one of the world's largest banks, recently teamed with Boulder, Colorado based Internet security company, Webroot Software. Webroot will supply Citibank's customers with a free security audit that will check many aspects of their customers' security. One aspect that the software will check is to see if the

customer's computer is infected with any kind of computer spies that might compromise either the bank or the customer. This will only help to protect their assets, by protecting the end user from fraud. Recent lawmaking is also helping to cut down on unethical spyware practices. Recent litigation has went through against a New Hampshire based company that takes computers hostage until the user goes to their site, where they can then buy so called 'spyware-removal software' to remove the infections. The company essentially creates business for itself by infecting people's computers with spyware. Laws are being drafted to stop this unethical behavior (CNN 2004). One bill is known as the Software Principles Yielding Better Levels of Consumer Knowledge (SPYBLOCK) Act. It was passed in the House in 2003, and there are other forms of this bill in the Senate as well. Much speculation has been raised about how much legislation will help against spyware. The CANSPAM Act of 2003 is a great example of how software legislation doesn't change much of how the industry operates. Taming something as wild and wooly as the Internet is impossible to do, and taming one aspect of it is near impossible because of the constant merging and changing of technology, and all the uncertainty that lies within. Creating laws helps the government pay the bills, but it will not slow down or stop the people that create these vicious programs. The only way to stop the unethical use of spyware is to either root it from the source or catch it before it infects you. But how should society decide what use of spyware is ethical?

When trying to apply ethics to the issue of spyware, it becomes tough to distinguish what categories of spyware we should be analyzing, and what categories are obviously not ethical at all, and therefore need not be analyzed. For the purpose of this chapter, ethics can be thought of as "what is the right thing to do." Another way to think of this is "do to others what you would like them to do to you." This is a type of care-based thinking. When addressing ethics, there has to be a certain level of responsibility established. This is a simple thought process, but it can go a long way in today's society. This is explained by looking at an analysis of ethics and privacy by the *Journal of Organizational and End User Computing*:

If we were to agree that it is possible to address the ethical problems of security and privacy by extending the concept of responsibility, this would again raise many new questions and require us to collectively agree on the applicable norms, on the problems in question, on institutions of ascription, and on sanctions. Again, this is an area where the individual end user is concerned. If collective responsibility is to be successful, then even a superficial view indicates that this means that it is to be connected with individual responsibility. It will be the responsibility of individuals to participate in the discourses and processes that define suitable collectives as subjects as well as potential sanctions, and mechanisms of attribution. Furthermore, there must be a structure that allows drawing conclusions from individual to collective responsibility and vice versa. All of these are aspects that individuals should keep in mind, as well as where end users can and must play a central role (Stahl 2004, p. 72).

In looking at the categories of spyware that have been defined in this chapter, we can easily conclude that it is unethical to use phishing, key loggers, trojans, and system monitors. This is because they are used for malevolent purposes, and do not achieve a common good for society. The issue of ethics mainly applies to companies using adware. Is it ethical for companies to use adware to collect valuable marketing data? By applying the standards laid out by Stahl, it can be concluded that it is ethical if there are strict guidelines in place, and standard punishments established for the violation of these guidelines. Also, if ethics involves the end user, then it is unethical for the user to complain about being bombarded with spyware, if they do not take the appropriate steps to prevent their computers from being infected. The users must take a proactive approach to protect themselves. They must play a large role in establishing the ethical business use of spyware. Society still has long way to go in establishing these guidelines, but recent litigation will provide a step in the right direction.

It is apparent that there are many matters to be resolved regarding the issue of spyware. There must be strict laws and punishments put into place, to prosecute people who use spyware unethically. First, guidelines for the ethical use of spyware must be established. By accomplishing this, companies and end users can focus on protecting themselves from the malicious spyware threats that exist, and not have to worry about the unethical behavior of companies trying to gain marketing information or push sales. We still have a long way to go.

Works Cited

- Castelluccio, Michael. "Spyware! Who Put That on my Machine?" *Strategic Finance*. 2004: p. 57-58.
- CNN. "U.S. Files First Suit Against Internet 'Spyware.'" CNN. October 8, 2004. <<http://www.cnn.com/2004/LAW/10/08/tech.spyware.reut/index.html>>.
- Corbelli, Martino. "Spyware Poses a Genuine Risk to Corporate Security; Beware of Spies in the Machine." *Computer Weekly*. 2004.
- Greene, Michael. Personal Communication. September 9, 2004.
- Germain, Jack M. "New Era of Deadly Spyware Approaches." *TechNewsWorld*. August 14, 2004. <<http://www.technewsworld.com/story/35748.html>>.
- Salmond, Tom. "Phishing: Guidance, Best Practice, and Lessons Learnt." *Anti-Phishing Working Group*. 2004: p. 1-25.
- SpyCop. "The Different Types of Spyware." *SpyCop*. October 7, 2004. <<http://www.spycop.com/spyware-safety.htm>>.
- Stahl, Bernd Carsten. "Responsibility for Information Assurance and Privacy: A Problem of Individual Ethics?" *Journal of Organizational and End User Computing*. 2004: p. 59-78.
- TechWeb. "Trojan Automates Phishing Scam." *TechWeb*. August 30, 2004. <<http://www.techweb.com/wire/story/TWB20040830S0002>>.
- "What is Spyware?" *Webopedia*. October 7, 2004. <<http://www.webopedia.com/TERM/S/spyware.html>>.
- "What is a Trojan Horse?" *Webopedia*. October 7, 2004. <http://www.webopedia.com/TERM/T/Trojan_horse.html>.