I've Got My Eye On You!

Robert B. Fried, BS, MS

Abstract

The twenty-first century is filled with many new gadgets and technological innovations. At first glance, our society may appear to be rather advanced. However, looks can be deceiving. In reality, we are only at the forefront of what is in store for the near future. With the passing of each day, we may not know it, but our lives are becoming more and more digitized. A fully paperless society is on the horizon. As the digital world ushers itself in it will become important for one to protect his/her identity and privacy from those lurking in the distance.

This paper will focus on an attack known as 'shoulder surfing'. The methods utilized/employed in implementing this form of attack will be discussed. An example of an attack of this sort in action will be presented. Forms of protection and safety from such attacks will also be analyzed. Finally, several conclusions will be drawn regarding Shoulder Surfing.

In Plain View

What truly happens to data that is inputted into a computer system? It is true that the data is computed. However, it is also possible that something or someone else within close proximity to the computer read the information as well. That something or someone else could most likely be a shoulder surfer. Dr. Fred Cohen, a respected leader in computer security and information protection classifies shoulder surfing as an attack that involves "watching over peoples' shoulders as they use information or information systems" [1]. With the advent of many technological innovations that require the inputting of information, shoulder surfing has become a new tool for attackers who want to exploit the vulnerable within their immediate reach.

Who is Going to Be the Next Victim?

Of course there are those individuals who are cold to the coming of a fully digital age; however, a majority of people are welcoming the technology and the advancements it brings. These advancements include such things as the usage of telephone calling cards automatic teller machines (ATMs). In general, a majority of individuals who utilize these types of service or devices do so while in public view.

I've Got Your Digits!

Over the years many individuals have been victims of phone fraud. It is estimated that "phone fraud is a $4 billion-a-year problem". "There are more than 100 million telephone calling cards in circulation and phone companies want you to use them" [2]. Many people find that using a phone card is often more cost effective and convenient when wanting to make long distance calls either at the home or at pay phones. Rates per minute are always dropping which helps to make the

benefits of using a phone card more appealing. However, more people are using them and becoming victims of fraud.

Most people walk innocently up to a payphone and simply intend to make a phone call. One probably is more concerned about making their call then they are about the area or people immediately surrounding them. However, placing that phone call can attract the attention of any one of the hundreds or thousands of people passing by. One of these individuals passing by may just be a shoulder surfer.

According to Detective John Rizitelli of the Metropolitan Transportation Authority (MTA) in New York, many innocent people fall victim to shoulder surfers. In regard to individuals who utilize this form of attack he states "they call themselves shoulder surfers when they get behind a customer and copy the phone number down from a calling card". With knowledge of telephone calling card numbers, shoulder surfers can rack up hundreds or thousands of dollars in calls over a relatively short period of time by either making the calls themselves or selling the number to others. Often times people don't know they have been victimized until they realize that the number of minutes of credit on their callings cards has declined or their monthly statement in the mail the next month shows calls they did not make [2]. "Technically you are responsible for all charges on your long distance service account. Although the phone companies say they usually don't make people pay for fraudulent calls, it all adds up in the end" [2]. Shoulder surfing is regarded as a big problem in New York City. Rizitelli, whose beat includes Grand Central Station says, "more illegal numbers are taken out of Grand Central than any other facility" [2]. However, the problem of shoulder surfing is not confined to New York City's transportation facilities. The truth is that "shoulder surfing happens thousands of times every day all across America – wherever there are pay phones" [2].

Need Access to Your Cash? Well, So Do I!

The issue of shoulder surfing has also caused some concern within the banking industry. Today, most banks offer their clients many ways to complete their transactions. There is always the option of the old fashioned method of actually walking up in person to a bank and dealing with a teller. One can always chose to utilize the telephone and sit through all the options to engage in banking by phone. However, if one needs to make deposits or withdrawals or transfer funds after normal banking hours, the way to do so is through the utilization of an ATM. Most banks provide ATM access cards to their clientele when they open up a checking or savings account. Due to busy schedules and the growing need to have instant access to funds, the ATM has successfully integrated into society. ATMs are now being utilized in places such as malls, fast food restaurants, supermarkets and even at gas station pumps.

No matter where we look ATMs are always in sight. Their usage has become a normal part of our daily lives. Banks have even allowed for their clientele to utilize their ATM cards just as they would a normal credit card. To the clientele this is rather convenient since they know that the funds in their accounts dictate whether they should use either a credit card or their ATM "check card" to make a transaction or

purchase. However, the increased benefits and conveniences of ATM cards have also attracted the attention of others; particular that of shoulder surfers.

Shoulder surfing is a visually aided attack. Therefore, these attackers must utilize either their eyesight or other optical devices to capture the personal identification numbers (PINs) that people key into ATMs or other similar terminals to gain access to their accounts [3]. The attack can be accomplished fairly easily. Many shoulder surfers spy on their intended targets with devices such as binoculars or high-powered cameras that feature advanced focusing and zoom capabilities. Such features allow for shoulder surfers to attack from even a relatively far distance [4]. Most people don't assume that others are watching over their shoulders at the ATM or at a cash register. However, the person next in line at the grocer could be looking over your shoulder or possibly someone is glancing at you from another location focusing on your fingers as you reveal personal information that he/she might find extremely valuable.

What is the value of having someone's PIN if you cannot associate it with the account it is tied up with? That problem is often solved easily as the record of the transaction ends up in a trashcan within close reach of the ATM or point of sale terminal. Many people don't even think twice about throwing this record away. However, if a shoulder surfer is within reach, what these people don't know might hurt them. "By picking up discarded ATM transaction receipts left behind, criminals can match up PINs and account numbers and have all the information they need to manufacture fake plastics and gain access to the consumers' money. Thousands of dollars are at risk daily from 'shoulder surfing'" [3].

Let's Not Forget About Those Computer Users

Have you ever used a computer in the presence of someone else? Unless you've been living alone in a cabin in a secluded area down by the river and miles away from any signs of civilization, most likely you have. What we do at home or in the office at work can be visually monitored by others. At home, maybe it's a parent, spouse, child or sibling who merely glances at the screen as they pass you by as you sit by the computer. Or maybe while at your place of employment your supervisors or even co-workers come into your office or cubicle to engage in conversation while you're diligently working/typing away. These scenarios are all quite typical. With the widespread use and application of computers within society, computer users do not have immunity to an attack staged by a shoulder surfer.

With respect to your home, a family member may be curious to see what information you have stored on the computer. A member of the family may also be nosy and want to know the user names or passwords to websites or accounts you might access via the Internet. In the comfort of your own home you may be less likely to think that one of your family members may be a shoulder surfer; however, it may very well be the case.

Due to a job requiring extensive travel or simply due to a lack of office space, many companies can chose to have an individual perform their work while away on a business trip or at home. Connecting to work

from an off-site location by way of 'remote access' is fairly common these days. All the employee needs to connect up to his/her home office is a computer with a modem, the proper telephone number or website to access the company's system/network, a user name and a password [5]. To an employee, off-site access may be an extremely convenient tool. However, if information about how to access a company's system/network is in plain view on an employee's computer system, this can be extremely dangerous. To a shoulder surfer glancing by, this information can be very valuable if this particular attacker wanted to gain access to information about that company.

At your place of employment you might even be at risk. Co-workers might be curious as to the activities you engage in on your computer. If their jobs require that they do different tasks then you, they may want to learn how you do your job. They may want to look at the programs you utilize to perform your job. Even worse, they may want to check your e-mail accounts. These are all possible motives of the shoulder surfer who may just be around the corner in the next cubicle.

Who can forget about those portable computers referred to as laptops? Many manufactures of laptops are now making them smaller and more battery efficient. Such improvements have allowed for computer users to easy take these computers with them wherever they go. Individuals who are passengers on planes and trains are now using laptop computers. Having access to data anytime and anywhere is extremely convenient. A majority of laptops are even made with screens that feature incredibly sharp resolution. This particular feature is great for the eyes of the computer user. Essentially, they no longer have to squint to see the screen like in the old days. However, a shoulder surfer within close proximity is now getting a clearer view of the information being inputted or outputted onto/from that particular computer.

You Wouldn't Be the First Victim

Stephen Ryan is an individual who fell victim to a shoulder surfer. One day, while utilizing one of the many public pay phones in Grand Central Station in New York City, a shoulder surfer watched Ryan. Ryan was simply using his telephone calling card to place a call. However, what he didn't know was that at that moment he was also exposing his calling card number to the individual watching him. After completing his phone call, Ryan hung up the phone and went about his business. "In only four days, his card number was used to make more than 100 calls to Michigan, the Dominican Republic, Massachusetts, Florida, Spain, Rhode Island, Venezuela, New Jersey, Yemen, Washington D.C., California and Washington. The bill, before the phone company realized what was going on and cut it off – about $1,000" [2]. Ryan, upon learning of the fraudulent activity on his card stated, "I was aware this was a problem and still got nailed". Stephen Ryan is like most people, aware but not cautious. This incident opened up Ryan's eyes to the problem of shoulder surfing. As a result, he says he wouldn't be making any more calls from Grand Central Station pay phones [2].

Who's Got Your Back?

Shoulder Surfing has gotten much attention over the years. Many suggestions have been made to help people make themselves less vulnerable to such attacks. Furthermore, improvements have been made to the devices or within the facilities where attacks of this sort typically take place. These suggestions and improvements are based mainly on common sense, logic and a little bit of street smarts.

Many telecommunications companies have tried to eliminate the amount of telephone fraud occurring at pay phones by installing automatic card readers and plastic shields onto the phones. By doing this, the need to key in any information other than the desired phone number the calling card customer wishes to reach, is eliminated [6]. However, not all pay phones are equipped with such features. As a result, telephone companies offer a few suggestions to keep oneself from becoming a target: "protect yourself by keeping your card hidden from view to keep others from seeing it. When dialing, cover the keypad with your other hand. If you must give your card number to the operator, speak directly into the mouthpiece and turn your back from the public" [7]. Others familiar with phone fraud suggest that one be aware of their immediate surroundings. If someone appears to be acting suspicious or gets too close, it is recommended that one move to another phone nearby [8]. It is also recommend that one purchase an automatic phone dialer. This sort of device generates beeps, which are hard for a shoulder surfer to interpret, making it virtually impossible for them to steal a phone card number [9].

In New York City, the Metropolitan Transit Authority (MTA) has taken certain measures to combat phone fraud caused by shoulder surfers. Undercover sting operations are conducted on a periodic basis within Grand Central Station. Working in conjunction with AT&T in New Jersey, who supplies the phone cards, undercover officers pretend to utilize pay phones in hopes of having a shoulder surfer nearby. If anyone attempts to shoulder surf, this will be noticed. However, so will the calls that the attacker will try to make with the stolen credit card number. AT&T can trace any calls made by the attacker using the calling card numbers he/she stole from the undercover officer. These traces will serve, as proof that the arrest made was justifiable [2].

The banking industry has also made some modifications to their ATM terminals in recent years. In earlier years, many ATMs had screens that were eye level to the user. Now, many ATMs are designed with a touch screen that is at an angle away from plain view of others. Furthermore, many ATMs are equipped with cameras. These cameras are a good way to deter shoulder surfers and another other individuals who want to stage an attack in this sort of environment [8]. Although all these new improvements help reduce attacks of this sort, it is still always important to be aware of one's immediate surroundings. Furthermore, it is always important to know how to properly use the ATM and do so relatively quickly. Scrambling through briefcases or purses for PINs and such might attract attention to possible shoulder surfers nearby. If one is smart, quick and safe, a shoulder surfer will probably move on to another target.

Computer users can also take certain measures to combat shoulder surfers. First and foremost, computer users should always be aware of their immediate surroundings. They should always be aware that someone

might at some point decide to glance at their computer screen if it is within close proximity. If possible, one should try and point their screen away from others. In the case of a laptop computer this may be easy. However, with bulky cathode ray tube (CRT) monitors attached to desktop computers, this may be somewhat difficult to accomplish.

A computer user can also avoid being the target of a shoulder surfer by making user names and passwords for access to computers, terminals or program applications long and difficult to guess [10]. It should also be stressed that one "make sure passwords are not echoed when they are keyed in" [11]. Furthermore, it is also important that a computer user choose a password that is easy to remember, yet hard to forget. Moreover, it is also a good policy for a computer user to change passwords periodically [10].

Summary, Conclusions, and Further Work

Shoulder surfing is a form of attack that can strike at any time and anywhere people and technology meet. As time passes, our lives will become more and more digitized. We will still have a name, but a special signature, code, or number may also help to positively identify us.

Many new technological innovations are slowly being introduced into today's society. Large majorities of people are embracing all the new gadgets and gizmos coming onto the market. Things are becoming more convenient and less time consuming. However, convenience and efficiency tend to also bring about an increase in vulnerabilities.

No matter how advanced a society we become, one thing is certain; we must always remember to protect our identity, privacy and integrity. Shoulder surfers are individuals pick a vulnerable target and exploit the information obtained from the person whose shoulder they looked over. They have the potential to steal someone's identity or disrupt someone's integrity or right to privacy. Technological innovations can be great; however, one must be extra cautious when utilizing them.

Experts in the field can always attempt to improve on technology and make things safer to use. However, improvements and such are not always the answer. In regard to attacks such as shoulder surfing, Vincent Vono says it best: "User education is the means to combat these types of information gathering, to block the leaking of information before its too late" [12]. Technology will always continue to advance. Ultimately, it is up to the user of that technology to use it responsibly and protect himself/herself while doing so.

References

[1]. Cohen, Fred. Attack 55: Shoulder Surfing.

http://all.net/CID/Attack/Attack55.html

[2]. Thompson, Lea. "Surfing For Digits". MSNBC.com.

http://www.msnbc.com/news/302773.asp?cp1=1

[3]. "Public Service Announcement Advices Holiday Shoppers on ATM Account Security".

http://nsi.org/Tips/atm.htm

[4]. "Fontoura Warns: The 'Eyes' Have It 'Shoulder Surfers' Steal Your Numbers".

http://www.essexsheriff.com/eyes.htm

[5]. Maier, Philip Q. Handbook of Information Security Management: Physical Security: Chapter 10-3-1.

http://www.ccure.org/Documents/HISM/699-703.html

[6]. The World Spy: Shoulder Surfing.

http://www.logophilia.com/WordSpy/

[7]. Citizens Communications: "Protect Yourself from Telephone Fraud".

http://www.citizenscommunications.com/cs_phone_fraud.cfm

[8]. Nulty, Thom. "Shoulder Surfers Create Airport and Depot Danger". Sacramento Business Journal: Aug. 20, 2001.

http://sacramento.bcentral.com/sacramento/stories/2001/08/20/smallb4.html

[9]. Magellan's Travel Guides - Passport to Business Travel".

http://www.magellans.com/guides/pbt6.html

[10]. Yager, Tom. "Securing Windows NT Server". NetworkMagazine.com: Feb 01, 1999.

http://www.networkmagazine.com/article/NMG20000509S0037

[11]. OUCC 26 User Authentication: "How Are Passwords Compromised?: Shoulder Surfing!"

http://www.utoronto.ca/security/ouccp33.htm

[12]. Vono, Vincent. "A General Overview of Attack Methods". SANS Institute: Jun 25, 2001.

http://www.sans.org/infosecFAQ/threats/attack_methods.htm

About the Author

Robert Fried holds a B.S. and an M.S. in Forensic Science with a concentration in Advanced Investigation. He also holds Certificates in Law Enforcement Science, Forensic Computer Investigation, and Information Protection and Security from the University of New Haven and SEARCH. Fried has extensive knowledge of forensic science, however, most recently he has worked extensively in the developing field of

"digital forensics" and has published in this area by organizations such as the SANS Institute. He is also a member of the NorthEast chapter of the High Technology Crime Investigation Association (HTCIA).