

# 2

## **Is Banking Online a Safe Alternative to the Old Fashioned Paper and Pen?**

Jamie Stoll & Matthew Collett

### **Introduction**

The newest form of identity theft is known as account hijacking, i.e. unauthorized access to a given account. Whether the successful break-in occurred from information gathered online or from personal documents that did not get shredded. Account hijacking can be accomplished in a number of ways: retrieving hard-copy documents, luring consumers into giving up usernames and passwords, loading malicious software onto public or private computers, and via the most familiar method: hacking. Regardless of method, account hijacking is the fastest growing type of consumer fraud. "In 2003, 10 million Americans discovered they were victims of identity theft with a total cost approaching \$50 billion" (Putting). The ease of break-ins is partly a result of weak yet accepted security: "Our current culture, where identity is verified simply and sloppily, makes it easier for a criminal to impersonate his victim" (Schneier). Online banking has become an easy target for account hijacking, with valuable information just waiting to be stolen. How safe is online banking and what is being done to protect this personal information?

### **Background**

Giving up privacy in order to conduct more efficient and timely financial transactions can pose a big security risk, yet many Americans still choose to do so everyday. With the click of a button, purchases made within the last day, week or even earlier can be displayed. What prevents a hacker from stealing that information or a malicious program from saving and downloading it elsewhere? Financial institutions have implemented several consumer security measures to reassure their customers of the safety of online banking. These include encrypted numbers and letters that have to be entered to gain access to a site and a lock icon indicated a trusted and secure site. Although these security measures may appear to be sufficient at first glance, they are

being sabotaged and exploited by account hijackers using methods of their own.

## **Phishing**

Phishing can come in the form of an e-mail or fake website, asking for personal information such as name, address, social security number, age and even account numbers and passwords. Once this information is obtained by the phisher, it can be used for opening new credit card accounts, obtaining car and home loans, and even buying real estate. Most, if not all, large financial institutions and electronic bill-paying services (such as PayPal) have been subject to phishing attacks (Putting). This topic is covered in greater detail in a later chapter.

## **Hacking**

Financial institutions are frequently targeted by hackers because they contain valuable information about their customers. Fraudsters hack into financial institutions' databases or service provider systems to steal confidential customer information to use at their discretion (Putting). Many people believe that their financial institution has strict laws and policies regarding security, but, realistically, the development and implementation of most security and protection programs is the responsibility of the individual company. The federal Gramm-Leach-Bliley Act, or GLB, only provides minimal requirements to protect your financial information, and in the end these regulations are actually guidelines rather than strict rules for compliance (Is).

## **Hard-copy Documents or Looking Over Someone's Shoulder**

Forgetting to shred physical personal documents can lead to severe consequences. There have been many reported incidents of banks, credit card companies and even retail shops throwing away documents with sensitive data without shredding them before hand. "Current and former account holders of the Circuit City credit card are being notified that their personal information was thrown out with the trash" (numbrX). Thieves also resort to "dumpster diving," where they rummage through trash to get sensitive and confidential information, which is much more labor intensive than other methods. Once they have this information they can easily steal someone's identity. Although this is a much harder way of retrieving information it does happen and people should be aware of this risk.

## **Using Insiders**

Industry analysts and security professionals estimate that 65 to 70% of identity theft is committed by confidential information being stolen by employees or participants in transactions or services (Putting). This form of hacking is often unpredictable and actions against it are the responsibility of the company involved. It is more common than not to have security cameras, employees checking other employees, and forms to be filled out when dealing with money. Companies tend to not notice such problems until something is out of the ordinary. Then, it is simply a matter of them discovering the theft in time and promptly taking action.

## **Malicious Software**

Malicious software programs can be put onto personal or public computers without the users' knowledge, and can be used to collect various types of personal information such as passwords, usernames, account numbers, etc. These programs are known as "spyware" and can come in several forms, from pop-up ads to unknown icons installed on your desktop. Spyware removal programs exist, but without widespread awareness of these issues this method of theft is hard to detect and prevent.

## **How Banks are Securing Information?**

The newest ways that banks are attempting to increase information security is to require customers to identify certain preset pictures, multi-factor authentication, and electronic bank notes.

### **Preset Pictures**

When a customer opens an account they are prompted to choose a picture that will pop-up when logging into their account online. This technology is beneficial, but could become obsolete if scammers find a way to get a copy of the preset pictures, or begin sending phishing e-mails to find out what particular picture a customer has.

### **Multi-Factor Authentication**

Banks are now implementing multiple security measures to gain access to an online account. Some of these new and existing technologies include tokens, thumbprints, retina scans, and other data. Tokens are battery-powered devices that display a random six digit password every 60 seconds (Banks). Along with entering the token password, customers still need to enter their personal username and password. Some banks are even implementing retina scans and thumbprints to verify the customers' identity.

### **Electronic Bank Notes**

"The blinded note numbers are 'unconditionally untraceable' that is, even if the shop and the bank collude, they cannot determine who spent which notes" (Chaum). Electronic bank notes are basically messages signed using a particular key, and then the bank would have another key in order to verify the account. Here is an example of how electronic notes would work:

To withdraw a dollar from the bank, Alice generates a note number (each note bears a different number, akin to the serial number on a bill); she chooses a 100-digit number at random so that the chance anyone else would generate the same one is negligible. She signs the number with the private key corresponding to her "digital pseudonym" (the public key that she has previously established for use with her account). The bank verifies Alice's signature and removes it from the note number, signs the note number with its worth-one-dollar signature and debits her account. It then returns the signed note along with a digitally signed withdrawal receipt for Alice's records (Chaum).

Although this system appears to be very secure because of the randomness and security processes, electronic bank notes still pose problems of hacking. For instance, if the notes are stored in a database at the bank, they can be hacked into. In order to prevent duplication of the notes and to ensure their privacy and protection from outside hackers, a bank must implement an efficient and centralized verification system.

## How Safe is Online Banking and is Personal Information Protected?

Information is being accessed and stolen so easily because the right precautions are not being taken to prevent theft. Shouldn't banks be stricter with security policies in order to protect consumers? How many customers are aware of the risks involved with online banking? Does age, gender, or a previous fraud experience affect a person's outlook regarding banking online? The following firsthand research was conducted to determine the average consumers' knowledge about online banking and the security risks involved.

### Survey Research

In order to gain an insight into what online banking customers know about online security threats, an 11-question survey was conducted. The survey was administered online through facebook.com, and distributed to a senior level class at the University of Colorado as well as to the employees of respective the researchers' family members' workplaces. The questions were created to target the weaknesses and strengths of online banking. Two of the questions were rated on a ten-point scale with one being the lowest possible score a respondent can give and ten being the highest.

Table 1 reveals the quantitative results of the survey. Through analysis of the data gathered, certain conclusions were reached about how gender, age, and experience with online banking fraud can affect an individuals' knowledge and opinion of online banking.

**Table 1. Survey Results**

	All Respondents	Female Respondents	Male Respondents	Do Not Bank Online	Online Banking Fraud Experience
Average Age	32.5	33.5	30.4	37.8	39.1
% Male	33.3%	0%	100%	27.3%	37.5%
% Female	66.7%	100%	0%	72.7%	62.5%
% With A Bank Account	100%	100%	100%	100%	100%
% That Bank Online	79.6%	77.8%	83.3%	0%	62.5%
Average Safety Rating When Banking Online (1-Not Safe, 10-Very Safe)	7.9	7.8	8	5.7	6.2
% That Had A Personal Experience With Online Banking Fraud	14.8%	14.3%	16.7%	27.3%	100%
Average Worth Of Online Banking (1-Not Worth It, 10-Very Worth It)	7.7	7.3	8.4	5.8	5.4

## **Gender and Attitudes**

Studying the gender of the respondents along with their respective results one can conclude that there are slight differences in how females and males feel about banking online. Males are more likely to bank online compared to females, with results showing that 83.3% of the male respondents bank online as opposed to 77.8% of the female respondents, although this difference of just over 5% is not drastic. In order to understand this disparity, it is necessary to examine the questions surveyed relating to feelings toward online banking.

This result can be directly correlated to how safe the respondents feel banking online is as well as how the convenience of online banking can outweigh the risks involved. The survey findings show that when asked how safe they feel banking online is, on a scale of one to ten (one representing not safe at all, ten representing very safe), male respondents feel safer than female respondents with average scores of 8 and 7.8 respectively. When asked if the risks were worth the convenience provided by online banking, rating the risks on a scale of one to ten (one representing not worth it, ten representing very worth it), male respondents answered an average of 8.4 while female respondents answered with an average of 7.3. These statistics support the conclusion that female respondents are less likely to bank online than males. Despite the minimal quantitative difference in males and females' feelings of safety, when examining if the risks are worth the rewards of convenience, a larger disparity exists. These results suggest that as a whole, women do not value the convenience of online banking over the risks it poses in comparison to their male counterparts, who feel that the risks are worth the rewards of convenience.

## **Age and Use**

Does age affect how people adapt to new and advancing technologies, such as online banking? The average age of survey respondents was 32.5 years old. Of those who currently do not bank online, the average age was 37.8. This statistical difference of over five years suggests that the older a person is, the less likely they are to bank online (assuming that they have a bank account, as all the respondents in the survey did). This could be caused by many factors. People can become set in their ways, and if they are used to banking in person, it can be difficult to change and adapt to the online banking process and technology. In a world of rapid technological advances, it can be difficult for a person lacking experience with such technologies to successfully acclimate to them.

The average age of the respondents surveyed who have had a personal experience with online banking fraud was 39.1 years old. This is compared to the average age of all respondents being 32.5 years of age. Since online banking fraud has and continues to affect so many people, the more time a person spends banking online, the higher chance they have of experiencing online banking fraud, which helps explain the statistical differences from above. This age disparity can also be explained by the theory that older online banking customers are unaware of the newest technological advances in online banking fraud, and are thus potentially more susceptible to falling victim to them. Either way, survey results show that the older a person is, the greater the chance they have of being exposed to some type of online banking fraud.

## **Personal Experiences with Banking Fraud**

Of all survey respondents, nearly 15% had a prior personal experience with online banking fraud through either their own personal experience, or that of someone they know. The statistics show that if a respondent fell into this category their feelings about banking online were severely effected. Out of a highest possible score of ten, the respondents who have had a personal experience with this type of fraud gave online banking an average safety rating of 6.2, a decrease of 1.7 points from the overall average safety rating of 7.9. They also had an average answer of 5.4 when asked to rate the convenience of online banking versus the possible security risks. This score is more than a 2-point decrease from the survey average of 7.7, and is expected to be due to the individual personally experiencing the consequences of this type of fraud. Of these respondents, 62.5% of them still bank online but are becoming increasingly more careful about their private information.

## **Why Do Some People Not Bank Online?**

According to the survey, 20.4% of respondents do not bank online but still maintain an active bank account. After further analysis of the collected data, it is clear why these individuals have made this decision. Out of a highest possible score of ten, the average rating given when asked how safe they feel while banking online was 5.7, down from the survey average of 7.9. Also, the respondents who do not bank online rated an average of 5.8 when asked to weigh the convenience of online banking to the risks involved. This is down from the 7.7 survey average. It is apparent that these respondents do not bank online due to safety and security issues, and do not feel that the convenience provided by online banking outweigh the security and privacy risks involved.

The survey conducted produced a large amount of quantitative data that was analyzed and used in making many conclusions about online banking security in the previous pages. However, the survey also contained important questions that required qualitative responses from the respondents. These responses are also extremely important to gain an understanding of the opinions of online banking customers, and how aware they are about important security issues. The following contains summaries of the answers given.

## **Why Do People Bank Online?**

In order to understand why so many people bank online while simultaneously accepting the risk of exposing themselves to online banking fraud, it is important to recognize the advantages online banking offers to the customers. Of the people surveyed who use online banking, 100% of them answered "convenience" when asked why they bank online. The ease of online banking and the ability to make financial transactions without having to leave the comfort of home is an attractive incentive to banking customers. Online banking can also save customers money on checks that would be used to make the same transaction in person. Customers can also keep close track of their accounts to monitor if there has been any fraudulent or unusual activity. There are undeniably many positive aspects of banking online,

which could make it difficult to resist these conveniences, even when considering the negative aspects.

### **How Do Criminals Obtain Personal Information?**

It is essential to examine the respondents' awareness of the methods used to extract personal information from online accounts to pinpoint the areas where customers are more likely to fall victim to online banking fraud. Of all the answers given, the most common responses were "stealing social security numbers, sending out bogus emails in the attempt to gain personal information, and hacking into a computer". Although these are all valid ways of stealing personal information, many of the methods described in the beginning of this chapter were absent from the responses. These commonly given answers demonstrate that many of the respondents are aware of possible threats, but there are still some respondents that are completely unaware of any threat whatsoever. It is important for the safety of online banking customers that they become aware of the various ways criminals can obtain private information.

### **How Banks Can Increase Security**

One of the last questions in the survey asked respondents "what can banks do in order to increase security with online banking". Other than technology advances, the most common responses were "to increase awareness of the types of online banking fraud, and take precautions to protect oneself". Banks could accomplish these objectives by requiring customers to read a packet of updated online banking scams and what steps to take to avoid falling victim to them. Another option would be for banks to offer free computer security software when customers sign up for online banking. This would ensure that those customers who are not aware of the importance of securing their computer will have the proper software to do so.

### **Weaknesses**

As with any survey research there are weaknesses that need to be addressed. The primary weakness of the survey conducted arises from the small sample size of respondents that completed the survey. In order to gain data that would more strongly support the previous conclusions, a larger sample of people would have to be surveyed. Another weakness encountered was the under-representation of certain demographics. It cannot be determined if class or race concentrations would reveal different survey results, but a more diverse sample could have produced more accurate statistics to better represent the online banking community as a whole. Also, every respondent was either in college or had college degrees, which is not likely to be representative of the customers who use online banking. These respondents may be more aware of the steps to take in order to protect themselves than others due to their education. Lastly, the survey conducted switched between quantitative responses and qualitative responses. It would be important to remain consistent during each part of the survey in order to keep respondents interested and possibly less confused.

### **Further Considerations**

Due to time constraints, various types of research and considerations could not be investigated or addressed. First, creating a more in depth survey including such categories as race, income level, location, education level, and party affiliations would have helped gain a deeper insight into the diversity of online banking customers. With this knowledge correlations could be found among respondents to determine whether attitudes vary within these categories, as well as how those attitudes affect what precautions are taken for protection and security. It would also be beneficial to personally interview online banking professionals about the future of the industry, as well as about the biggest issues regarding online banking security. Finally, conducting actual experiments with online banking customers regarding new technologies would be valuable to the progress of online banking in the future. It would be imperative to explore these issues further in order to expand on this chapter and the issues discussed within.

## **Conclusion**

Through extensive research and analysis, the following conclusions have been reached. For the most part, consumers are very unaware, or are not taking the time to be concerned about their security in terms of online banking. In such a technological era, it seems that people would be more aware of the dangers and risks that involve sensitive information and the Internet. What seems to be playing a role is that people have such busy lives, that they would rather sacrifice their security than take the time to make sure the right precautions are taken to protect it. It is also apparent that consumers need to be better informed regarding the security steps required to protect their private information from those trying to acquire it.

Research data concluded valuable insight into gender and age differences concerning issues involved in online banking. It is apparent that in a world where speed and time efficiency are becoming increasingly important to an individuals success, the convenience of online banking would be the only choice when trying to keep up with the competition. It is for this reason that younger people are more likely to bank online, because they have to maintain and strive for a competitive advantage when making the transition into the business world. There is no question that the emergence of online banking has increased the rate at which people conduct business today.

With identity theft costing billions of dollars, it is staggering that online banking customers are so highly unaware of the different methods criminals use to obtain private information. Banks need to take more initiative to inform their customers of the potential dangers involved with online banking fraud. They need to understand that online banking sells itself through its convenience and ease of use, and that their role should be as a guardian with respect to their customers' information. Until these security issues are resolved, criminals will continue to reap the benefits from the overall lack of knowledge and action by both banks and online banking customers.

## **Works Cited**

Banks Try New Systems to Protect Online Users. 2 Jun. 2005. MSNBC. 5 Mar. 2007. <<http://www.msnbc.msn.com/id/8071171/>>.

Chaum, David. Achieving Electronic Privacy. Scientific American. Aug. 1992: 96-101.

Is Your Financial Information Safe?. Sept. 2004. Privacy Rights Clearinghouse /UCAN. Mar. 4, 2007. <<http://www.privacyrights.org/fs/fs24e-FinInfo.htm>>.

numbrX Security Beat. 8 September 2006. Privacy Rights Clearing House. 16 March 2007. <<http://www.numbrx.net/category/banks/>>.

Putting an End to Account –Hijacking Identity Theft. 14 Dec. 2004. Federal Deposit Insurance Corporation. Mar. 1, 2007. <<http://www.fdic.gov/consumers/consumer/idtheftstudy/index.html>>.

Schneier, Bruce. "Solving Identity Theft." Forbes.com 22 Jan. 2007: 1.