
# Mitigating Online Account Takeovers: The Case for Education

**Michelle Castell**

Retail Payments Risk Forum Survey Paper
Federal Reserve Bank of Atlanta
April 2013

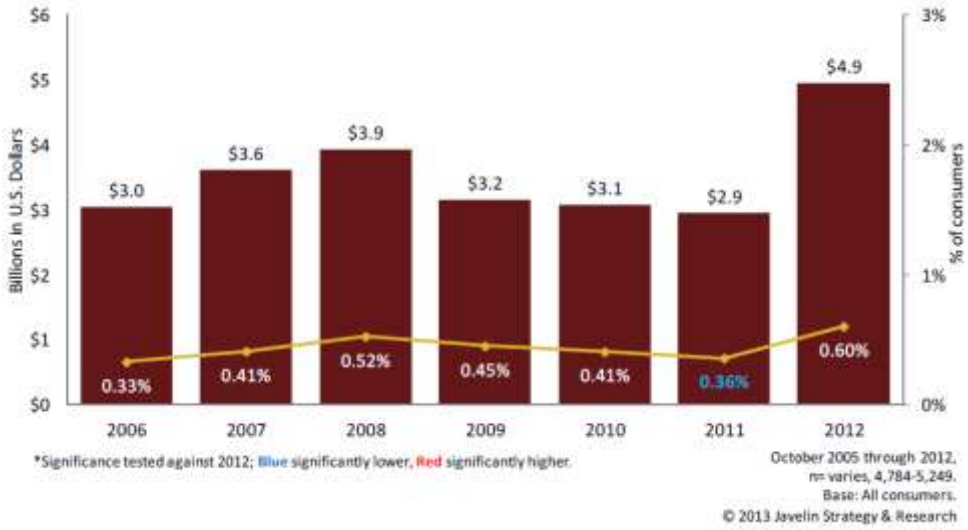
**Abstract:** Online account takeovers are one form of identity theft. They occur when an unauthorized party gains online access to an existing bank account by stealing the access credentials to the account and then conducts illegal transactions. These incidents are increasing in both frequency and levels of financial loss.

Today's cyber landscape is rapidly connecting people spanning the globe. This growth in connectivity, convenience, speed, technology adoption, and payment options provides the benefit of allowing individuals and businesses to more easily and efficiently conduct their online financial activities. Individual behavior and motivation, legal boundaries, and technology advances are all major factors contributing to this explosive growth. Unfortunately, these factors have also spawned another form of criminal activity; one that is more difficult to detect as well as prosecute. This paper examines the underlying methods used in online account takeovers, reviews the economic impacts for both the perpetrators and the victims, and identifies risk mitigation strategies for the various parties involved.

## I. Online Account Takeover Defined

An online account takeover occurs when someone other than the authorized account holder gains access to an existing account.[a] The target of an account takeover is a customer holding an account at the financial institution, and the ultimate goal of a takeover is to remove, steal, procure, or otherwise affect funds of the targeted customer.[1] While account takeovers are most often achieved through the use of malicious software that can exploit just one entry point into a network to start the theft, fraudsters may also use social interaction to prompt individuals into divulging account information. This information allows the fraudsters to access the account and move the money out of the account in a very short time. A recent Javelin study estimated losses from account takeover fraud of over $4.9 billion in 2012, representing a 69 percent increase over 2011. The same study concluded that much of this increase is likely attributable to security vulnerabilities in online and mobile channels, as well as shifts in consumers' use of technology.[2] While this $4.9 billion in losses includes other consumer accounts such as loans, insurance, telephone, and utilities—in addition to deposit accounts at financial institutions—the data illustrate the growing incidence of account takeovers.

**Account Takeover Fraud Incidence and Total Fraud Amount by Year**



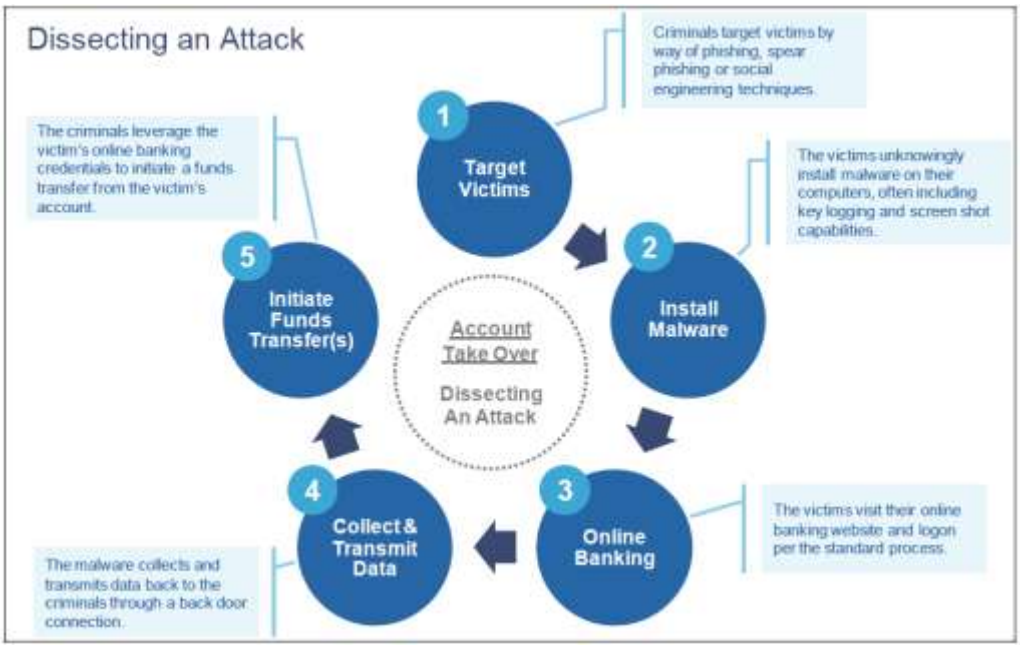

Source: "2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters." Javelin Strategy & Research, February, 2013.

[a] Any form of identity theft generally involves some type of account takeover activity, whether it involves financial or personal identification. For the sake of simplicity, the term "account takeover" is used in this document instead of "online account takeover" to refer specifically to gaining access credentials to the target's deposit account at a financial institution.

## II. Anatomy of an Account Takeover

Although the account takeover sequence can be initiated through various means, most often the consumer or an employee of the targeted business is lured into opening e-mail attachments or responding to social media friend requests, which often redirect the person to compromised websites. As shown in the diagram below, cyberthieves may use phishing[b] or spamming[c] in order to gain access to the computer system.

There are several methods of obtaining the account information depending on the ultimate goal of the intrusion effort. However, Trojan keystroke loggers are commonly used. This malicious software (malware) monitors and captures keystrokes including account access credentials and sends them to the cyberthieves, to gain access to the account. This malware can be customized to target groups of individuals with the goal of accessing either financial or proprietary information. Once compromised, the criminal has access to the user passwords and credentials allowing him or her to control the system, transfer funds out, or gather and transmit data as desired.




Source: "Fraud Advisory for Businesses: Corporate Account Take Over." United States Secret Service, FBI, IC3, and FS-ISAC.

[b] *Phishing* is an e-mail fraud method in which the perpetrator sends out a legitimate-looking e-mail to try to gather personal and financial information from recipients.

[c] *Spamming* is the use of electronic messaging systems to send unsolicited bulk messages, especially advertising, indiscriminately.

## III. The Role of the Internet

The explosive growth of the Internet across the globe has provided numerous benefits to individuals. Since 2000, the number of Internet users has increased over 566 percent, accounting for nearly two billion more active participants. This represents an increase from six percent of the world's population to 34.3 percent as reported in June 2012.[3]

Corporate users of the Internet have also expanded. A survey of small businesses across the nation revealed that 90 percent report using online resources to help manage their business operations.[4] Online activity by business owners or employees includes online banking and the use of the Automated Clearing House (ACH)[d] services as an effective means for direct deposit payroll, bill pay services, and vendor payments.

## IV. Demographics and Risk Behavior of Internet Users

In addition to the growing population accessing the Internet and conducting online financial transactions, the demographics of online users have also changed. The Gen Y and millennial segments consistently use a mobile phone and opt for electronic payments as a standard way of life. Conversely, most seniors believe that mobile phones are for talking and not conducting banking transactions; they tend to rely more on cash and checks as a means of payment versus electronic payments.[5] These differences highlight the shift in the amount of potential risk younger people are willing to take regarding their personal finances. It could be concluded that today's younger generation seem less concerned about safety in part due to the zero liability guarantees from credit card companies and banks. A 2012 survey of 431 consumers in the Americas uncovered some concerns related to card fraud—primarily the increasing skill and ability of the fraudster and the time and hassle to resolve fraud. The concern over financial loss was a distant fourth on the list.[6]

These different segments generally display different responses to online fraud vulnerabilities, as each generation has different expectations and different needs. Categorically, the younger Gen Y is criticized for making too much personal information available on a public forum—the web—despite their awareness that fraudsters and hackers exist and are constant threats. According to the recent Javelin study, this generation was most likely to respond to fraud by changing

[d] ACH is a nationwide electronic funds transfer system that provides for the interbank clearing of credit and debit transactions and for the exchange of information among participating financial institutions. Electronic funds transfer, also known as EFT, is the electronic exchange of money from one account to another (by wire), either within a single financial institution or across multiple institutions, through computer-based systems.

payment behaviors and switching their bank or credit card providers.[7] By comparison, the seniors category, although the most conservative when it comes to online banking and Internet use, is also the most trusting and most likely to fall prey to fraudulent scams to obtain personal or banking information. Considered to be largely unaware of scamming or phishing schemes, the seniors need an education much different from that of other generations. Educating all age groups is important, but given the trusting nature of the seniors, specific focus on the warning signs and dangers lurking on the Internet would help this vulnerable group and potentially assist in preventing account takeovers.

## V. Accessing the Internet

Along with the shift in demographics, the methods of accessing the Internet have expanded. What was once a hard-wired computer connected to the Internet has morphed into handheld devices, including tablets and smartphones, with far more capability than the desk top computers of the last decade. Smartphones are becoming more prevalent worldwide due to low cost and PC-like functionality. There are currently six billion mobile subscribers worldwide representing 87 percent of the world's population. This includes over one billion smartphones, a number predicted to double by 2015.[8] Each of these devices represents an additional channel for account takeovers to occur. Estimates show that at any given time, there are 1.2 billion people accessing the web from their mobile device. Additionally, in 2011 alone, 8 trillion text messages were sent.

## VI. Malware and Its Role in Account Takeovers

One of the more prevalent and sophisticated types of malware used in recent account takeovers efforts is called Zeus. Since the malware was first identified in 2007, cyberthieves have transformed Zeus by modifying its source code,[e] making it difficult for antivirus software to detect it. Zeus is often spread through phishing attacks or man-in-the-browser attacks (MITB). In an MITB attack, the victim's browser is infected with the Trojan, which modifies the actions of the computer user in real time and can also work independently of the user. The Trojan lies in the victim's browser waiting for the user to access certain websites, such as online banking sites. After the user is successfully authenticated, Zeus "piggybacks" on the user's session, intercepting and modifying details of the transaction. Further adding

[e] *Source code* is the programming language used to write a computer program. Malware source code can be copied, modified, and molded into a new threat with relative ease. In May 2011, the source code for the Zeus Trojan was leaked to the public and what once sold for thousands of dollars was now available for free.

to the accessibility of fraudulent resources, the source code for Zeus was leaked on the Internet in May 2011, allowing anyone to take it and rewrite it.

The year 2012 witnessed the largest account takeover on record, an event known as Operation High Roller. The attack spread from Europe and Canada to the United States and did not require any human intervention. The attack involved modified versions of Zeus, which were used to skim money from high-balance accounts onto prepaid debit cards and to modify the statement balances to mask the transactions. The malware was installed on computers through tainted links in e-mails, or when users visited malicious websites or legitimate pages already compromised by hackers. The attack not only serves as an example of how malware can be used to execute account takeover, but also demonstrates the ease, speed, and proficiency with which this can occur with the use of the right malware.

Although the more widespread and well-organized attacks involve expensive, sophisticated technology, cybercrime has proliferated to the underground online marketplace and the "small-time" cybercriminal. Criminals can actually shop for off-the-shelf malware and hardware products to buy. This scenario is referred to as Crime as a Service (CaaS). The organizational structure of these underground cybercriminal groups mirrors that of a legitimate corporation. They are controlled by executives who set up the business model, oversee the operations, and ensure that the business provides a sufficient return on investment. Managers are hired to oversee the recruitment of staff. They run help-wanted ads soliciting those willing to make money working online. These businesses stay small and are very careful who they sell to, usually requiring a "referral" to gain access. It is the perceived legitimacy of this cybercriminal business that is fueling the growth of malware and making it easier to successfully execute account takeovers. Due to hosting providers of these organizations often being often found in political safe havens such as Russia and China, closing illegally operated host networks is a difficult task.[9]

Another attack method using botnet malware that is gaining popularity is called Disruptive Denial of Service (DDoS) attack. According to the Financial Services Information Sharing and Analysis Center (FS-ISAC), a DDoS attack is a coordinated cyberattack intended to disrupt the availability of an information processing system or application by consuming network bandwidth or by overwhelming the target system with simultaneous data connections from multiple autonomous sources.

Historically, the DDoS perpetrators appeared to be activist or hacktivist related simply to make a political statement. However, 2012 witnessed a shifting toward

cybercriminals who wanted to disguise their account takeover attacks while the target financial institution's IT resources were diverted to dealing with the DDoS attack. In a DDoS attack that occurred over the 2012 Christmas holidays, $900,000 was successfully wired out of the bank accounts of a California construction company. The DDoS attack disabled the bank's website while money was transferred to 62 money mules so the company could not access its account information through their bank and become aware of the activity. "It's not clear what tactics or botnets may have been used in the DDoS attack, but the cyberheists+DDoS approach matches the profile of cybercrime gangs using the Gameover Trojan—a **ZeuS Trojan** variant that has been tied to numerous DDoS attacks initiated to distract attention from high-dollar cyberheists," wrote Brian Krebs in his blog, *KrebsOnSecurity*.[10]

In addition to the risk of experiencing financial theft, organizations under a DDoS attack could also incur financial and reputational loss due to lack of productivity, business disruption, extortion, asset loss, and customer dissatisfaction. The magnitude of potential loss from the fraud activity such as the one above makes this type of attack extremely dangerous.

## VII. Additional Methods for Account Takeovers: How Social Engineering Plays a Role

Account takeovers do not always involve malware as the means for the criminal to gain the targeted victims online banking credentials. Data are often readily available through public websites and can be used by fraudsters to request changes to a customer's profile (such as a change of password or address) or to add second account holders—actions that can then be leveraged to more easily perpetrate fraud. When correct personal data is used by fraudsters to change a victim's account profile, identifying and monitoring the potential fraud becomes far more challenging. This in turn results in an account holder's monitoring of their own account as the primary line of defense. With the growth of social networking sites such as Facebook, personal data such as date of birth, phone number, or mother's maiden name are often easy to come by, allowing perpetrators to contact an institution's customer service department to make changes to the victim's account just by using the information that was in the public domain.

In August 2012, a dangerous blind spot was uncovered when a hacking took place that combined partial data obtained from the websites of two well-known businesses, Apple and Amazon. This incident did not involve computers or a compromised website, just the telephone. According to one victim, Mat Honan, a

*Wired Magazine* writer, the crime happened because of the accessibility and availability of information needed by the fraudsters to gain access to his accounts.

> What happened to me exposes vital security flaws in several customer service systems, most notably Apple's and Amazon's. Apple tech support gave the hackers access to my iCloud account. Amazon tech support gave them the ability to see a piece of information—a partial credit card number—that Apple used to release information. In short, the very four digits that Amazon considers unimportant enough to display in the clear on the web are precisely the same ones that Apple considers secure enough to perform identity verification. The disconnect exposes flaws in data management policies endemic to the entire technology industry, and points to a looming nightmare as we enter the era of cloud computing and connected devices.[11]

This incident exemplifies the interconnectedness of the Internet**.** It is imperative that collaboration exist across all customer channels as detection and solution methods are implemented.

## VIII. Legal Implications

As has often been the case when guidelines, regulations, and laws have not kept pace with product and service advancements made possible by technology innovations, the resolution of the ultimate financial liability for monetary losses resulting from an account takeover is no different. Judgments have been mixed in the court system due to different interpretations of the governing provisions of the UCC. UCC 4A provides that the risk of loss for an unauthorized transaction lies with a customer if the bank can establish that its security procedure is a commercially reasonable method of providing security against unauthorized payment orders. The challenge comes in the courts determining if the bank's procedure is *commercially reasonable* based on the circumstances of the incident.

A ruling made in 2011 in favor of a small business (Experi-Metal Inc. v. Comerica Bank) magnifies the potential impact of one employee's actions on an entire business and its financial institution. In this case, an employee responded to an e-mail he believed was from the employer's bank, Comerica. The e-mail directed him through a fraudulent link to a fake (phished) bank website, where he entered the requested passcode. Within hours, the attackers made 97 wire transfers for more than $500,000. The funds were transferred to accounts in five different countries and never recovered. In this case, the court favored the business, stating that the

bank should have had in place fraud detection mechanisms to detect and analyze "risk factors."

The account takeover method used in this case is similar to that of the 2009 Patco Construction Company (Patco's Construction Company v. Peoples United Bank) account takeover in which the cyberthieves transferred $589,000 out of Patco's bank account over a six-day period. Despite the fact that the bank used challenge questions as a two-factor authentication method—questions the thieves successfully answered—the court found in favor of the company. The court placed the liability of the loss on the bank, ruling that the bank failed to notify Patco that the transactions were flagged as "very high risk" because they were inconsistent with the timing, value, and geographic location of Patco's regular payment orders.

As an example of the specificity of the circumstances in each account takeover case, in March 2013 BancorpSouth received a summary judgment from a U.S district court in Missouri on a suit filed by one of its customers (Choice Escrow and Land Title, LLC v. BancorpSouth). In 2009, cyberthieves gained access to the company's online banking ID and password and made an unauthorized wire transfer of $440,000 to a corporate bank account in Cyprus. Choice Escrow alleged that BancorpSouth Bank's security procedures were not "commercially reasonable" because BancorpSouth did not mandate the use of dual and separate IDs/passwords but only made that option available. The court ruled that since Choice Escrow was offered and explicitly declined in writing the use of dual controls, they were liable for the loss.

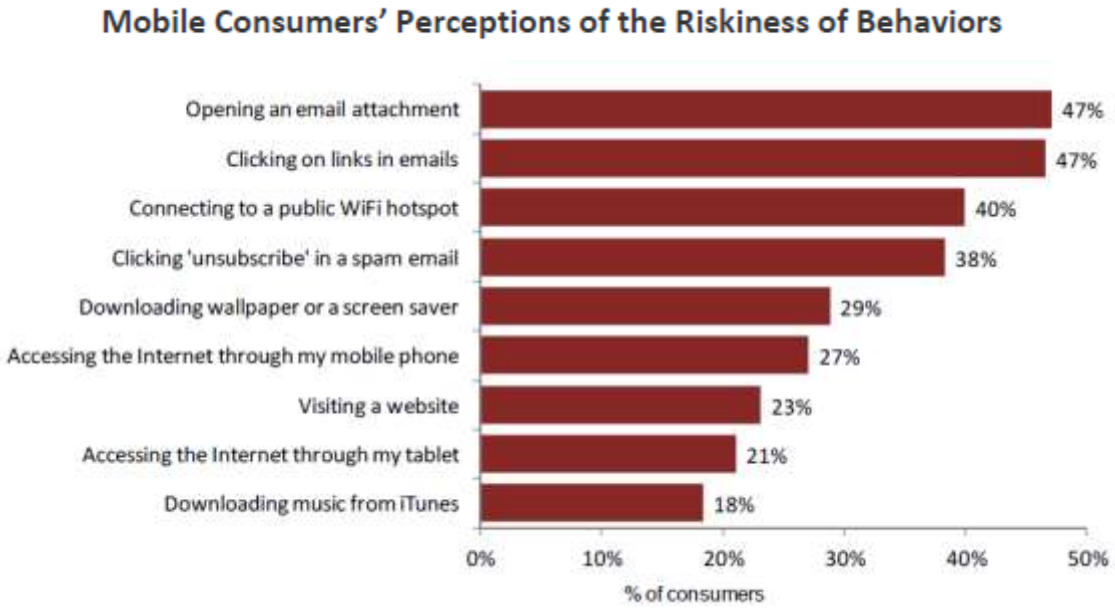
In all three cases, the banking credentials of each company were compromised through malware introduced by an employee's actions, actions that subsequently led to account takeovers resulting in tremendous financial losses.

## IX. Technology: The Problem or the Solution?

Are the rapid advances in technology leading to solutions or increased vulnerability? Commercial and retail products are available to safeguard against phishing, keystroke logging, and endpoint takeovers, as well as man-in-the-browser attacks, but are they being effectively used? Antivirus software has long been available for consumer protection. However, statistics show that 17 percent of computers do not carry any virus or malware protection.[12] In addition, a recent survey found that 40 percent of organizations do not have the in-house capability to prevent and detect cybercrime.[13] Most consumers and businesses appear to be reactive rather than proactive when it comes to cybercrime. Mitigating

consequences of certain attacks is adequate if preparation is complete and the individual or organization has a plan in place to execute. Without preparation, no software can completely protect against account takeover attacks.

As new technology evolves and solutions emerge to successfully mitigate some forms of account takeovers, thieves no doubt will shift their attention to less defended targets. Mobile devices now provide fraudsters a variety of ways by which to compromise the data stored or transmitted by those devices, thus opening additional doors to account takeovers. In fact, according to the graph that follows, fewer than 50 percent of mobile consumers find many otherwise dangerous behaviors to be risky when they are in a mobile environment.

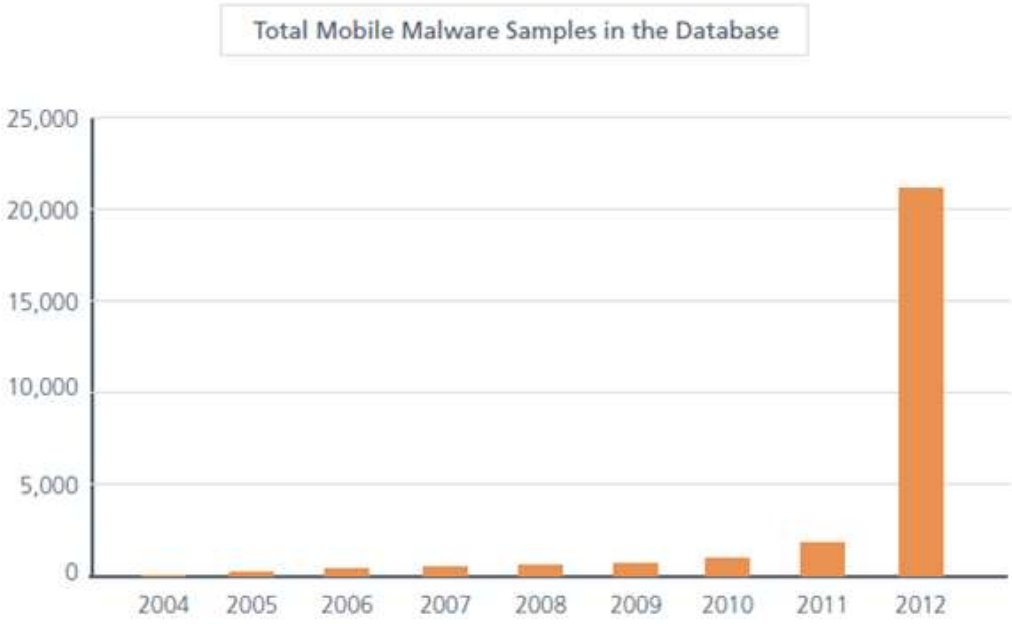



Source: *2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters*. Javelin Strategy & Research, February 2013.

Furthermore, studies reveal that smartphone users are three times more likely to provide their login information when prompted by mobile applications than those accessing the Internet from a personal computer.[14] With these volumes, fraudsters using technology to interact with users, including mobile users, are greatly enhancing their chance of perpetrating a successful attack. For example, obtaining account credentials through text messaging rather than e-mail—a method called "smishing," which is based on SMS, the abbreviation for "short message service"—is quickly becoming a fraud tool of choice. In this case, the mobile customer receives a text message that appears to be from a legitimate business directing the customer

to a malicious website or to an automated telephone system where the customer is prompted for their account ID and password information.

Mobile devices, much like personal computers, often contain a comprehensive record of one's life, including everything from personal and business contacts and messages to access to photos, social networks, shopping habits, and rewards information. If a mobile device is compromised, the amount of information available to a fraudster can be as damaging as information from a computer. A study conducted on European users found that although 84 percent of users have antivirus software on their computers, only 10 percent have protective software on their smartphones. The primary response given for low participation was "no knowledge that it was necessary and did not know that it existed."[15] Recent data published by McAfee Labs make it is clear that mobile devices need protective software because the amount of mobile malware planted on mobile devices increased significantly in 2012.




Source: *McAfee Threats Report*: Third Quarter 2012. McAfee Labs.

From a cybercriminal perspective, it's just as easy to access a financial institution or business account through a mobile text or e-mail as it is through a computer. While free antivirus applications are available and can help protect against many of these scams, educating the user on the vulnerabilities and risks of not having antivirus protection should still be on the forefront as one of the most effective defenses against account takeover fraud.

Should antivirus applications become standard on smartphones? One phone manufacturer recently announced it was teaming up with a virus protection company and will begin shipping most Android models with out-of-the-box protection against application malware and viruses. This partnership could be a significant first step in virus protection for smartphones, especially if other phone manufactures follow suit.

## X. Educate the User

Technology is only a portion of the solution. Educating customers, consumers, and employees how to interact with technology is also important. As new technologies emerge to successfully prevent many types of fraud, as well as new ways to access the Internet and available payment options, fraudsters will quickly find the weakest entry point and shift direction. Thus, training should be designed to evolve with these shifting risks. According to the Global Economic Crime Survey conducted by PwC (PricewaterhouseCoopers), 42 percent of all business organizations admit to having no cybercrime training for employees. Although the majority of respondents cited "face to face" as the most effective form of training when it comes to cybercrime awareness, only one in four had conducted such training, because it is generally time-consuming and more costly to conduct.[16]

Can organizations influence the behavior of employees' electronic habits? Can behaviors learned at work translate into personal computing habits? One study identified that the tone set by the top senior management in the company can help identify and mitigate fraud. Companies that are ingraining a cyber-risk-aware culture and that have a cyber-crisis-response plan are more likely to identify and mitigate behavior that can lead to account takeovers. And, an employee's computing behavior at work translates to personal computing behavior.[17]

A number of steps can be taken to minimize account takeovers. Below are actions that companies, banks, and individuals can take to reduce the likelihood of an attack.

Companies:

- Educate employees repeatedly through multiple channels of communication on the risks of clicking on unknown e-mails, links, or web pages.
- Block employee access to social sites.
- Conduct banking activity on stand-alone computers without access to e-mail or web surfing.

- Align organizational functions such as information technology, internal audit, and the board of directors to instill a cyber-risk culture, including defining who is responsible for what when it comes to cybersecurity.
- Deploy multifactor, multilayer security for access to financial accounts.

Banks:

- Require specific bank-downloaded virus software on client computers prior to engaging in financial transactions (personal and business).
- Require multifactor, multilayer security for access to customer, especially business customer, accounts.

Individuals:

- Use strong passwords and avoid using the same password for multiple sites, especially those where you handle financial transactions.
- Install and maintain malware and virus protection software.
- Avoid conducting personal banking and financial transactions on public computers or through public network sites.
- Cautiously assess before clicking on e-mail links or responding to e-mail or text requests.
- Practice safe Internet surfing.
- Practice safe shopping, and be cautious when entering payment information, including checking to ensure the website has a valid URL.
- Use common sense.

## XI. Financial Institution Communications: Is the Message Loud Enough?

Both consumer and commercial financial accounts can fall victim to account takeovers as fraudsters look for high-dollar targets. The growth of electronic banking through PCs and mobile devices has expanded the opportunities for account takeover crimes.

Financial institutions should be motivated to succeed at educating all clients because of the potential for them to absorb losses for both consumer and commercial clients resulting from fraudulent activities. Some financial institutions offer online access only with required hardware and software solutions, but this approach is not effective should the customer access an account through a mobile device. Customer education is considered to be an effective means to reducing account takeover fraud. But is the educational message reaching the intended audience? A 2012 survey of 5,223 consumers conducted by the Aite Group revealed that 43 percent of U.S. respondents "don't recall receiving any anti-fraud information from 'their' financial institution."[18] Could the shift from paper to electronic communication methods be at fault? Most online banking users no longer receive any physical (tangible)

correspondence from their bank since the "paper opt-out" movement gained momentum. Financial institutions believe they are sending the message and educating their customers, but if the customer never receives the message, then the message is not effective.

## XII. Conclusion

Account takeover attempts are on the rise and will continue to grow. From the criminal perspective, they are financially lucrative, have a low risk of detection and prosecution, and are accomplished easily through adapted scams. In short, criminals are adapting their tools and their behavior, seeking large rewards with relatively low risk.

The methods to perpetrate account takeovers are proliferating. Most often, criminals target victims through "phishing," with mass e-mails disguised to look legitimate, text messages that require a reply, fraudulent attachments, popup menus that appear on computers, or other interactive methods. In addition, DDoS attacks have now been confirmed as distractors while account takeovers occur unknowingly to the victim.

The number of potential targets for attack is also growing. The explosive use of the smartphone has provided an additional opportunity for fraudsters to gain access to personal accounts. With statistics confirming that users are more likely to click on attachments on a smartphone, the likelihood for a successful attack may be higher when the attack takes place through a smartphone. It is the unsafe behavior of individuals as well as the plethora of information available on social media sites that can assist fraudsters.

Businesses are increasingly becoming victims as fraudsters look for higher-balance alternatives and as the use of personal devices in the workplace—"bring your own device," or "BYOD"—have blurred the boundaries between business and personal space. Companies should be motivated to educate their employees to reduce their own risk of loss. They already have the authority and relationship with employees as well as the communication platform to provide the education. Financially, the stakes are greater for businesses than for the consumer because of the businesses' lack of liability protection under Regulation E.[f]

[f] Regulation E provides a basic framework that establishes the rights, liabilities, and responsibilities of participants in electronic fund transfer systems such as automated teller machine transfers, telephone bill-payment services, point-of-sale terminal transfers in stores, and preauthorized transfers from or to a consumer's account (such as direct deposit and social security payments). The term "electronic fund transfer," or EFT,

Financial fraud is as prevalent among the elderly as it among youth. Educating all generations will ensure that the message of Internet safety is spread among all potential users, although the form of that education will vary from one segment to the other. Other venues, such as schools and senior centers, can and should play a role in Internet safety education to reinforce the message or even extend the message to those whom banks might not reach.

Software companies, handset manufacturers, and telecommunication providers should also be motivated to mitigate fraud because their products are used in committing fraud. Mitigating fraud removes barriers to the uptake of their products. These products can also be used as a platform to provide education.

While technology can help deflect the attacks, no amount of technology solutions will suffice if they are not used or are used incorrectly. Preinstallation of antivirus software on mobile devices can help, but education is still a fundamental step in preventing account takeovers. Although most financial institutions acknowledge that education is an important service for their customers, the education that most of these institutions offer thus far has not been highly effective, based on the continued risky behavior of consumers and business customers as well as reported statistics showing that fraud efforts are proliferating and account takeovers are growing. The number of account takeover attempts reported at 100 financial services firms surveyed increased from 87 in 2009 to 314 in 2011.[19] With mitigating financial fraud as the goal, banks should be motivated to provide education and are in a position of trust to communicate with their customers.

Elimination of account takeovers is unlikely, as the rewards will continue to outpace the consequences. However, the magnitude and frequency can be reduced as a result of collective education practices. With the combined efforts of financial institutions, businesses, schools, software companies, and telecommunication providers, to name a few, the goal to reduce account takeovers while enhancing online electronic habits could be achieved.

---

generally refers to a transaction initiated through an electronic terminal, telephone, computer, or magnetic tape that instructs a financial institution either to credit or to debit a consumer's asset account.

## XIII. Endnotes

[1] "Account Takeover Activity," Department of the Treasury Financial Crimes Enforcement Network advisory notice (FIN-2011-A016), December 19, 2011.

[2] *2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters*. Javelin Strategy & Research, February 2013.

[3] "World Internet Usage and Population Statistics: June 30, 2012," Internet World Stats, www.internetworldstats.com/stats.htm.

[4] "The Shift in Small Business Behavior: 90 Percent Networking Online, According to Manta Survey," Manta press release, September 12, 2012.

[5] Benson, Carol C. and Scott Loftesness. *Payment Systems in the U.S.: A Guide for the Payment Professional*. Glenbrook Partners, 2010.

[6] Inscoe, Shirley W. *Global Consumers React to Rising Fraud: Beware Back of Wallet*, a report on the Global Card Fraud Survey, ACI Worldwide and Aite Group LLC, October 2012.

[7] See note 2.

[8] World Bank, "Mobile cellular subscriptions," search.worldbank.org/data?qterm=mobile%20subscribers&language=EN.

[9] Fortinet, *2013 Cybercrime Report: Cybercriminals Today Mirror Legitimate Business Processes*, www.fortinet.com/sites/default/files/whitepapers/Cybercrime_Report.pdf.

[10] Krebs, Bryan. "DDoS Attack on Bank Hid $900,000 Cyberheist," *Krebs on Security*, krebsonsecurity.com/2013/02/ddos-attack-on-bank-hid-900000-cyberheist/.

[11] Honan, Mat. "How Apple and Amazon Security Flaws Led to My Epic Hacking." *Wired Magazine*, August 6, 2012.

[12] Scott, Cameron. "Nearly a Fifth of U.S. PCs Have No Antivirus Protection, McAfee Finds." *PC World*, May 29, 2012.

[13] *Cybercrime: Protecting Against the Growing Threat*. PwC, November 2011.

[14] *The Year in Phishing*, RSA Fraud Report, January 2012, www.rsa.com/solutions/consumer_authentication/intelreport/11635_Online_Fraud_report_0112.pdf.

[15] "Mobile Security Software—What It Must Do," Kasperksy Lab, June 6, 2011, newsroom.kaspersky.eu/en/texts/detail/article/mobile-security-software-what-it-must-do.

[16] See note 13 above.

[17] Marks, Jonathan. "Putting the Freud in Fraud: Why the Fraud Triangle Is No Longer Enough." Crowe Horwath webinar, March 7, 2012, www.crowehorwath.com/freud_fraud/.

[18] See note 6 above.

[19] "Chubb Cyber Endorsement Addresses Increase in Bank Account Takeover Frauds," Chubb Group of Insurance Companies press release, December 11, 2012.