IEEE SECURITY & PRIVACY

PEER REVIEWED

November/December 2012 (Vol. 10, No. 6) pp. 63-69
1540-7993/12/$31.00 © 2012 IEEE

Published by the IEEE Computer Society

Is Everything We Know about Password Stealing Wrong?

Dinei Florêncio , Microsoft Research

Cormac Herley , Microsoft Research

ABSTRACT

Passwords are but one link in the cybercrime value chain. Contrary to popular belief, compromised users are made whole and thieves have a hard time monetizing stolen credentials.

It's not what you don't know that kills you, it's what you know for sure that ain't true.
—Mark Twain

It is worth, at the outset, dispelling a widely held misapprehension about password stealing. Thieves certainly steal passwords, and money is certainly a large part of their motivation. However, when they successfully extract money from financial accounts, individual consumers do not pay. In the US, Federal Reserve Regulation E limits consumer liability to US$50 in the event of fraud (this is separate from Regulation CC's $50 limit for credit card fraud) and covers "any electronic transfer that is initiated through an electronic terminal, telephone, computer or magnetic tape." [1] This regulation governs banks, brokerages, and credit unions, and many organizations go beyond it and offer consumers a zero-liability policy.

Bank of America, for example, "guarantees zero liability for any unauthorized activity

originating from Online Banking or Bill Pay." [2] Wells Fargo says, "We guarantee that you will be covered for 100 percent of funds removed from your Wells Fargo accounts in the unlikely event that someone you haven't authorized removes those funds through our Online Services." [3] Fidelity "will reimburse your Fidelity account for any losses due to unauthorized activity," [4] and "under HSBC's $0 Liability, Online Guarantee, you're covered 100% and liable for $0." [5] Even nontraditional financial institutions offer this guarantee. For example, in eBay's December 2009 10-K filing, the company states, "PayPal currently voluntarily reimburses consumers for all financial losses from transactions not authorized by the consumer, not just losses above $50." [6]

Thus, in the US, individual consumers are largely insulated from the direct financial consequences of credential theft (we later briefly mention losses of small businesses and indirect losses). (Although consumer protections in the US are good, they are by no means unique. EU Directive 2007/64/EC of the European Parliament limits consumer liability to €150, and many banks go beyond this. Mannan and van Oorschot found that most major Canadian banks offer a "100% reimbursement guarantee for online banking fraud losses," but they also suggest that most consumers are unlikely to meet the standard of care required to be eligible. [7]) Consumers who have their accounts emptied through stolen credentials are made whole. Of course, the cost of the fraud does not just go away: covering fraud is a cost that gets passed back to consumers in the form of increased fees. However, the idea that consumers are "just a few clicks away" from having their accounts irretrievably emptied is simply incorrect. There is a world of difference between being personally liable for losses and sharing losses that are diluted across the whole population. Although "we all pay for cybercrime" is true in a general sense, individual users do not face grave financial risk.

We begin with this misconception because it is widely held and generates enormous confusion. Regulation E also has far-reaching consequences for who loses money, how much is lost, and where the bottle-necks lie in the password-stealing pipeline. Although Regulation E is not secret and occasional references to it have appeared, [8], [9] its implications are seldom pursued in the academic security literature.

For fear of misunderstanding, it is worth explicitly stating that we limit the scope of our remarks in this article to financially motivated password-stealing attacks against the bank accounts of US consumers. We do not examine password theft from email or social networking sites. We do not explore other aspects of cybercrime. We touch only briefly on nonconsumer losses and make no mention of corporate accounts or other vital assets protected by passwords.

Although we make no claim that our conclusions generalize beyond banking losses to US consumers, this case is large enough to be interesting and instructive. Online banking is done almost exclusively with passwords in the US. Thus, using what might be considered the lower bound in terms of security, US banks offer the upper bound in protection: zero liability. Anderson observed that although dumping liability on consumers is far more common in the UK, this has not resulted in less fraud or savings in the amount spent on security. [10]

Does it Still Exist?

Monday, Feb 18, 2013

In the wake of the Yahoo password breach, I scratched my

Emptying Accounts Is Hard

Back to Top

The fact that US banks offer zero liability lets us infer much about losses and the fraud protection mechanisms in place. We now argue that Regulation E implies that emptying accounts is far from simple.

Once a thief has stolen passwords, he or she needs a way to transfer money from victim accounts. This must be irreversible and ideally should be untraceable. There is little point in doing the transfer if it can be rolled back, and there is high risk if it leaves a trail that leads to the thief's door. We now argue that this is hard. Suppose that this isn't the case. That is, suppose that doing irreversible untraceable money transfers from a bank account (armed only with a password) is easy. If so, this opens an enormous vulnerability to self-theft. Any Internet banking user can transfer his or her money to another account (that he or she controls), then claim fraud and demand reimbursement. Repudiation is easy if the transfer is untraceable. The money cannot be recovered if the transfer is irreversible. Regulation E compels the bank to make the (dishonest) customer whole.

However, getting away with this scam is not as easy as it looks. Banks cannot allow easy repudiation of irreversible transfers for which they have offered zero-liability guarantees. They must be able to distinguish fraudulent transfers initiated by a thief and repudiated transfers initiated by the account holder. Otherwise, every customer can commit fraud without even needing to steal a password. It is sufficient that this determination can be made after the fact if the account holder tries to repudiate the transfer. For example, repudiation of an ATM cash withdrawal requires that the account holder is not captured by the ATM camera and has a plausible argument as to how the thief acquired both the card and PIN. Repudiation of an online transfer requires that the receiving account cannot be linked to the customer.

Ideally, this is done with a "John Doe" stepping-stone bank account that can be used to relay money to cash. However, anti-money-laundering provisions of the Bank Secrecy Act (1970) and Title III of the USA Patriot Act (2001) make setting up a bank account under an assumed name difficult. To comply with these laws' customer identification provisions, US banks require a government-issued ID, a Social Security number, and an in-person appearance at a (generally camera-monitored) bank branch to open an account. Most banks consult the ChexSystems database—a catalog of the disputed transactions and checks that consumers have bounced—before opening a new account.

Documents can be forged, but these defenses increase the effort, expense, and risk. They also limit the throughput—accounts that receive fraudulent transfers are frozen quickly and cannot be used further. So, at scale, this approach to fraud requires not one or two John Doe accounts, but many. If a thief can clear five transfers through an account before it is frozen, he or she requires one-fifth as many accounts as stolen credentials.

Krebs has documented a number of thefts from small businesses; these stories make clear that banks have considerable success in reversing transfers. For example, of $2

million stolen from Global Title Services, $1.8 million was reversed; of $217,000 stolen from the Metropolitan Entertainment & Convention Authority (MECA), $147,000 was reversed; of $1.9 million stolen from Experi-Metal, $1.34 million was reversed; of $110,000 stolen from United Way of Massachusetts Bay, all was blocked or reversed; and of $801,495 stolen from Hillary Machinery, $600,000 was reversed. [9] Because small businesses typically have a greater number and diversity of transactions than consumers do, fraud is almost certainly far harder to detect there. That emptying accounts is hard is further corroborated by the observation that stolen credentials are offered for sale on underground markets at fractions of a penny on the dollar. [11], [12]

This analysis assumes that fraudulent transactions are noticed and reported. For large transfers, this seems safe: we assume that few consumers would fail to notice a $10,000 transaction. But what of smaller amounts? Is it easier to avoid detection if a thief makes many small transfers? We argue that this is unlikely. Suppose a thief does many $10 transfers. If p is the probability of any individual transfer being detected, then to have a 50 percent chance of extracting $10,000, the thief needs $(1 - p)^{1000} > 0.5$. This gives $p < 0.0007$, meaning that the chance of each transfer being detected should be lower than 0.07 percent. Attempting large transfers seems the better approach.

The different procedures and legal status involved also suggest that banks understand nonrepudiation and are keenly aware of the different risks posed by reversible and irreversible transactions. If banks are to protect themselves, irreversible transactions must be hard to repudiate. Western Union transfers and cashier checks are inherently irreversible but require in-person appearance, presentation of ID, and a signature (and are not covered by Regulation E). ATM withdrawals are covered, but because they require a two-factor authentication—possession of a card and knowledge of a PIN—at a camera-protected machine, they are hard to repudiate. Getting cash in exchange for a check is extremely difficult unless the recipient has an account at the bank, in which case, the bank knows whom to debit if things go wrong. Any transfer that requires only a password to initiate is easy to repudiate. If it is covered by Regulation E, it must also be reversible.

We assume that banks do not simply transfer funds covered by Regulation E and hope for the best. US banks handled approximately 100 million checks and 75 million automated transfers per day in 2009. [13] They are very familiar with fraud, money laundering, check washing, counterfeiting, the possibility of insufficient funds, and counter-party risk. They also know that once they hand over cash, any subsequent problem becomes their problem. They limit their risk by offering zero liability only when they can reverse an easily repudiated transaction.

Mules, Not Victims, Lose Money

Back to Top

It is difficult to get a bank to transfer money irreversibly in a way that can later be repudiated. And password-enabled transfers can always be repudiated. Thus, password thieves have a problem: as things stand, the fruits of their labor are worthless. They can see the money; they just cannot get it out in a way that ensures that it stays out.

Thieves respond by taking to heart a wise saying attributed to Butler Lampson: "Every

problem in computer science can be solved by adding another layer of indirection." Rather than incur the effort, expense, and risk of opening John Doe accounts, thieves simply enlist others who already have accounts. The solution is to use a human proxy, convincing someone with rather less fraud experience than a bank to act as a relay. It is largely for this reason that draining accounts is usually done through *money mules*.

The money mule's role is to turn a traceable, reversible transaction into an untraceable, irreversible one. [14] Using a stolen password, the thief transfers money (traceably and reversibly) to the mule's account using, for example, online bill pay. On receipt, the mule sends this money (untraceably and irreversibly), minus a "commission," to the thief. By using, for instance, Western Union for this transfer, the mule has made it irreversible and untraceable. By authorizing the withdrawal with a signature, the mule gives up any ability to repudiate. The mule has thus given up any consumer legal protections that he or she might have enjoyed. The mule accepts a bad transfer and initiates a good one.

Consider a fraudulent transfer of $9,000 from a compromised account. Using online bill pay, the thief sends $9,000 from the victim's account to the mule. The mule sends $8,100 to the thief and keeps a $900 commission. Once fraud is discovered, the victim is reimbursed, and reversal is attempted from the mule account. Thus, before discovery, the victim, mule, and thief have gains of –$9,000, $900, and $8,100, respectively. After discovery and reimbursement, they have $0, –$8,100, and $8,100, respectively.

Notice that the thief is up precisely the amount that the mule is down (or in debt). The thief is really stealing from the mule, not the compromised account, although this fact does not become clear until the dust settles. Thus, money mules are not merely unwitting accomplices; they are the true victims in credential-theft fraud. Their accounts are not simply vital stepping stones in the evacuation of funds; their accounts (not the victims') are the ones being pillaged. If the transaction cannot be reversed (for example, the mule has insufficient funds), then the bank (either the victim's or the mule's) is left with uncollectible debt.

If the thief really steals from the mule, why does he or she need the original victim account? Recall that victim-to-mule transfer was necessary to create the illusion of a legitimate task for the mule and the temporary availability of funds for the critical mule-to-thief transfer. Thieves recruit mules with semiplausible stories of work-at-home schemes. Often, the mule is led to believe that this is a real job acting as clearing agent or account manager for a foreign firm, or as a secret shopper. Transfers just below $10,000 are the most popular amount (transfers above $10,000 require a Currency Transaction Report under the Banking Secrecy Act), and Western Union and MoneyGram are popular payment channels. [8] That all transactions must be handled with urgency is, unsurprisingly, a common theme.

Passwords Are Not the Bottleneck

Back to Top

If emptying accounts armed only with a password is hard, then are passwords truly the keys to the kingdom? There is ample evidence that passwords are being stolen at a

considerable rate. Holz and colleagues discovered 10,770 banking passwords in a seven-month examination of key-logger drop zones (locations where key loggers send their findings for later collection by the thief). [15] Brett Stone-Gross and colleagues found 8,310 in a 10-day examination of the Torpig botnet (an annualized rate of 303,000). [16] RSA found nearly 300,000 banking credentials in an examination of the Sinowal Trojan. [17] The Zeus botnet, which some accounts credit with infecting more than 3 million machines, has financial-data theft as one of its primary goals.

Theft of non-financial -credentials occurs at even greater rates. In the last two years, numerous organizations, such as Rock-You, Gawker, and even IEEE, have had leaks of thousands or even millions of user passwords. Many claim that these nonfinancial credentials can be leveraged to access more valuable accounts.

So, banking passwords are being stolen in considerable numbers. We have seen that emptying accounts is hard and that mules, not victims, lose money. The password merely provides a way to offer something of apparent value (the victim-to-mule transfer) that will persuade the mule to part with something of real value (the mule-to-thief transfer). The victim's password is only one small part of the elaborate process of socially engineering the mule into parting with money.

If passwords are not the bottleneck, what is? Back-end fraud detection by banks is a good candidate. This reduces the number of compromised accounts that can be emptied. Mule recruitment is another good candidate. Studies of underground-economy markets indicate a great demand for mules. [11], [12] Cisco's 2010 Annual Security Report claimed that "the ratio of stolen credentials to available mule capacity could be as high as 10,000 to 1." [18] The RSA blog put it succinctly: "no mules = no cash." [19] Krebs, who claimed to have interviewed more than 150 money mules, said, "most money mules get a single transfer" and "each mule is worth slightly less than $10,000 to the cyber gangs." [9] It is difficult to imagine mule recruitment keeping pace with the current level of credential theft. Annualized, the Torpig data alone (that is, one botnet) would imply the need for a third of a million mules (at Krebs's estimate of one transaction per mule). [9], [16]

Underground Markets Are Not Thriving

Back to Top

The cybercrime underground economy is often portrayed as a criminal utopia, rivaling aboveground markets in activity and sophistication. Some claim that illicit goods trade freely and that great specialization exists. [11], [12] These accounts suggest that some black marketeers offer credentials for sale, some offer kits, and newcomers can buy what they need and sell what they produce.

However, the parallels between aboveground and underground economies go only so far. One major point of difference is price—credentials are apparently offered for sale at pennies on the dollar in underground markets. [11], [12] Thomas and Martin reported that credentials of $10 million face value were offered for $500. [11] Symantec reported that accounts that it estimated as being worth $5.3 billion were offered for $163 million. [20] This is enormously puzzling if cashing out is simple. Why would anyone sell credentials

that unlock an account with a $5,000 balance for $5? It makes much more sense if emptying accounts is hard and stealing passwords is merely the first step in a difficult, error-prone process that only occasionally succeeds. [21] If credentials are offered for sale at 5 percent of face value (this is a loose upper bound on the asking price [11], [12], [20]), then 5 percent of the value goes to the person who steals the password and 95 percent goes to the person who empties the account. This shows that emptying the account is by far the more valuable task. It defies common sense that those who steal passwords would give up 95 percent of the finished product's value if they had any means of obtaining the money themselves.

In the chain of events that begins with stealing a password and ends with the untraceable, irreversible receipt of cash, passwords are merely one raw material that goes into the creation of the finished product. Every transaction requires a mule who is recruited and socially engineered into laundering the transaction. Although passwords can be stolen on an industrial scale, the same does not appear to be true of mule recruitment. The premium that emptying accounts enjoys shows that passwords are largely a commodity. This suggests that only a small fraction of stolen banking passwords result in the successful extraction of money. If mules are scarce and stolen passwords are plentiful, then only the best prospects among the compromised accounts will be selected for evacuation.

What of the reports of easy money being made in underground markets? As far as we are aware, no published account has claimed to have observed a single transaction closing or a single dollar changing hands in underground markets. [21] The observations we have are of offers to buy and sell. [11], [12] Reports that banking credentials are selling for $10 [20] do not mean that any transaction at that price has actually bween observed. It merely means that at least one person who claimed to have those credentials offered to sell at that price at least once. Participants are anonymous, posting is free and can be automated, cheating is easy and common, [16] and there is no contract enforcement. There is little to prevent cheating and every incentive to deal dishonestly.

It is fair to say that many people in Internet chat rooms, bulletin boards, and dating sites do not represent themselves truthfully. There is no reason to believe that this should be better in underground markets, and many reasons why it might be worse. We simply have no idea what fraction of advertised transactions close. We have no idea what fraction represent real credentials as opposed to boastful claims, repeat sales, or attempts to cheat. Thus, estimating cybercrime by taking activity on these channels at face value is, to put it no stronger, unsound. The view that underground markets are an easy-money utopia is based on a rather credulous interpretation of the observations. Rather, we suggest, it is the dumping ground for unused (and, in many cases, unusable) credentials that have little value.

Credential Stealing Is a Terrible Business

Back to Top

Suppose we ignore the illegal and unethical nature of credential stealing and evaluate it strictly as a business prospect. Is this a business with some intrinsic durable competitive advantage, as Munger says that Berkshire-Hathaway demands of an investment? The

advantages have been discussed often: stealing can be done remotely, it can be automated, little training or capital outlay is required, and prosecution is extremely rare. Almost anyone can do it. The popular and trade presses frequently run stories telling of easy cybercrime riches.

Yet, there are also disadvantages. First, no barrier to entry exists; there is open access to the opportunity. New entrants keep arriving as long as the opportunity is profitable, which leads to the tragedy of the commons. [22] If a fixed pool of money is shared among many thieves, the average return drops as more thieves arrive. This continues until the opportunity is no better than those elsewhere. However, the pool does not remain fixed; it shrinks as a consequence of the thieves' effort. When stealing becomes common, countermeasures increase: browsers deploy phishing warnings and blacklists, service providers remove malicious sites more quickly, and banks place increased effort on back-end fraud detection. A steady stream of phishing emails might alert even unsophisticated users to the phenomenon. The average return thus has an increasing denominator (thieves continue to arrive) with a decreasing numerator (the pool shrinks).

There is no protection for intellectual or other property. Successful innovations are quickly copied by others, limiting their value to the originator. There is no lock-in, brand loyalty, or other factor that helps maximize revenue from a customer. So, stealing credentials meets none of Munger's criteria. When competitive advantages arise, they are neither intrinsic nor durable, and the pace of change is relentless. Finally, no contract enforcement exists. Credential-stealing businesses cannot rely on even the most basic tool of commerce. Therefore, dishonesty is a way of life, and dealing with anyone you do not know personally is fraught with risk. The lack of such a mechanism poses a profound difficulty in the development of a mature economy. [23] None of the ingredients that we typically associate with good businesses are present.

What of the market size? How big a pot of dollars is shared among password-stealing thieves? As we have shown, in the consumer space, Regulation E implies that it is not victims who lose money but mules. Rather than targeting the account balances of all Internet users, credential stealers are taking from those who can be persuaded to act as human relays. This is a small fraction of the population and almost certainly concentrated among the poorest. This considerably limits the opportunity. We show elsewhere that widely circulated estimates that place cybercrime losses in the billions are based on bad statistics and are entirely unreliable. [24]

What of small businesses? Their losses are not covered by Regulation E, and they are frequently targeted. Krebs has covered numerous cases of small businesses being successfully attacked. [9] The amounts are larger than in the consumer space, and banks are reluctant to shoulder the losses. Because small businesses have more money than consumers but lack the security and audit controls of large organizations, they might represent the ideal targets for credential-stealing criminals.

Although small businesses are better targets, there are far fewer of them. The US Census

Bureau found that there were 1.25 million businesses with between 10 and 1,000 employees in 2008. [25] This is almost a factor of 200 lower than the number of consumers. If 1 percent of small businesses were successfully targeted annually, and the average haul was $10,000 (that is, the maximum amount to avoid a transaction report, and the average amount that Krebs claims a mule is worth), this opportunity would be $125 million. Although by no means small, this is a long way from the billion- or even trillion-dollar losses that password stealing is often claimed to generate.

Finally, to avoid mule recruitment and other scams, users are often cautioned that "if it sounds too good to be true, then it is." This is sensible advice. However, it is no less sensible in examining the plausibility of stories of cybercrime riches. It is naive, indeed, for a user to believe that a stay-at-home job requiring no training, skill, or experience will pay handsomely. However, it is no less naive to believe that a cybercrime job requiring no training, skill, or experience will do the same. It makes no sense that a script downloaded from the Internet can generate a steady stream of income. It defies common sense that "those without great skills can barter their way into large quantities of money they would never earn in the physical world." [4] Legal or not, aboveground or below, the demand for easy money seems likely to always exceed the supply. It is ironic that the magical thinking that we caution users against in their online affairs is baked into the consensus view of password stealing.

The Indirect Costs

Back to Top

In July 2009, a teller at a Key Bank branch in Seattle pursued a would-be robber after a botched holdup attempt. [26] He leapt over the counter, chased the man for several blocks, knocked him down, and held him until the police arrived. Two days later, Key Bank fired the teller. He had violated long-standing bank policy to cooperate in every way and never resist a robbery.

We suggest that the reason for this policy is that banks understand a very simple principle: fear is bad for business. It is far better to comply with the demand than to risk a brawl or gunfight in the bank lobby. No bank wants the perception that it valued money more than customer and employee safety. The $40 million that traditional bank robbers in the US steal per year is entirely manageable. Similarly, Regulation E and zero-liability guarantees are not the result of altruism; they are just good for business. Limiting consumer liability lessens the anxiety about banking online. It costs little if covered repudiable transactions are reversible.

The idea that consumers are just a few clicks away from grave financial harm makes a compelling narrative, but it is simply incorrect. However, this does not mean that password stealing is a minor problem. The indirect costs of cybercrime almost certainly dwarf the direct losses by orders of magnitude. Although password-stealing victims are spared direct losses, they might spend considerable time and energy resolving the mess. Mules bear the full brunt of successful cash-out operations and are probably least able to handle the losses. The entire Internet-using public pays an enormous indirect cost in being compelled to adopt security measures that would not otherwise be necessary. Those who have had an email password stolen to send spam know what a miserable

experience that is, and it is little consolation to hear that the hacker probably earned very little.

We acknowledge that the picture we paint in this article is not a proof; we present it as a plausible, rather than definitive, explanation of observations. However, the conventional view appears to require that banks do not understand the importance of non-repudiation. We suggest that our view is far more consistent with what we know.

Our challenge to the conventional view also raises interesting questions. First, if passwords are not the bottle-neck, would replacing them or making them harder to steal have any influence on the total harm done by credential thieves? If a large lake of credentials is drained by a narrow pipe of mules, reducing the inflow to the lake might have no effect on the net harm done. Enormous energy has been devoted to replacing passwords with something more secure. Yet, no clear picture exists of how much harm this would eliminate.

Second, some people assume that banks want to pass the liability for fraud to consumers. Is this really so? If emptying accounts is hard, then credential theft losses might be far smaller than imagined, and borne by mules rather than banks. When perceived risk is greater than actual risk, it can be profitable to absorb the risk and charge for it. Rental car companies are not merely willing, but anxious, to accept liability for any damage to the car for $35 per day; various companies aggressively market identity theft protection for $12 per month. Banks enjoy a huge information advantage over consumers: they know how much fraud costs them, whereas consumers merely hear horror stories of cybercrime losses. [22] Passing the liability to consumers (as Anderson argues UK banks do [10]) would seem to be wasting a profitable opportunity.

Finally, many suggest that the switch in recent years from hacking for sport to hacking for financial gain represents an extremely serious escalation. This is sometimes offered as evidence that users must finally get serious about security, banks should eliminate passwords, and so forth. We offer the somewhat provocative thought that this switch is good news, not bad. The banking system has been hardened by centuries of exposure to fraud and money laundering. In spite of the enormous effort devoted to password stealing, banks offer zero-liability guarantees to customers and keep losses manageable. A fixed population of hackers will almost certainly do less harm by attacking hardened targets such as banks than if they applied the same energy elsewhere. Getting in and getting out with money is a far harder problem than simply causing destruction. If the goal were mayhem and destruction rather than moneymaking, we might be a great deal worse off.

We thank the anonymous reviewers and Joseph Bonneau, Paul C. van Oorschot, and Frank Stajano for comments that helped improve the article.

References

1. “Part 205: Electronic Fund Transfers (Regulation E),” US Nat'l Archives and Records Administration, 2011; www.fdic.gov/regulations/laws/rules6500-3100.html .

2. “Banking Solution: Zero Liability Guarantee,” Bank of America, 2005; www.bankofamerica.com/onlinebanking /real_banking_soln/ noflashrobert.html.

3. “Online Security Guarantee,” Wells Fargo, 2012; https://www.wellsfargo.com/privacy_security/ onlineguarantee.

4. “Fidelity Customer Protection Guarantee,” Fidelity, 2012; https://401k.fidelity.com/public/content/ Shared/SecurityProtectionGuarantee.

5. “HSBC's Personal Internet Banking Security Pledge,” HSCB, 2012; www.us.hsbc.com/1/2/home/personal-banking/ pibonline-guarantee.

6. “United States Securities and Exchange Commission Form 10-K, eBay Inc.,” no. 000-24821, 2009; www.sec.gov/Archives/edgar/data/1065088/ 000119312510033324d10k.htm.

7. M. Mannan and P.C. van Oorschot, “Security and Usability: The Gap in Real-World Online Banking,” *Proc. New Security Paradigms Workshop* (NSPW 07), ACM, 2007; www.ccsl.carleton.ca/paper-archivemannan-nspw07.pdf .

8. R. Stross, “Don't Take This Bait (but You're Safe If You Do),” *The New York Times*,28 Nov. 2009; www.nytimes.com/2009/11/29/business29digi.html .

9. B. Krebs, *KrebsonSecurity,* blog; http:/krebsonsecurity.com.

10. R. Anderson, “Closing the Phishing Hole—Fraud, Risk and Nonbanks,” *Proc. Federal Reserve Bank of Kansas City Conf. Nonbanks in the Payments System,* 2007; www.cl.cam.ac.uk/~rja14/Papersnonbanks.pdf .

11. R. Thomas and J. Martin, “The Underground Economy: Priceless,” *;login:,* vol. 31, no. 6, 2006, pp. 7–16; http://static.usenix.org/publications/login/ 2006-12/openpdfscymru.pdf.

12. J. Franklin et al., “An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants,” *Proc. ACM Conf. Computer and Comm. Security* (CCS 07), ACM, 2007, pp. 375–388.

13. “The 2010 Federal Reserve Payments Study: Noncash Payment Trends in the United States: 2006–2009,” US Federal Reserve System, Dec. 2010; www.frbservices.org/files/communications/ pdf/press2010_payments_study.pdf.

14. D. Florêncio and C. Herley, “Phishing and Money Mules,” *Proc. 2010 IEEE Workshop Information Forensics and Security* (WIFS 10), IEEE, 2010; http://research.microsoft.com/pubs/143095 mules.pdf.

15. T. Holz, M. Engelberth, and F. Freiling, *Learning More about the Underground Economy: A Case-Study of Keyloggers and Dropzones*, tech. report TR-2008-006, Reihe Informatik, 2008; http://honeyblog.org/junkyard/reportsimpersonation-attacks-TR.pdf .

16. B. Stone-Gross et al., “Your Botnet Is My Botnet: Analysis of a Botnet Takeover,” *Proc. ACM Conf. Computer and Communications Security* (CCS 09), ACM Press, 2009, pp. 635–647.

17. “RSA Online Fraud Report,” RSA, Oct. 2008; www.rsa.com/solutions/consumer_authentication/ intelreportFRARPT_DS_1008.pdf.

18. “Cisco 2010 Annual Security Report,” Cisco, 2011; www.cisco.com/en/US/prod/collateral/vpndevc security_annual_report_2010.pdf.

19. RSA FraudAction Research Labs, “Follow the Money, and Go for the Mules!” blog, 6 Oct. 2010; http://blogs.rsa.com /rsafarlfollow-the-money-and-go-for-the-mules .

20. “Symantec Internet Security Threat Report: Trends for January–June 07,” white paper, Symantec, Sept. 2007; http://eval.symantec.com/mktginfo/enterprise/ white_papersent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf .

21. C. Herley and D. Florêncio, “Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy,” *Workshop on Economics of Information Security,* 2009; http://research.microsoft.com/apps/pubs?id=80034 .

22. C. Herley and D. Florêncio, “A Profitless Endeavor: Phishing as Tragedy of the Commons,” *Proc. New Security Paradigms Workshop* (NSPW 08), Assoc. Computer Machinery, 2008; http://research.microsoft.com /apps/pubs?id=74159 .

23. A. Greif, “Contract Enforceability and Economic Institutions in Early Trade: The Maghribi Traders' Coalition,” *American Economic Rev.,* vol. 83, no. 3, 1993, pp. 525–548.

24. D. Florêncio and C. Herley, “Sex, Lies and Cyber-Crime Surveys,” *Workshop on Economics of Information Security,* June 2011; http://research.microsoft.com/apps/pubsdefault.aspx?id=149886 .

25. “Statistics about Business Size (Including Small Business)from the U.S. Census Bureau,” US Census Bureau, 2012; www.census.gov/econsmallbus.html.