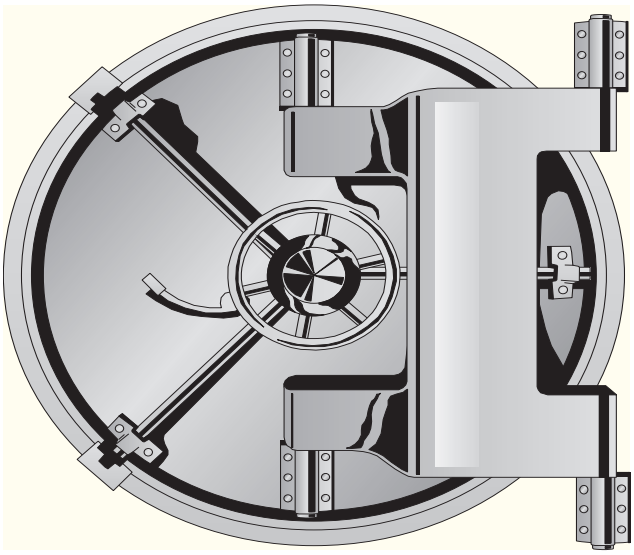
Wealth Creation

. . . and Preservation

3rd Quarter 2006 | Special Report | $25.00 per copy

PRESERVING YOUR



PRIVACY

IN THE INTERNET AGE

It doesn't really matter how much money you have if someone can quickly take it away from you. In our day of high security, gated communities, and 128-bit encryption it is astonishingly easy to steal another person's possessions, savings, and identity. This issue is devoted to helping you avoid many of the common mistakes people make in compromising their financial security.

The Internet has literally changed everything related to personal finance. There is vastly more information available today than ever before, and it is literally "at our fingertips". In fact, "information overload" often leads to "analysis paralysis" because we simply have too much information to deal with. Not all the information on the Internet is correct or even useful, and sifting through it can be very time-consuming.

When I first received my MBA in 1978 I went to work for a national service bureau company which was selling computer timesharing services. Their mainframe computers, each of which was far less powerful than a bottom-line Pentium computer today, were located in a secure and nondescript location somewhere in Ohio. Their primary concerns were physical security, and they used a system of encoded badges to restrict access. There was little concern about the security of data transmission because the technology was new and there were no hackers. All data was transmitted via phone lines and dial-up modems. Remember, at the time the Internet did not exist, and neither did ATM machines or personal computers. In fact, it was there in San Francisco that I saw the first store open to sell Apple computers in 1979.

As data transmission improved financial institutions began sending more and more information over phone lines. Once the Internet was developed and popularized it began to replace telephone transmission. Improved internet technology, Windows and personal computers made it less and less expensive to operate online, until a few years ago virtually all personal financial information became available online or, if not made available, could be hacked into by using the Internet to access the company's mainframe computers. Credit cards created just that much more personal information which could be retrieved either for legitimate purposes or for criminal activity.

Today, whether you have a personal computer and access the Internet or not, much of your personal information is available to you and others on the Internet. That means that you can be victimized by thieves on the other side of the planet or right next door, thieves who can gain power over all your finances and your life. You have probably read more than one story of how an unsuspecting person has lost a job, a drivers license, medical insurance, savings and investments, his home, or something else of value. The stories are true, and the real danger is exacerbated by both the laws designed to protect our privacy and those designed to invade it.

Typical stories of identity theft

I recently received a letter from the VA via the IRS about a VA employee who took home personal data for up to 26.5 million veterans and some spouses. The employee's home was burglarized and the data stolen. All 26.5 million of us are directed to be especially cautious about our financial affairs - for the rest of our lives, I assume.

Here are some other examples of what has been happening in recent months:

A hacker broke into the California state controller's computer system and gained access to the names and Social Security numbers of 265,000 state employees — including elected officials.

Earlier this year a hacker accessed 8 million credit card numbers by breaking into the database of a company that processes transactions for Visa, MasterCard, American Express and Discover. The credit card companies said there was no evidence the numbers had been used for fraudulent purchases, but people don't steal data without the intent of using it or selling it. It's always good to watch for updates on these stories, like these:

Thieves posing as Ford Motor Credit Co. personnel accessed a credit bureau database and stole credit reports of more than 30,000 consumers. The U.S. Attorney's Office in New York said its investigation uncovered more than $2.7 million in financial losses.

A clerk of New York state's Insurance Fund was arrested for using others' personal financial information to set up credit accounts and purchase more than $100,000 worth of goods, including $70,000 in computers.

Thousands of incidents like these have been reported to the news services, and a few have found their way into newspapers and TV. However, most companies do not disclose such thefts unless they are required to. Many companies do not

encrypt their data, and finding which ones do can be very difficult. Some firms can not tell when their systems have been compromised and information stolen.

How it's done

Thieves don't need a computer to steal your personal information. "Dumpster diving" has become a common pastime. Even a credit card solicitation you throw out can be used to steal your identity, which is why I strongly urge all my clients to have and use a cross-cut shredder at home. Please shred *everything* you no longer need that bears your name and address, and anything that might link you to a financial institutions where you do business.

This is where the "paranoia" comes in. In our wonderful, high-tech 21st Century we need to act as if they were out to get us, for they are. It's nothing personal, most of the time; the thieves are not interested in kidnaping because such crime carries a heavy sentence. They can steal or extort as much and more by violating laws with much lesser penalties. Such crimes seldom draw public attention and are far easier to commit. The odds against getting caught and convicted are very high.

How easy is it for someone to rob you today? A waiter who holds your credit card for several minutes out of your sight can do significant damage. Your credit card company probably will not hold you responsible for the charges you did not authorize, but you will have to endure at least the inconvenience of changing account numbers, filing a statement, and checking your credit reports to make sure nothing incorrect has been posted. Keeping your information on any commercial website (retailers, nonprofit organizations, and so on) can be hazardous. Verifying personal information over the phone to a complete stranger who called you is another good way to get yourself into trouble.

One of the most dangerous things you can do with your computer is to open an email message which looks like "the real thing." The simple rule to follow is "when in doubt, throw it out." I occasionally delete legitimate email from clients because I cannot be completely sure about it. Having lost an entire computer and all its data to a virus, I am loath to risk losing another - or worse.

Viruses, spam, "phishing", worms, Trojan horses - they're all put out there to damage your computer, steal your money and your identity. Don't think for a minute that these criminals will ever be caught and punished, because they won't. Even if they were, their friends and relations would continue to use your stolen information. It used to be safe to make an online transaction when you had gone to the company's website, but even that can be perilous because some malicious software can redirect you to a fake site. Oh, and beware of dialing phone numbers with the are code 900 - it can cost you hundreds of dollars a minute, and those bills are legitimate.

If you become a victim, the loss of money or identity (or both) is only the beginning. The process of "clearing your name" and re-establishing your accounts and business relationships is time-consuming and expensive.

Identity Theft Shield

There are products and services that can help prevent identity theft. Most of them are concerned with your credit cards; the best work with all of your personal information including your Social Security number, driver's license number, financial accounts, health records, and your credit card information.

The best service I have found is Identity Theft Shield, a service offered through Prepaid Legal Services. I use Identity Theft Shield myself and offer it to my clients. Please contact me through my website for more information.

Identity Theft Shield is inexpensive and comprehensive. Most important, if your identity is stolen Kroll International, the security firm that offers the service, will do most of the work to set things straight for you. This is very different from what most other services offer.

Building a fortress around your data

What can you do to protect yourself? These ideas are good for starters:

- Buy and use a cross-cut shredder.
- Buy and use good antivirus and internet security software on all your computers. Keep the software current.
- Don't open suspicious emails, and be wary of those that don't look suspicious.
- Never provide information over the phone or over the internet unless you initiated the call or the transaction.
- Sign up for the national Do Not Call list and your state's list, if any.
- Don't get pulled into a conversation with a criminal. Most solicitations sound good at the start, and a personal question comes up early on. If you answer it truthfully, you have already compromised yourself. You do not know how much the caller already knows about you, nor where he got his information.
- When the caller is talking about lowering the interest rate on your mortgage don't tell him your mortgage is paid off or that you don't have a mortgage.
- When the caller says he or she is working for some benevolent association to benefit widows of police or fire personnel, if you have that emotional tug we all get and wish to be charitable you should insist on receiving information about the organization in the mail which you can independently verify. Most thieves will hang up; some of those who do send information in the mail work for themselves, not the nonexistent organization you are reading about.
- When you are offered discounts on the medications you are taking, please don't tell the caller what medications (if any) you are taking.
- Instruct your children about internet and phone security just as you instruct them about strangers who come to the house or hang around the playground.
- Don't store your income tax information at a Website. Don't store <u>any</u> real financial information on a site like msmoney.com.
- Peruse your financial statements regularly to detect fraudulent transactions.
- Change your passwords occasionally. Don't use the same password for each of your accounts. Don't use passwords and numbers anyone who had access to your personal information could guess.
- Use an anti-spyware program (I use Ad-Aware Professional Edition) to detect and remove tracking software that copies your information and sends it on to the thieves.
- Put a security lock (password) on your own wi-fi network, and don't log on to your financial accounts at an Internet café.
- Your phone book residential listing should not include your address.
- Tell telephone solicitors not to call you again. When you do business over the phone, tell the company not to sell your personal information.
- Don't include your telephone number when you complete warranty and registration cards, or in other places. Don't answer any of the marketing questions (especially age and income) on the card.
- Use a credit card for online purchases, not a debit card.
- Try to restrict your online transactions to websites that begin with https://. The 's' means 'secure', as does the closed padlock on the lower right of the screen.
- *Please* don't write your PIN number on your ATM or debit card as so many people do.

Because I signed up for the national Do Not Call list, and because of other laws which are in effect to protect me, most of the telephone solicitations and junk emails I receive are illegal. Unsolicited FAXes are also illegal. However, I am inundated with each of these things every day. Does that give you some idea of how little regard thieves have for the law?