Update
NPMA LIBRARY UPDATE

JAN/FEB
2007

Insert this update into the NPMA Pest Management Library, which can be purchased from the Resource Center. Phone: 703-352-NPMA (6762); Fax: 703-352-3031

The GROWING Threat of Identity Theft

It's All About the Numbers

Identity theft is all about numbers - your birth date, Social Security, credit card and bank account numbers, PINs, and passwords.

"Once a crook has your number," says Michael Weisburger, president of NPMA's endorsed insurer, Weisburger Insurance Brokerage, "he can wipe out your accounts, open new lines of credit, authorize electronic transfers, secure loans, buy property, file for bankruptcy, get fake ID, even get arrested. All in your company's or even your name."

Millions of Americans have their identity stolen every year. You could be next. Why?

More than 100 million data leaks have occurred in the past two years alone — hacked, stolen, lost or otherwise accessed from the government, financial services, health care companies, educational institutions, and general businesses. Those leaks include the names, addresses, Social Security numbers, and other private information on individuals — perhaps you among them, which makes them highly vulnerable to identity theft. For many, it's just a matter of time.

There are other ways that individuals and companies are at risk.

Personal ID Theft

Beyond ill-gotten electronic records, one can simply lose vital personal numbers *physically*. Your wallet or purse could be stolen; your house, auto or company vehicle robbed.

Dumpster divers could rummage through your rubbish, digging out account numbers and other personal info about you. At the ATM, a shoulder surfer might peek over your shoulder as you type in your PIN number. A dodge called skimming could capture your credit/debit card mag-stripe info with a device illegally piggy-backing on that ATM or retail outlet card reader.

Another reasonably simple means crooks use to kidnap identities is the *telephone*.

Example:
A warrant has been issued for your arrest, according to the caller, because you failed to report for jury duty. You protest that you never got the notice. "Mmm, maybe our records are in error; please verify your birthdate and Social Security number."

Or, the "IRS" calls to tell you you're being audited (or are due for a tax refund) and needs you to "confirm the Social Security number we have on record."

Beyond these low-tech tricksters, identity theft nowadays can involve quite a different can of worms, or viruses or Trojan Horses infecting your *computer*.

"Phishing," a mass distribution of spam e-mails, appears to come from legitimate businesses or organizations. The e-mail is meant to trick you into sending personal, financial or security information to authentic-seeming Web sites operated by fraudsters.

To date, roughly a quarter of home computers receive e-mails every month that appear to come from the user's bank or Internet service provider or another real company asking for credit card or other personal info.

Other Examples:

- Brand spam, supposedly from high-visibility logo firms like Wal-Mart or Home Depot or Starbucks, promises a $50 or a $100 shopping card, perhaps, if you'll just click on a link, type in your personal data and take a survey.

- Fake job listings, according to an Internet firm that recently warned millions of its users, are being used to gather and steal personal information from unsuspecting job seekers.

- The lawsuit scam preys on the deep-seated fear most of us have of being hauled into court. When worried victims open the e-mail attachment, malicious code embedded in the text downloads onto their PCs.

- "The ever-popular Nigerian scam offers you an opportunity to make a lot of money by helping the writer, a high-up government official, naturally move millions," Weisburger warns. "All they require is your telephone and fax numbers, a piece of your letterhead paper stamped and signed and, of course, your bank account name and number for security purposes. Easy to see through, you say? The Secret Service still gets 100 telephone calls from victims of the Nigerian scam and three to five hundred pieces of related correspondence – every single day."

Basically, cyberpickpockets are out to hijack personal information, and if they can't get it one way, they will surely try another.

Children's Social Security numbers are ideal targets, for their clean credit and absence of criminal histories. More than 400,000 kids had their identities stolen one year, two-thirds of them by close family members.

It's safer to omit the exact birth date in an obituary nowadays. And if the deceased is an older woman, one shouldn't mention her maiden name, which is often used as a secondary security check by financial institutions.

Add all these ploys to some sneaky technological moves, and you've got powerful techniques for prying out personal information. One latest wrinkle is keylogging.

Instead of directly asking the user to enter personal data, cybercriminals are embedding code into fake e-mail news articles about cyclones, or bird flu or phony "requests for proposals," perhaps. Like other forms of pernicious software, this code installs a back door into your PC. When you visit your bank online, for example, the programs silently copy the keystrokes and send the stolen userIDs and passwords back to the crooks.

Internet fraudsters keep coming up with a never-ending supply of ways to persuade victims to open an attachment, click on a link or innocently enter personal data on a fake Web page. As one victim put it, "There are more criminals on the Internet street than there are policemen."

The Cell Phone

Cell phones are handy. But they generate data not only on where you're using them, but also the incoming and outgoing numbers, as well as other information that can be stored, sorted and, ultimately, stolen right out of the air by someone on the same network – in the neighborhood, at the local Starbucks or just passing by your house on purpose in a vehicle.

The reality is that practically anyone - a suspicious spouse, a nosy neighbor, even a business rival – can get their hands on your phone records to do with as they will. Compile a list of your best customers perhaps.

And don't throw away those old personal or business cell phones or try to sell them on eBay. All sorts of sensitive personal and corporate info piles up inside them, and deleting them may be more difficult than you think. Check with your wireless carrier and your phone's manufacturer first.

ID Theft and Fraud in Business

We also have to be concerned about ID theft in business. Your business.

Outside of financial institutions, credit bureaus, payment processors and data brokers, employers are the keepers of the largest collections of personal information. We've got to do a better job than ChoicePoint, Boeing, Time Warner, Citibank, and the big insurance company AIG — all of which have been part of the 100 million losses of personal data.

Ought-to-be secure information typically walks out the door in one of three ways: 1) hackers grab it; 2) employees steal it or; 3) companies lose it — through incompetence, poor gatekeeping, bad procedures or some combination of the three.

Some industries — health care, child care, eldercare, financial services, as well as delivery services and in-home contractors (like yourselves) — are at high risk of being held liable for crimes their employee's commit.

Coping Strategies

With all this, how can you possibly protect yourself from Identity Theft?

On the Personal Side

- Carry minimum personal information with you regularly.
- Keep your ATM card separate from its PIN, keep your children's Social Security card and copies of your credit cards, front and back, locked up at home in case you need to report their theft.
- Consider using a locked mailbox to receive mail at home or at the office.
- Never leave checks or other sensitive mail out for pickup. For extra security, drop your outgoing mail at the post office.
- Check all your financial statements fully every month.
- Get a credit report at least once a year (see box).

Be careful on the telephone. The only time it's acceptable to reveal personal information over the phone is if you initiate the call. Don't give out credit card or Social Security numbers to anyone unless you know why it's needed. If you're suspicious, hang up and contact the company requesting the info directly.

On your computer, use different passwords for different accounts — banking, credit card, e-mail services, etc. It's a pain, but it's worth it. If you receive a suspicious e-mail, do NOT reply to it or click on the Web site link. Don't respond to e-mails requesting personal info, no matter how official they look and never click on a link or an attachment from an e-mail sender you don't know. If a deal you're offered looks too good to be true, it probably is. Update computer virus protection software regularly, and download all the latest operating system and browser security patches. Use firewall software, especially for computers with DSL or cable modem Internet access.

"Most importantly," Weisburger points out, "the very best investment you can make is in crosscut shredders — at least one for your home and as many as you need for the office."

Run through it any paperwork that contains personal information — especially pre-approved credit card offers, ATM and charge receipts, insurance statements, checking and bank statements. Destroy any no-longer-needed paperwork that contains Social Security numbers, account numbers, birth dates, or other info a crook might use to go on a spending spree — on you. Consider viewing your financial account statements online, and opt-out of receiving paper statements in the mail if possible.

CREDIT REPORTS

To order copies of your credit reports (at least once a year), to report errors promptly and in writing, or to arrange a fraud alert, contact the three major credit reporting agencies:

- Equifax, 800-685-1111, P.O. Box 105851, Atlanta GA 30348
- TransUnion, 800-888-4213, P.O. Box 1000, Chester PA 19022
- Experian, 888-397-3742, P.O. Box 2002, Allen TX 75013

On the Business Side

Where employees are concerned, there's a load of data you need to protect, not just names and Social Security numbers, but direct deposit bank account numbers, driver's license numbers, relatives' names, and health information. For your own sake, don't make it easy for anyone to walk off with your customer list, or payroll info like wages, bonuses, hours worked, garnishments, child support payments, charitable contributions, and so forth.

How do you prevent such problems?

- Physically: Lock up documents, with special care to paychecks, stubs, tax forms. Make sure this data is secure from weekend prying. Limit data printed on pay stubs and paychecks.
- Electronically: Establish multiple security layers of access to computers. A firewall keeps outsiders out. A password system allows access only to authorized employees. Encryption keeps sensitive data from being seen by anyone without an authorized key. Limit specific data access only to people who need it.
- Tighten up security: When an employee leaves change all passwords and security codes available to the terminated employee, if appropriate. Require the immediate return of computer disks, compact disks, keys, and laptops.
- Destroy old computer disks and CD-ROMs: Wipe electronic fields and completely erase, according to manufacturer instructions, any data from computers, PDAs and cell phones before disposing of them.
- Train your staff: Your payroll people should be aware that personnel information is a controlled substance. A successful program to protect payroll data will combine techniques that address physical documents, computer files and employee practices as well.

After the Fact

- File a report with the local police and keep a copy.
- File a complaint with the Federal Trade Commission (see box).
- Alert the credit reporting agencies.
- Notify banks, creditors and utilities; close accounts accessed by thieves; and choose new passwords and PINs.

Take immediate steps to correct your records. Document every phone call and follow up in writing, using certified mail, return receipt requested. NEVER send original documents, and always keep a copy of any letters.

If you believe you've been a victim of identity theft, federal law allows you to place a fraud alert on your credit report for 90 days (see box), legally compelling lenders to ask tougher questions to verify an applicant's identity.

A new service offers to handle all the paperwork, every 90 days, to keep a perpetual alert on your credit file. The credit bureaus themselves offer their own monitoring services, which alert you within 24 hours of significant activity on your file, unfortunately, after the horse has bolted.

There are insurers now in the U.S. who offer ID theft coverage to individuals at reasonable rates. Coverage varies but may include lost income, expense reimbursement, attorney fees, recovery and restoration services, as well as after-the-fact aid and comfort.

"Technology is getting more complicated," Michael Weisburger points out, "and crooks are getting smarter to keep pace with it. It's important we do everything we can not to fall a victim to identity theft."

By Michael A. Weisburger, CLU, ChFC
President, Weisburger Insurance Brokerage
www.weisburger.com

CONTACT THE FTC

Check out the Federal Trade Commission's Web site at **www.ftc.gov**. Click on the banner headline, *Fighting Back Against Identity Theft*, which will lead you to two very useful publications:

- "Deter/Detect/Defend," a two-page summary of how to avoid ID theft, and
- "Take Charge," a 40-page booklet you'll find worthwhile to keep in the office for reference purposes, in case you or one of your employees ever runs into trouble.

To file a complaint, visit the FTC Web site at **www.consumer.gov/idtheft**.