IDENTITY THEFT

reported by someone claiming to be Tim O'Toole

No, it's not about someone pretending to be heir to the throne of Lower Slobovia. Nor is it likely that someone will undergo plastic surgery so they can attend your high school reunion, as you! Identity theft is just the latest edition of an age-old tradition. It is no longer cost-effective to break into your home to steal your property, risk apprehension, then fence second-hand goods at a considerable mark-down.

It's much more efficient to purchase brand new goods, with warranty, and let someone else pay for them. Free shipping and no sales tax are a bonus for the digi-thief.

You've probably seen the movie ***Catch Me If You Can***, about Frank Abagnale – a child prodigy who started with a PanAm decal from a Revell model plane, then parlayed that into millions of dollars in bad checks. After a miserable stint in a French prison, Frank reversed course, and now heads a major anti-fraud company helping defend corporations from forgery.

But there is a new generation of con artists out there (as featured in a current credit card commercial), who recognize the weak underbelly of modern e-commerce.

Using psychology and technology, rather than lock picks and windows shims, they are beginning to cost us real money, even by Pentagon standards.

On Thursday, February 26, 2004 the New York State Internal Control Association featured a presentation on Identity Theft by John J. Sennett, a recent retiree of the FBI. Sennett is now employed by the Department of Public Service as their Director of Utility Security.

While acknowledging that the Secret Service[1] are the experts in this field, Sennett's presentation offered intriguing insights into the criminal mind, and the "socially engineered" mind of the victim.

His presentation also awakened some family memories for me, which will inevitably intrude without warning in this article. But here goes:

Once upon a time we all lived in small towns, and like the bar in ***Cheers***, everyone knew your name. You shopped in person at local stores, and paid cash, or ran up a tab at the company store. Your face and your signature were the only identification you needed.

Then Social Security arrived, to defend us from total penury and starvation (there was a lot of that going on after 1929). A generation ago, a sign of maturity was getting your own checking account after you finished school and were gainfully employed. Your employer paid you by check, and you paid your recurring bills by check (e.g., phone, electric, rent, car insurance). You probably bought groceries by check once you started feeding more than one of you.

Credit cards started happening with gusto in the 60's. I know this because my father retired from the FBI in 1965, to take a job as Vice President of Diners Club, the leading entertainment credit card of that era. Would you believe way back then, there were people forging credit cards? Charges over a set dollar amount had to be approved by phone call from a restaurant or hotel to Diners Club.

Waiters talked to human beings at 1 Columbus Circle, and everyone was happy. The diner was happy because he or she had just impressed a

[1] This will make my brother happy. He specializes in collaring Nigerians who engage in imaginative banking practices in North Carolina.

business contact, was close to closing a big deal, and had his or her employer pay for the lobster and champagne.

Then some unscrupulous employees started keeping track of credit card names and numbers, selling the data to counterfeiters in Queens, NY who could print and emboss some very authentic looking credit cards. The phony cards might have a useful shelf life of only 30 or 45 days, but each card had a high or open-ended credit limit, so it was worth the effort. In those days it was said that you could steal more with a briefcase than you could with a gun.

Today, you don't even need the briefcase.

Enough preamble, here's the meat of John Sennett's presentation.

It's now the 21st Century, and banking, commerce and the Internet have changed the rules of the game. It all started toward the end of the 20th Century with the proliferation of credit cards. Consumer-oriented Visa, MasterCharge, and Discover all eclipsed the more effete titans (Carte Blanche and Diners Club), while American Express picked up the corporate side. Following Sears, Roebuck's lead, more and more companies turned to color catalogs to ply their trade, as 800 numbers replaced expensive bricks & sticks stores. Add the Internet and dot.com websites, and "distance shopping" became the new reality.

…it was said that you could steal more with a briefcase than you could with a gun.

Today, you don't even need the briefcase.

Teens who used to steal hubcaps now learned how to hack into mainframe computer systems with lowly Commodore 64 computers and 300 baud modems. If your purse or wallet were stolen, you worried more about the data in them, than the dollars lost. Laws were passed to limit the honest consumer's liability to $50 for each lost or stolen credit card. If you didn't keep a copy of that lost data elsewhere (names, numbers and 800 phone lines for each credit card; drivers license, bank number, etc.) you would spend hours retrieving that information with lots of time on hold being told your call was important).

Now when we talk of "identity theft" we are talking about two technically different items:

- **Account Theft** – a stable indignity, whereby someone gets a hold on an active credit card number, and via Internet or 800 number, orders merchandise to be shipped to a different address;
- **Identity Theft** – a growing phenomenon, whereby someone uses your personal descriptors to open up new credit accounts, then runs up mega-debts in your name.

In the first example, you may realize something is wrong when you get your next credit card statement. In the second example, you may never see a bill until a collection agency knocks on your door demanding repayment of $30,000 for that fuschia Lexus.

Complaints to the Federal Trade Commission have been doubling annually for the past few years regarding that second example (250,000 complaints in 2003). Losses to businesses are now $32.9 Billion (an average of $10,200 to each business), while losses to consumers total $3.8 Billion (an average loss of $1,180 to every victim).[2] What's worse, the average victim of identify theft will spend an average of 60 hours re-negotiating a good credit rating, and resisting the bill collectors.

To understand how we are being victimized by this new technology, we need to look at human psychology. After all, most of us are social, gregarious creatures, who want to get along, play well with others, learn to share, and not run with scissors.

[2] On the plus side, we are less frequently bothered by boiler room con artists and telemarketers at dinner time. On the minus side, it's a bit like termites eating away at the foundation of your house. You don't know there's a problem until it's too late.

John Sennett referred to something called the **Six Peripheral Roots to Persuasion**[3]:

1. **Authority** - we tend to believe something is true, if it is stated by, or attributed to an authority figure;
2. **Scarcity** – this item is in short supply, or on sale for a limited time only, but you must act quickly;
3. **Liking/Similarity –** we want people to like us, and we like to relate to folks with similar interests or history (the old college tie, service buddies, ethnic or religious affiliation);
4. **Reciprocity** - I'd like to do something nice for you, you've been such a nice audience. I can offer you a free 56K modem, all you need to pay is the shipping and handling (which will cost twice what the item is worth);
5. **Commitment and Consistency –** we want to "be nice", and keep or promises;
6. **Social Custom –** we tend to value and trust the written word, even if it's just dots on a computer screen, or an amazing offer in an e-mail.

Hearing John's words, I was reminded that this is an election year, and a lot of the powers of persuasion relate to more than e-commerce scams.

Having dissected our own brains, Mr. Sennett went on to describe the mind-set of the perpetrators, who have nothing but contempt for their gullible marks. They refer to a victim as a "mooch", saying the victim wanted something for nothing, and instead them gave them "nothing for something."

I've always heard that "if it's too good to be true, it's too good to be true", and "it's hard to cheat an honest man". We are always looking for a bargain. John Sennett is into power tools[4], and has been known to "distance shop" for routers in the wee hours of the morning.

Before getting into a discussion of tips for protecting yourself from scams, John offered more anecdotes on identify theft, including one Arab terrorist who was a sleeper agent in Canada. Acquiring the baptismal certificate of a dead Québecois, he was able to upgrade that to a dozen identification items. (Even then, an alert Immigration official prevented him from completing his mission when he attempted entry to the United States via the state of Washington).

The **scams are not limited to credit card purchases** of durable goods. Verizon now has 400 investigators on staff delving into phone bills charged to someone else's credit card (hopefully not yours). The electric utilities have a similar problem. Yes, there are conveniences to digital shopping, but headaches as well to the naïve and gullible.

When questioned about what steps we could take to avert financial catastrophe, Mr. Sennett admitted he didn't own a shredder, but he did reconcile his bank statements promptly, reviewed his credit card bills (more power tools) immediately, and tempered his "socially engineered" gullibility with a healthy dose of "buyer beware".

He recommended we each photocopy the contents of our wallets, and store that data in a safe place. Be sure to have current anti-virus software on your computer (to protect yourself, and be a good citizen, avoiding infecting others).[5]

We are more likely to be victimized by bogus e-commerce come-ons. Given the large scale of the Internet, a new "digital boiler room" scam need only succeed in 1/10th of 1 %. Encryption techniques, e-mail filters, additional authentication measures and even bio-metric devices can help reduce the chance of chaos.

[3] Dave Barry might think this would make a great name for a rock band.

[4] Binford Tools meets Benford's Law.

[5] Editor's Note: A Firewall is critical if you have Internet service via a cable modem (like Road Runner). A firewall is desirable even if you are using a phone modem.

Sennett recommended you go to the big three credit reporting agencies annually to review your ratings. They are Equifax, Experian and TransUnion. If you lose your Social Security card (or someone starts claiming your number), call the Social Security Administration at 1-800-269-0271.

The Federal Trade Commission has a website devoted to ID theft: www.consumer.gov/idtheft

Their website offers valuable instructions, plus an AFFIDAVIT form (PDF file) for those of you who may have been the victim of identify theft.

Also, a new law is taking effect in New York State this year, requiring all new ATMs to print only the last five digits of your account code on receipts (and existing machines must be retrofitted or replaced by 2007).

Sennett also warned us of "frame spoofing", or those insidious pop-up screens that appear when using the Internet. They look genuine, but can draw you into a scheme, and lure you to reveal your credit card number. And those on-line auctions play up the "scarcity" of collectibles, drawing absurd bids, even if the merchandise is delivered.

The follow-up discussion by the group yielded a few more valuable observations and ideas. For example, have one credit card with a low credit limit that you use of on-line shopping (save your Platinum card for impressing friends at restaurants). Watch out for spam that looks like authentic, incredible offers from major corporations or absurd discounts on name-brand items. For that matter, watch out for e-mail links that take you to what looks like a respectable website (complete with color logs).[6]

They are just "**phishing"** for personal information about you (credit card numbers, date of birth, bank account, mother's maiden name). Delete any letters you receive from former oil ministers of Nigeria, who need your help moving an account off-shore. Think of unsolicited e-mail as the equivalent of a stranger knocking on your door. Do not provide personal identifying information to anyone over the phone, or via e-mail or Internet. If your bank needs to be reminded of your mother's maiden name, tell them you will call them back, then phone your local branch manager.

I'd like to close on an upbeat, personal note about identity theft. The year was 1967, and the FBI were trying their damnedest to get something on Joe Bananas, the crime family capo from New York City. His business associates (euphemism) had extorted the open-ended use of a Diners Club card from a losing gambler. Said card was then used by Joe's son Salvatore, then sanitized as Bill Bonnano, living in Arizona, riding horses, wearing southwest style clothing, and acting respectable. When the gambler tired of the outrageous "vigorish", he went crying to **Diners Club**, and they succeeded where the FBI had failed – getting an indictment and conviction of Salvatore for using someone else's credit card. My father's former co-workers were chagrined (to put it mildly), but they learned from the experience.

We should all learn from our experiences.

Did I mention that the US Secret Service has a fascinating CD-Rom about electronic evidence, credit card forgery ("Forward Edge")? Not available in stores. They also have a detailed guide to seizure of electronic evidence at http://www.secretservice.gov/electronic_evidence.shtml .

[6] As good citizens we need to discourage spam, by NOT responding to such unsolicited offers. When you are ready to buy something, go to www.walmart.com or www.victoriassecret.com . In such instance you have the assurance that you are going to the real on-line store, not a spoof. Of course, OFT's WebSense will block the second site, but you get the idea.