

# From Your Deputy Executive Director

By  
Matt  
Puckett

## Protecting Your Identity

It's a nightmare scenario: Your bank account is run dry, your credit is ruined, or worse yet some thug with a vendetta against you learns where you and your family live. In today's world, with the ubiquitous dissemination of your personal information, this nightmare can become a dreadful reality.

Although Florida has a number of restrictions to its public records that help to protect your identity and your families, more is always needed. Yet try as we might to

protect you in the public sector, it is often what is available in the private sector that allows your information to fall into the hands of the bad guys. We always strive to provide information that is beneficial to you and your family, so please read the following two articles on how you can help protect your identity. Some of the information is overlapping and obvious, but all of it is very useful. Please read it and share it with your family and friends.

Stay safe.

February 13, 2008 Article featured by MSN Money Staff:

### Your 5-minute guide to protecting your identity

Here are 20 steps to protect yourself from identity theft—and seven ways to clean up things if you become a victim.

Thieves may sell your information on the black market or use it to obtain money, credit or even expensive medical procedures. Unless you're vigilant in protecting your records, you'll have to work even harder to repair the damage to your credit. The average victim spends 30 to 40 hours rectifying the problem.

Some of the e-threats to your identity are:

- **Phishing.** You get an e-mail that appears to be from your bank or an online service, most often PayPal or eBay, instructing you to click on a link and provide information to verify your account.
- **Pharming or spoofing.** Hackers redirect a legitimate Web site's traffic to an impostor site, where you'll be asked to provide confidential information.
- **Smishing.** This is phishing done with text messaging on your smart phone. It instructs you to visit a bogus Web site.
- **Spyware.** You've unknowingly downloaded illicit software when you've opened an attachment, clicked on a pop-up or downloaded a song or a game. Criminals can use spyware to record your keystrokes and obtain credit card numbers, bank-account information and passwords when you make purchases or conduct other business online. They also can access confidential information on your hard drive.

You don't need to have a computer to become a victim.

- **Vishing — voice phishing.** You get an automated phone message asking you to call your bank or credit card company. Even your caller ID is fooled. You call the number and are asked to punch in your account number, PIN or other personal information.
- **Bank-card "skimming."** Crooks use a combination of a fake ATM slot and cameras to record your account information and PIN when you use a cash machine. Your credit or debit card also can be skimmed by a dishonest store or restaurant worker armed with a portable card reader.
- **Crooks will steal your wallet** or go through your mail or trash.

More than half of identity theft cases involve credit card fraud. Checking accounts are the second most popular target. But some crooks have other plans:

- At least 250,000 people have been the victim of medical identity theft in the last several years. Crooks use fraudulently obtained personal information to get expensive medical procedures or dupe insurance companies into paying for procedures that were not done.
- The victims of about 5% of reported identity theft cases are children. The fraud often goes undetected for years—until the young adult applies for credit.

### 20 tips to protect yourself

*You can take steps to protect yourself from identity fraud:*

- Keep your confidential information private. Your bank or credit card company won't call or e-mail to ask for your account information. They already have it.
- Keep an inventory of everything in your wallet and your PDA, including account numbers. Don't keep your Social Security card or any card with your Social Security number, such as an insurance card, in your wallet.
- Stop getting banking and credit card information in the mail.
- Monitor your bank and credit card transactions for unauthorized use. Crooks with your account numbers usually start small to see if you'll notice.
- Keep your vehicle registration and insurance forms in a sealed envelope in your glove box and lock it and your car when at home or away.
- If you conduct business online, use your own computer. A public computer is less secure, as is wireless Internet.
- Look for suspicious devices and don't let anyone stand nearby when you use an ATM. Take your card and receipt with you. Keep your PIN in your head, not in your wallet.
- Don't store credit card numbers and other financial information on your cell phone.
- If you're job hunting using resume Web sites, don't apply unless the employer has a verifiable address.

*Protect your computer from vulnerability:*

- Keep system and browser software up to date and set to the highest security level you can tolerate. Install anti-virus, anti-spyware and firewall protection, and keep them up to date as well. When possible use hardware firewalls, often available through your broadband connection router.
- If you use wireless Internet access, make sure that you get help from someone who understands wireless security when you set up your access point or router.
- Back up your data and store it way from your computer.
- Don't open e-mails from strangers. Malware can be hidden in embedded attachments and graphics files.
- Don't open attachments unless you know who sent them and what they contain. Never open executable attachments. Configure Windows so that the file extensions of known file types are not hidden.
- Don't click on pop-ups. Configure Windows or your Web browser to block them.
- Don't provide your credit card number online unless you are making a purchase from a Web site you trust. Reputable sites will always direct you to a secure page with an URL starting with *https://* whenever you actually make purchases or are asked to provide confidential information.
- Use strong passwords: at least six characters, including at least one symbol and number, and no reference to your name or other personal information. Use a different password for every site that requires one, and change passwords regularly.

*Continued on next page.*

## BAD DAY BLUES

### You Know You're Having a Bad Day When...

Your horn sticks on the freeway behind 32 Hell's Angels motorcyclists.

You've been at work three hours before you notice that your fly is open.

Your twin sister forgets your birthday.

Your birthday cake collapses from the weight of the candles.

You call suicide prevention and they put you on hold.

You have to sit down to brush your teeth in the morning.

Everyone avoids you the morning after the company office party.

Your income tax refund check bounces.

It costs more to fill up your car than it did to buy it.

The bird singing outside your window is a vulture.

Your blind date turns out to be your ex-wife.

You put both contacts in the same eye.

Your mother approves of the girl you are dating.

Your doctor tells you that you're allergic to chocolate.

You have to borrow from your Visa card to pay your Mastercard.

Nothing you own is actually paid for.

Everyone loves your driver's license picture.

The health inspector condemns your office coffee maker.

You invite the peeping Tom in ... and he says no.

People think that you're 40 and you're only 35.

You call your wife and tell her that you'd like to eat out tonight and when you get home, you find a sandwich on the front porch.

You start to put on the clothes that you wore home from the party last night... and there aren't any.