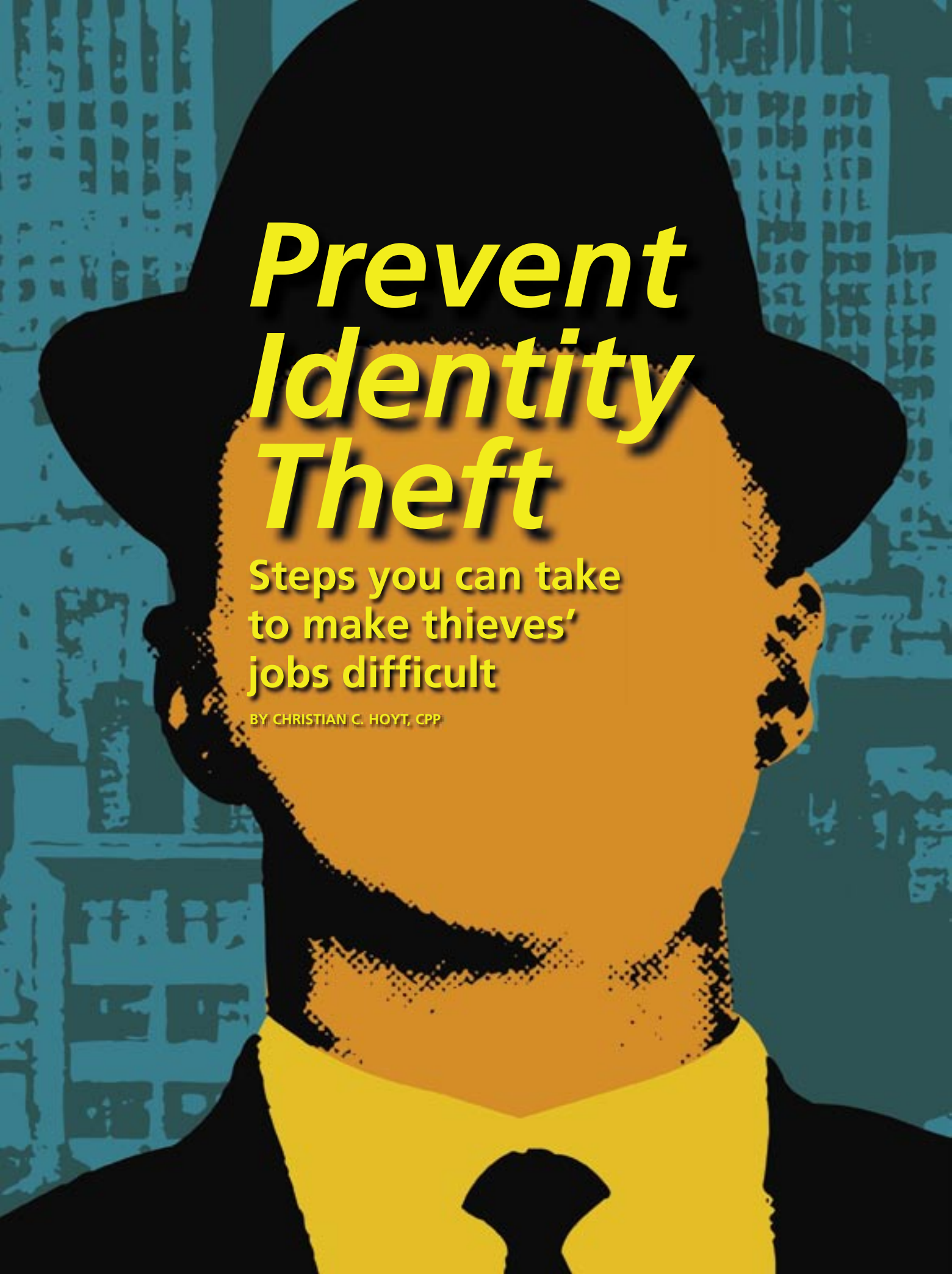

# Prevent Identity Theft

## Steps you can take to make thieves' jobs difficult

BY CHRISTIAN C. HOYT, CPP

The term "identity theft" was first codified in the Identity Theft and Assumption Deterrence Act of 1998. This Act makes it a "federal crime when someone knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law."[1]

Additionally, the Act defines a "means of identification" as "any name or number that may be used, alone, or in conjunction with any other information, to identify a specific individual." Identifying information is noted to be, among other things, a name, social security number, date of birth, driver's license or passport number, employer or taxpayer identification number, or telecommunication identifying information or access device.

The law also directs the Federal Trade Commission (FTC) to establish a central complaint system to receive and refer identity theft complaints to appropriate entities, including law enforcement agencies and national credit bureaus.

Prior to 1998, victims had little recourse to prosecute their attackers. In one instance, a couple whose identities were stolen in the early 1990s were subjected to hundreds of thousands of dollars of credit card debt. While they spent thousands of dollars trying to clear their names, the thief added insult to injury by calling and mocking them, bragging that they could not arrest him under the current legal system.

Today, identity theft is a recognizable term, but it still lacks a proper definition. For the most part, identity theft is lumped together with fraud, but it is really a crime category of its own. Deceiving someone to attain money, or accessibility to money, is typically what people think of when they think of fraud, but identity theft takes the deception to another level.

When a criminal steals your identity, not only does he or she commit fraud, they also destroy your credit. As victims learn, it is far easier to resolve the theft of funds from bogus credit cards and bank accounts than it is to restore the good credit history you spent a lifetime building.

Identity theft affected over nine million people in the U.S. in 2004. Joanna Crane, Identity Theft Program Manager at the Federal Trade Commission, identified three main types of theft. The first is credit card fraud, which is the simplest form and will cost the victim an average of $140. The second is bank account fraud in which a thief accesses your bank account; this type costs an average of $230. The final offense is the most complicated. When your identity is stolen—and before you are aware of it—the thief opens new accounts or obtains loans in your name. This offense averages $1,180.

## Consumer Intervention

Three areas where consumers can take the lead in preventing identity theft, according to Crane, are phishing (and its related offense, pharming), which is a form of Internet fraud; mail and document security; and protecting personal information. "People need to be a lot more skeptical and cautious," said Crane of these areas.

Phishing is the practice of sending spam e-mail or pop-ups that attempt to lure the victim into revealing personal information. Crane described a new scam in which the perpetrator offers

*(continued on page 23)*

# Phishing, Fraud and FUD

BY RAVI GANESAN

Phishers have hit the online world, as Willie Sutton famously said, "because that's where the money is." Information that resides in HR and payroll applications is prime information phishers can leverage to perpetuate fraud and theft, and must be protected.

Phishers started by sending emails out to millions of people per day, claiming to be from a trusted source, and asking for ids and passwords. They often try to play upon fear, uncertainty, and doubt (FUD). The phisher wants two things:

- To steal identity data to help them commit identity fraud
- To steal a password so they can log on as that user and steal important information, including identity data

Recently, phishers have become more devious. Now, an innocent looking e-mail with your company's brand on it could download a keystroke logger or spyware (software that runs in the background without your knowledge) onto the machine so that wherever that person goes, the phisher gets their password. This supplies lots of places the phisher can steal from—including your HR or payroll applications

Here's what you can do now, before the damage occurs.

- End-User Training. Ideally we'd all like to keep users from going to phishing sites in the first place, but let's face facts. That user sees your brand and trust it. That's why phishing works. So, start training your employees now to be wary of email that looks like it came from your company, but has grammar or other errors. Tell them now that you'd never email them asking for their password, company ID, or social security number.
- Use Stronger Authentication. If your user does get lured to a phishing site, make what the phisher gets useless. Look for authentication systems that do not send secrets, but rather prove knowledge of the secret. Your signature works this way—by signing your name, you're not showing that you know your name, but rather that you can sign it, in the special way only you know how to do. Look for authentication systems with some intelligence and forethought behind them—for example—a system that allows you to change the strength of authentication and manage multiple levels of authentication.
- Don't Buy Into FUD. Use common sense in thinking through which measures will help with which part of the problem. User education will not keep some people from falling for these scams, and the strongest authentication in the world won't help if the user types their passwords into the phishing site. If you start now, you can protect the brand and employee trust you've worked so hard to build.

*Ravi Ganesan is the Founder & CEO of TriCipher, Inc. He can be reached at 650-372-1300 or via email at ravi@tricipher.com.*

to send the victim an item of value, and requests a payment less than the item's value in return.

Once the victim has sent the payment, the perpetrator gains access to either a personal check or credit card information and the stealing begins. Phishing artists are clever and go to great lengths to entice you into revealing your data. To test your "skeptical skills," visit http://survey.mailfrontiercomsurvey/quiztest.html and take the online survey.

Unless you get 9 out of 10 correct on this quiz, you should take steps to deal with a potential phishing scam. First, do not give out personal data unless you actually know the person or company that e-mailed you, and you are familiar with their e-mail format.

Second, limit the use of e-mail for sending and receiving critical information. E-mail is not secure; therefore, it is vulnerable to interception. Third, keep abreast of your bank and credit card statements. Monitor transactions weekly, so if someone steals your data, you can catch it before the thief can get too far. Finally, although most people do not have Internet firewalls on their home computers, everyone should have some form of anti-virus software that will limit the number of phishing e-mails they receive.

Pharming redirects the user to a phony Web site. It is akin to domain spoofing. Typically, pharming victims do not even know they have been sent to a bogus Web site. According to Jordan Cohen, Director of ISP and Government Relations for Bigfoot Interactive, "The main concern is no longer spam. It is about being protected from ID theft."[2]

Microsoft and Yahoo are both working on some form of e-mail caller ID to try to slow these fraud trends. The biggest component in stopping this form of identity theft is the consumer. As a nation of Internet users, consumers need to be aware of scams and recognize that the trust associated with brick and mortar companies does not exist in cyberspace. If you have received a phishing e-mail or been redirected to a pharming Web site, please forward the email or link to spam@uce.gov.

### Protect Paper Documents

Paper records and hard copy mail are the primary tools of an identity thief. Think of the many documents mailed to your home—and thrown away—in a week. I receive at least five credit card offers each week. Shredders and security mail boxes are readily available and should be used whenever possible.

Crane offered three simple pointers regarding paper security. First, consider sending all of your mail from either a post office box or from one of the standard blue post office collection containers. Better yet, pay and receive as many bills online as possible.

A single piece of mail stolen from your mailbox that contains a personal check opens another avenue for a thief. More importantly, understand that if a thief uses your credit card, you are only liable for up to $50, but if he or she gains access to your ATM or debit card, your liability increases to $500.

Second, if you do not have a secure mailbox (one with a lock), try to retrieve your mail promptly. The longer your mail remains in an unsecured mailbox, the greater the opportunity for vital information to be stolen. Because it is impossible to know what mail to expect each day, mail could be taken without your knowledge—until your identity is stolen.

Third, shred documents that contain personal information. If you are not in a position to purchase a shredder, be a human shredder. Ripping up important documents five or six times and separating the pieces into separate receptacles is one solution. Many companies have shredders at work that can be utilized.

Do you throw credit card receipts away? Don't do it! Rip them into at least four pieces before tossing them in the trash. If you void a check, make it difficult to piece back together. Be sure to obliterate the MICR line at the bottom of the check as best you can. Tossing whole documents into the trash makes thieves' jobs easier.

The primary way for someone to steal your identity is through your social security number, so protect it. Also, protect your mother's maiden name because this is a typical question for retrieving passwords. These pieces of information should be your biggest secrets.

According to a survey conducted by the Better Business Bureau, over 40% of identity fraud is derived from the theft of

*(continued from page 24)*

## Identity Theft Web Sites

For more information on identity theft, check out the following Web sites.

**(www.privacyrights.org)**
—Take an "Identity Theft IQ Test" on this site.

**(www.identitytheft.org)**
—A comprehensive site with numerous resources for fighting identity theft

**(www.identity-theft-help.us)**
—A site containing many links to helpful information on identity theft.

a purse, wallet, checkbook, credit card, or the availability of critical information to friends, family, or acquaintances. There are many new ways in which an individual's identity may be stolen, but the traditional methods of theft and deception still account for the highest percentage of incidents.

### Protect Critical Information

First of all, do not carry your social security card with you because it is a key piece of information a thief will need—and will have—if he or she steals your purse or wallet. You may be able to cancel your credit cards, but the thief will have access to your social security number, your name, and your address, which will put him or her in a great position to steal your identity.

Secondly, request that your social security number not be printed on any workplace forms. For example, the payroll department needs your social security number, but it does not need to print it on your check stub.

Finally, make sure that your social security number is not your drivers' license number. Some states were doing this, but you can request a different number.

"You don't have to give everyone your social security number," said Crane. Most companies will not refuse your business if you do not give them your social security number, she explained, and you should be skeptical of the intentions of those that do.

To check on your social security account, you can request a Social Security Personal Earnings and Benefit Estimate Statement by calling (800) 772-1213, or on the Web at www.socialsecurity.gov. This report will allow you to verify wages that have been credited to your social security number, plus it is a great way to track your career earnings.

If you are between the ages of 25 and 64, you should also receive a Social Security Statement from the Social Security Administration about three months before your birthday each year. Please check it carefully when it arrives in the mail.

### Make Thieves' Jobs Difficult

Identity theft is a serious and growing problem. As more business migrates to the Internet, the phishing and pharming schemes will become more sophisticated and devious. Do not make the thieves' jobs easier by handling your personal documents and information haphazardly.

Informed consumers are a better "firewall" than anything that can be purchased for your computer. Be wary, learn about scamming trends, and, most importantly, protect your personal data. Be a smart consumer, and identity thieves will lose their resources.

> Paper records and hard copy mail are the primary tools of an identity thief.

*Christian C. Hoyt, CPP is Vice President of Pay USA, Inc.*

[1] The Identity Theft Assumption and Deterrence Act of 1998 can be found on the Federal Trade Commission's Web site at www.ftc.gov/os/statutes/itada/itadact.htm.

[2] Reproduced from an article in www.technewsworld.com in accordance with its usage restrictions.