
The Belleville Beat

Belleville Police Department
Belleville, IL 62220

March 2005
Volume 11, Number 3

From the Desk of Sgt. Don Sax

More than 11,000 Illinois residents said they were victims of identity theft in 2004, according to a federal report released last month. This month's issue of *The Belleville Beat*, March 2005, provides information from the Federal Trade Commission on ways to protect yourself.

How Not to Get Hooked by a 'Phishing' Scam

Internet scammers casting about for people's financial information have a new way to lure unsuspecting victims: They go "phishing."

Phishing is a high-tech scam that uses spam or pop-up messages to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, or other sensitive information.

According to the Federal Trade Commission (FTC), phishers send an email or pop-up message that claims to be from a business or organization that you deal with – for example, your Internet service provider (ISP), bank, online payment service, or even a government agency. The message usually says that you need to "update" or "validate" your account information. It might threaten some dire consequence if you don't respond. The message directs you to a Web site that looks just like a legitimate organization's site, but it isn't. The purpose of the bogus site? To trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

The FTC, the nation's consumer protection agency, suggests these tips to help you avoid getting hooked by a phishing scam:

- If you get an email or pop-up message that asks for personal or financial information, do not reply or click on the link in the message. Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address. In any case, don't cut and paste the link in the message.
- Don't email personal or financial information. Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's Web site, look for indicators that the site is secure, like a lock icon on the

browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.

- Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- Use anti-virus software and keep it up to date. Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge. Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically.
- A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection. Finally, your operating system (like Windows or Linux) may offer free software "patches" to close holes in the system that hackers or phishers could exploit.
- Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them.
- Report suspicious activity to the FTC. If you get spam that is phishing for information, forward it to spam@uce.gov. If you believe you've been scammed, file your complaint at www.ftc.gov, and then visit the FTC's Identity Theft Web site at www.consumer.gov/idtheft to learn how to minimize your risk of damage from ID theft. Visit www.ftc.gov/spam to learn other ways to avoid email scams and deal with deceptive spam.
- The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Protecting Against Identity Theft

How can I prevent identity theft from happening to me?

- As with any crime, you can't guarantee that you will never be a victim, but you can minimize your risk. By managing your personal information wisely, cautiously and with an awareness of the issue, you can help guard against identity theft.
- Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or are sure you know who you're dealing with. Identity thieves may pose as representatives of banks, Internet service providers (ISPs) and even government agencies to get you to reveal your SSN, mother's maiden name, account numbers, and other identifying information. Before you share any personal information, confirm that you are dealing with a legitimate organization. You can check the organization's Web site as many companies post scam alerts when their name is used improperly, or you can call customer service using the number listed on your account statement or in the telephone book.
- Don't carry your SSN card; leave it in a secure place.
- Secure personal information in your home, especially if you have roommates, employ outside help or are having service work done in your home.
- Deposit outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox. Promptly remove mail from your mailbox. If you're planning to be away from home and can't pick up your mail, call the U.S. Postal Service at 1-800-275-8777 to request a vacation

hold. The Postal Service will hold your mail at your local post office until you can pick it up or are at home to receive it.

- To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you're discarding, and credit offers you get in the mail. If you do not use the pre-screened credit card offers you receive in the mail, you can opt out by calling 1-888-5-OPTOUT (1-888-567- 8688). Please note that you will be asked for your Social Security number in order for the credit bureaus to identify your file so that they can remove you from their lists and you still may receive some credit offers because some companies use different lists from the credit bureaus' lists
- Carry only the identification information and the number of credit and debit cards that you'll actually need.
- Place passwords on your credit card, bank and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers. When opening new accounts, you may find that many businesses still have a line on their applications for your mother's maiden name. Use a password instead.
- Ask about information security procedures in your workplace or at businesses, doctor's offices or other institutions that collect personally identifying information from you. Find out who has access to your personal information and verify that it is handled securely. Ask about the disposal procedures for those records as well. Find out if your information will be shared with anyone else. If so, ask if you can keep your information confidential.
- Give your SSN only when absolutely necessary. Ask to use other types of identifiers when possible. If your state uses your SSN as your driver's license number, ask to substitute another number. Do the same if your health insurance company uses your SSN as your account number.
- Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks.
- Be wary of promotional scams. Identity thieves may use phony offers to get you to give them your personal information.
- Keep your purse or wallet in a safe place at work as well as any copies you may keep of administrative forms that contain your sensitive personal information.
- Cancel all unused credit accounts.
- When ordering new checks, pick them up at the bank, rather than having them sent to your home mailbox.

What should I do if someone has stolen or scammed my personal information or identification documents?

- If your information or identification documents were stolen or scammed, you have an opportunity to prevent the misuse of that information if you can take action quickly.
- For financial account information such as credit card or bank account information: Close those accounts immediately. When you open new ones, place passwords on these accounts. Avoid using your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.
- For SSNs: Call the toll-free fraud number of any one of the three major credit bureaus and place a fraud alert on your credit reports: Equifax, 800-525-6285; Experian (formerly TRW), 888-EXPERIAN (888-397-3742); Trans Union, 800-680-7289. This can help prevent an identity thief from opening new credit accounts in your name.
- To replace an SSN card: Call the Social Security Administration at 1-800-772-1213 to get a replacement.

- For driver's license or other identification documents: Contact the issuing agency. Follow their procedures to place fraud flags and to get replacements.
- Once you have taken these precautions, there really isn't anything more you need to do except to check for the signs that your information is being misused. You don't have to file an identity theft report with the police or with the FTC until you find out if your information is actually being misused. If another crime was committed, such as theft of your purse or wallet or your house or car was broken into, report that crime to the police.

I have a computer and use the Internet. What should I be concerned about?

If you're storing personal information such as SSNs, financial records, tax returns, birth dates, or bank account numbers in your computer, the following tips can help you keep your computer and your personal information safe from intruders:

- Update your virus protection software regularly, or when a new virus alert is announced. Computer viruses can have a variety of damaging effects, including introducing a program code that causes your computer to send out files or other stored information. Be on the alert for security repairs and patches that you can download from your operating system's Web site.
- Do not download files sent to you by strangers or click on hyperlinks from people you don't know. Opening a file could expose your system to a computer virus or a program that could hijack your modem.
- Use a firewall program, especially if you use a high-speed Internet connection like cable, DSL or T-1, which leaves your computer connected to the Internet 24 hours a day. The firewall program will allow you to stop uninvited guests from accessing your computer. Without it, hackers can take over your computer and access your personal information stored on it or use it to commit other crimes.
- Use a secure browser - software that encrypts or scrambles information you send over the Internet - to guard the security of your online transactions. Be sure your browser has the most up-to-date encryption capabilities by using the latest version available from the manufacturer. When submitting information, look for the "lock" icon on the browser's status bar to be sure your information is secure during transmission.
- Try not to store financial information on your laptop unless absolutely necessary. If you do, use a strong password - a combination of letters (upper and lower case), numbers and symbols. Don't use an automatic log-in feature which saves your user name and password so you don't have to enter them each time you log-in or enter a site. And always log off when you're finished. That way, if your laptop gets stolen, it's harder for the thief to access your personal information.
- Before you dispose of a computer, delete personal information. Deleting files using the keyboard or mouse commands may not be enough because the files may stay on the computer's hard drive, where they may be easily retrieved. Use a "wipe" utility program to overwrite the entire hard drive. It makes the files unrecoverable. For more information, see [Clearing Information From Your Computer's Hard Drive \(www.hq.nasa.gov/office/oig/hq/harddrive.pdf\)](http://www.hq.nasa.gov/office/oig/hq/harddrive.pdf) from the National Aeronautics and Space Administration (NASA).
- Look for Web site privacy policies. They answer questions about maintaining accuracy, access, security, and control of personal information collected by the site, as well as how information will be used, and whether it will be provided to third parties. If you don't see a privacy policy, consider surfing elsewhere.

Are companies allowed to print my entire credit card number on my receipt?

After December 4, 2006, companies will not be allowed to print your credit or debit card expiration date or more than the last 5 digits of your card number on your electronic receipt. Some businesses will be

required to make this change sooner, depending on the way they process credit card transactions. The law will allow receipts that are hand written or mechanically imprinted to show your entire number and expiration date, even after December 4, 2006. For more information see section 605(g) of the FCRA.

How can I prevent companies from using my personal information for marketing?

More organizations are offering consumers choices about how their personal information is used. For example, many let you "opt out" of having your information shared with others or used for marketing purposes. For more information, contact the Federal Trade Commission.

When should I provide my Social Security number?

Your employer and financial institution will likely need your SSN for wage and tax reporting purposes. Other businesses may ask you for your SSN to do a credit check, like when you apply for a car loan. Sometimes, however, they simply want your SSN for general record keeping. If someone asks for your SSN, ask the following questions:

- Why do you need it?
- How will it be used?
- How do you protect it from being stolen?
- What will happen if I don't give it to you?

If you don't provide your SSN, some businesses may not provide you with the service or benefit you want. Getting satisfactory answers to your questions, though, will help you to decide whether you want to share your SSN with the business.