CONSUMER ACTION NEWS

Non-Profit Org.
U.S. Postage
PAID
San Francisco, CA
Permit # 10402

Change Service Requested

221 Main Street, Suite 480 • San Francisco, California 94105 • www.consumer-action.org • Spring 2006

Privacy Issue

Electronic records may pose threat to medical privacy

Congress is moving rapidly to build a national electronic health system, prompting new concern and questions about the adequacy of the medical privacy protections under HIPAA, the Health Insurance Portability and Accountability Act.

In 2002, the U.S. Department of Health and Human Services (HHS) dashed the right of patients to control access to their medical records and permitted more than 800,000 health-related businesses and government agencies to look at personal health information without patients' knowledge or permission. New HHS rules allow health care providers to share patient records with employers, drug and insurance companies, marketing firms, credit reporting agencies, accountants, banks, lawyers, and other entities without patient permission, even for reasons unrelated to health care treatment or paying claims.

In 1996, Congress enacted HIPAA to make the U.S. health care system more efficient, encourage the development of a national health information system and establish standards for electronic transmission of health information. In passing HIPAA, Congress recognized the need for privacy in an electronic health environment but could not agree on the terms of a privacy law. Because Congress failed to enact health privacy legislation, HHS was given the task. The agency issued final privacy rules in late December 2000, with compliance required by April 2003.

Some see benefits for patients and providers in a national health network, such as better access to health records for a mobile society and a way to coordinate care after catastrophes such as Hurricane Katrina. Others find privacy threats in an easily accessed system of health records. They argue that inappropriate access might lead to discrimination in the workplace, schools, housing and insurance. People who fear that their health histories might be released inappropriately might avoid seeking necessary care.

"Patients own their health data and should control who has access to their

See "Medical records," page 4

Privacy: What's it to me?

The legal right to privacy has been recognized in the U.S. since the late 1890s, but its roots go back to this country's founding. While not specifically mentioned in the Constitution, it is generally accepted that U.S. residents have a right to be left alone and to be free of unwanted public scrutiny.

The importance of privacy is spelled out broadly in the Bill of Rights, which limits the government's ability to interfere with individual liberty and recognizes people's right to be left alone.

The First Amendment protects an individual's freedom to speak, think, assemble, organize, worship and petition without government or private interference. The Fourth Amendment limits government intrusion into our "persons, houses, papers and effects" and the Fifth Amendment protects against self-incrimination and keeps the government from forcing us to reveal private information.

While valid concerns remain about governmental intrusions, questions also are being raised about the impact of marketing and sales on our privacy. Aided by computers and the Internet, marketing companies collect information from a variety of sources with speed and ruthless efficiency.

Today, information is currency bought and sold on the open market. It may include details about you and your family, your job, your money, your health and your hobbies. Many companies that have gathered such facts during sales and other transactions believe that they own your data and may use it as they please.

The information collected about you usually winds up in databases used for marketing purposes and may lead to your receiving countless solicitations by mail, telemarketing, faxes and e-mail. Reputable companies will allow you to remove your name from marketing lists ("opt out"), but in most cases, you must take the initiative of doing this on a company-by-company basis.

Many people object to the idea that information is collected about them—even if it is never used. They question why companies are permitted to collect and sell

See "Privacy," page 3

How private are your phone records?

By Jennifer Daw Holloway

Think your cell phone records are for your eyes only? Think again. For the right price, almost anyone can obtain your records.

Interested parties may not be listening in on your conversations, but they're coming close—your phone records can be bought by anyone with the money to pay for them.

Information brokers sell phone records and offer cell phone tracking through a variety of web sites, such as Locatecell.com and Celltolls.com, sometimes for just over $100. The practice was rampant until recent publicity shone light on this dirty little secret industry and it mostly went underground. The silver lining in this storm cloud is that federal and state governments have taken notice.

The Electronic Privacy Rights Center (EPIC) has petitioned the Federal Communications Commission, asking the agency to find ways to stop the practice.

In early February, the House Committee on Energy and Commerce held a hearing at which the chairman of the Federal Trade Commission promised to crack down on this practice.

And on March 2, Congress passed the Law Enforcement and Phone Privacy Protection Act of 2006, designed to strengthen protections for law enforcement officers and the general public by providing criminal penalties for the fraudulent acquisition or unauthorized disclosure of phone records.

Most recently, a bill called the "Prevention of Fraudulent Access to Phone Records Act" won unanimous approval from the U.S. House of Representatives' Energy and Commerce Committee.

In addition, many states are passing tougher laws against the illegal sale of phone records. California law sets the gold standard for other states to follow. In 2005 a state law went into effect to prevent cell phone providers from adding customers' wireless numbers to a directory without first obtaining their written permission.

How do cell phone record purveyors get your records?

In most cases, scammers get your records under false, and illegal, pretenses. This practice is called "pretexting." Scammers use the Internet and the phone to get their information. They set up online accounts in your name and get access to your records, or call pretending to be a customer who has lost his or her password.

How can I stop these crooks?

EPIC suggests that you create a password for your cell phone account. Call your provider and ask it to block access to your account to anyone who can't give the correct password.

Opt out of customer proprietary network information sharing. According to EPIC, most companies use your records for marketing purposes and many also sell your records to other companies.

Make sure your phone is in your name, not your company's name. If you use a company cell phone, have the phone registered to you and the bills sent to you so no one else can view them.

If you use online access, change your password periodically and make sure your passwords are not easy-to-discover, such as your address or digits from your phone number. If you don't manage your account online, ask your phone company to inactivate Internet access so that no one else can access your account by pretending to be you.

According to many security experts, while tougher laws and educated consumers make a difference in protecting privacy, cell phone companies must be part of the solution. Many firms are already beefing up security.

Legitimate firms are fighting back by filing lawsuits against bad actors who sell phone records obtained through false pretenses. The firms can also employ technology to help prevent privacy breaches.

One technique is called "out of band authentication"—if you call your cell phone provider for access to records, it will send a text message to your phone with a PIN number that must be provided to the customer service rep before the conversation can continue. This authentication feature would narrow the chance that the person requesting the records is a scam artist.

Experts also suggest that phone companies monitor the workplace computer activities of their employees, since many information leaks are attributed to people within the company. If a customer service rep in a particular region looked up several records in another region, it could trigger an investigation. ■

Consumer Action

www.consumer-action.org

Consumer Action is a non-profit 501(c)(3) advocacy and education organization founded in 1971. CA publishes surveys and distributes multilingual educational materials in printed form and on the Internet.

Referrals and advice

CA will provide nonlegal advice and referrals on consumer problems. Chinese, English and Spanish are spoken.

(415) 777-9635
(213) 624-8327
TTY: (415) 777-9456
hotline@consumer-action.org

San Francisco

221 Main St., Suite 480
San Francisco, CA 94105
(415) 777-9648
E-mail: info@consumer-action.org

Ken McEldowney
Executive Director

Kathy Li
Director, San Francisco Office

Michael Heffer
Business Manager

Candace Acevedo
Associate Director, S.F. Office

Joseph Ridout
Consumer Services Manager

Nani Susanti
Technical Assistance

Hazel Kong
Office Manager

Ricardo Perez
Mail Room Operations

Joe Caldarola, Sol Carbonell, Ruth Gilbert
Consumer Advice Counselors

Mikael Wagner, Jamie Woo
Consumer Advocates

Kinny Li, Philip Mak, Annie Tran, Dennis Wong, Cui Yan Xie
Support

Los Angeles

523 West Sixth St., Suite 1105
Los Angeles, CA 90014
(213) 624-4631

Cher McIntyre
Director of Advocacy

Claudia Guevera
Consumer Advocate

Washington, DC

P.O. Box 1762
Washington, DC 20013
(202) 544-3088

Linda Sherry
Director, National Priorities
(Editor, Consumer Action News)

Jennifer Daw Holloway
Associate, National Priorities

Healthy Children Organizing Project

221 Main St., Suite 480
San Francisco, CA 94105
(415) 777-9648, Ext. 307

Web site: www.healthychildren.org

Neil Gendel
Director

Consumer Action News is printed by the Alonzo Printing Company, using recycled paper and soy-based ink.

Cold shoulder for ID thieves

States let you freeze your credit report

By Jennifer Daw Holloway

Approximately 9 million Americans fall victim to identity theft each year. And the cost to consumers tops $5 billion annually. How can you protect your credit and financial information from a potential thief? One way is to freeze access to your credit report.

A security freeze locks (freezes) access to your credit report and credit score. Without access to credit information, a business usually will not issue new credit. So anyone who is attempting to steal your identity would be blocked from opening new credit. When you want to get new credit, you use a special number (PIN) to unlock access to the credit file.

"There are really no downsides [to freezing]. Some people ask if it impacts credit scores but it doesn't," says Michelle Jun of Consumers Union.

Jun notes that a freeze will prohibit consumers from getting instant credit. "Some people see that as a downside, but really, how many people should buy a car at a moment's notice?" she asks.

Sixteen states have passed legislation that allows security freezes. However, some states limit the option to victims of identity theft.

If you live in a state that permits freeze protection, the law usually provides that you simply contact the three major consumer credit agencies and request the freeze. Depending on whether you are a victim or not, you may be charged to place the freeze. Most states allow a fee to lift a freeze, either for a set time period or for one creditor. The service costs about $10, but fees vary from state-to-state.

Security freezes don't apply to any person or entity with whom you have an existing account, or to law enforcement agencies and certain governmental agencies that need credit records for investigations and other legal reasons.

Credit freezing is different than fraud blocking, a provision of the federal Fair Credit Reporting Act. Fraud blocks allow victims to suppress fraudulent accounts that are the result of identity theft. Fraud blocking does not prevent identity theft, nor does it prevent the release of a credit report; it only limits fraud-related information from being included in your credit report.

Advocates are pressing Congress to pass a strong federal credit freeze law.

"Really the only way to bar any new accounts from being opened in your name is to implement a freeze," said Consumer Union's Jun. ■

State credit report freeze laws

These states allow you to freeze your credit report, although some of them limit the right to ID theft victims. Some of these states require ID victims to produce police reports and most charge non-victims fees to implement and lift freezes made solely for preventive purposes.

State	Applies To	Effective Date
California	All consumers	Jan. 1, 2003
Colorado	All consumers	July 1, 2006
Connecticut	All consumers	Jan. 1, 2006
Illinois	ID theft victims	Jan. 1, 2006
Kentucky	All consumers	March 24, 2006
Louisiana	All consumers	July 1, 2005
Maine	All consumers	Feb. 1, 2006
Nevada	All consumers	Oct. 1, 2005
New Jersey	All consumers	Jan. 1, 2006
North Carolina	All consumers	Dec. 1, 2005
South Dakota	ID theft victims	July 1, 2006
Texas	ID theft victims	Sept. 1, 2003
Utah	All consumers	Sept. 1, 2008
Vermont	ID theft victims	July 1, 2005
Washington	ID theft victims	July 24, 2005
Wisconsin	All consumers	Jan. 1, 2007

Source: Consumers Union (www.consumersunion.org)

Peeping on kids for profit

By Jennifer Daw Holloway

How much do marketers and web site operators know about your kids? Maybe more than you think.

Kids are big business for businesses—accounting for more than $500 million in household purchases alone. So it's not particularly surprising that information about your children is much sought after for marketing purposes.

But how do companies get this information? *You* might be giving them information about your family. Seemingly benign activities such as registering with certain parenting web sites can put your children's personal information for sale on the open market.

Maybe you'll get a mailbox full of child-related junk marketing or free samples of diapers or lotion—where's the harm in that? But think about this: What if your child's Social Security number falls into the wrong hands? Your child's identity could be stolen and the thieves could obtain credit cards and even get jobs using your child's identity.

Child victims make up only a small percentage of reported identity theft cases (approximately nine million each year) and most of the fraud is committed by family members, but children's ID theft is on the rise.

How do you know if your child's Social Security number has fallen into the wrong hands? It should raise a red flag if financial offers, such as pre-approved credit cards, begin arriving in your child's name. *Parenting* magazine says that if you attempt to establish a financial account for your child and find that one already exists, or if the application is denied due to a poor credit history, your child may be a victim of identity theft. Just the existence of a credit report in your child's name may be an indicator of fraud, because people who have never had or applied for credit don't usually have a credit report.

Don't give out your children's Social Security numbers (SSNs). Even doctors and schools don't need SSNs unless the children are receiving government benefits. Opt out of mailing lists when you open any financial accounts, so you'll be able to spot suspicious mail more easily.

If your child becomes a victim, call one of the three major credit reporting agencies and place a fraud alert. Then the agencies will notify you if anyone tries to obtain new credit within 90 days. The agencies must remove all suspicious activity from your child's report once you prove the child is a minor.

For more information, go to the Identity Theft Resource Center website (www.idtheftcenter.org) or the Federal Trade Commission's Kidz Privacy (www.ftc.gov/kidzprivacy). ■

Protect kids in cyberspace

Most kids today learn to use computers in preschool. This means there are plenty of kid-focused web sites offering games and chat rooms to entice young cyber surfers. Even the Federal Trade Commission (FTC) has a fun site for kids called Kidz Privacy featuring games and other amusing learning tools.

But the Internet can be a dangerous place for kids who don't understand how to protect their privacy. In 1998, the FTC developed rules to protect children on the Internet. The Children's Online Privacy Protection Act (COPPA) mandates that web site operators must:

Federal Trade Commission
www.ftc.gov/kidzprivacy

- Post their privacy policy—including what types of information they collect from minors, how it will be used and whether or not they pass the information on to third parties and obtain parental consent.
- Get parental consent in most cases before collecting or disclosing personal information.

To protect your kids, read the privacy policies posted by their favorite web sites to determine what types of information the sites might be collecting. Then decide whether you want to give consent. If you give consent, you can still say no to having your child's information sold or shared with third parties.

It's okay to change your mind—you can revoke your consent at any time. ■

—J.D.H.

Scammers' tech tricks

Recognize the signs of their deception

By Jennifer Daw Holloway

Scam artists have probably been around since the dawn of civilization. Maybe crooked cavemen who didn't feel like hunting conned their fellow tribesmen out of precious food. These days, scammers aren't after your dinner. They're after your personal information so they can use it for no good. And their techniques, phishing and automated cold calling, get help from sophisticated technology.

Don't get hooked

"We're updating our records, but we couldn't verify your information. Please click here to update and verify your information."

You may have received similar e-mails. It's a scam called "phishing." Phishers send seamless spam or pop-up messages to lure personal information (credit card numbers, bank account information, Social Security number, passwords, or other sensitive information) from unsuspecting victims.

According to the Federal Trade Commission (FTC), phishers send an e-mail or pop-up message that claims to be from a business or organization that you may deal with. This could be an Internet service provider (ISP), bank, online payment service or even a government agency. The message will ask you to "update," "validate," or "confirm" your account information. You're usually directed to a web site that looks legitimate. But it's a fake—set up by crooks who want to steal your identity and run up bills or commit crimes in your name.

The FTC suggests these tips to help you avoid getting hooked by a phishing scam:

• If you get an e-mail or pop-up message that asks for personal or financial information, do not reply. And don't click on the link in the message, either. Legitimate companies don't ask for this information via e-mail.

• If you are concerned about your account, contact the organization mentioned in the e-mail 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 yourself.

• Don't cut and paste the link from the message into your Internet browser—phishers can make links that look like they go to one place, but actually send you to a completely different site.

• Use anti-virus software and a computer firewall—and keep them up to date. Some phishing e-mails contain software that can harm your computer or track your activities on the Internet without your knowledge.

• Never e-mail personal or financial information. E-mail is not a secure method for transmitting personal information.

• If you initiate a transaction and want to provide your personal or financial information through an organization's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a web address (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 check for 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.

• Be cautious about opening any attachment or downloading any files from e-mails, regardless of who sent them, because e-mail addresses can be spoofed. These files might contain viruses or software to hurt your computer's security.

Turn off cold calls

Many reputable companies use cold calling to try to sell their wares or services. We've all gotten the calls—usually as we're sitting down to dinner!

Cold calls are not always from reputable companies. Scammers like to use "autodialers" to troll for marks. These devices are capable of dialing large numbers of random numbers automatically. Unless a company has your prior consent or an "established business relationship" with you, it cannot leave an artificial or pre-recorded message on your phone.

The FTC's Telemarketing Sales Rule gives you many protections against telemarketers:

• You may place your landline and cell phone numbers on the national Do Not Call Registry (www.donotcall.gov). Then all companies with whom you do not have a prior established business relationship will be prohibited from calling the registered numbers.

• Telemarketing calls for numbers not on the Do Not Call Registry are prohibited between 8 a.m. and 9 p.m.

• Telemarketers must tell you if it's a sales call, as well as the name of the seller and what they're selling before they make their pitch. If they're pitching a prize promotion, they must tell you that no purchase or payment is necessary to enter or win.

• It's illegal for telemarketers to lie about their goods or services, earnings potential, profitability, risk, the liquidity of an investment or the nature of a prize in a prize-promotion scheme.

• Before you pay for anything offered by a telemarketer, you must first be given the total cost of the goods, any restrictions on getting or using them and if the sale is final or non-refundable. In a prize promotion, you must be told the odds of winning, that no purchase or payment is necessary to win and any restrictions or conditions of the prize.

• It's illegal for a telemarketer to withdraw money from your checking account without your express, verifiable authorization.

• Telemarketers cannot lie to get you to pay, no matter what method of payment you use.

• You do not have to pay for credit repair, recovery room or advance-fee loan or credit services until after these services have been delivered. ■

Pretexting: How scammers use con games to get your personal information

Your personal information is a potential goldmine for scammers. How can you protect your Social Security number (SSN), telephone records and your bank and credit card account numbers?

Pretexting is the practice of getting your personal information under false pretenses. According to the Federal Trade Commission (FTC), pretexters sell your information to people who want to get credit in your name, steal your assets or investigate you.

Pretexters employ various underhanded techniques to get your personal information. A pretexter might simply call you claiming to be from a survey firm and ask you some questions. Once he has enough information, he can then call your bank and pretend to be you to steal your money. He can gain access to your bank accounts, your Social Security number and your credit report. And then he can steal your identity and set up accounts in your name or even commit crimes.

Pretexting is a con game and it is against the law. Under the Gramm-Leach-Bliley Act, it is illegal for anyone to:

• Use false, fictitious or fraudulent statements or documents to get customer information from a financial institution or directly from a customer of a financial institution.

• Use forged, counterfeit, lost or stolen documents to get customer information from a financial institution or directly from a customer of a financial institution.

• Ask another person to get someone else's customer information using false, fictitious or fraudulent statements or using false, fictitious or fraudulent documents or forged, counterfeit, lost or stolen documents.

Protect yourself

The FTC offers several tips for how to avoid falling victim to a pretexter:

• Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or know whom you're dealing with. Pretexters may pose as representatives of survey firms, banks, Internet service providers and even government agencies to get you to reveal your SSN, mother's maiden name, financial account numbers and other identifying information. Legitimate organizations with which you do business have the information they need and will not ask you for it.

• Be informed. Ask your financial institutions for their policies about sharing your information.

• Review your bank statements carefully and report any discrepancies to the institution immediately.

• Keep items with personal information in a safe place. Before you throw them away, tear or shred your charge receipts, copies of credit applications, insurance forms, bank checks and other financial statements, expired credit cards and pre-screened credit offers you get in the mail.

• Add passwords to 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, your phone number or any series of consecutive numbers.

• Be mindful about where you leave personal information in your home, especially if you have roommates or are having work done in your home by others.

• Find out who has access to your personal information at work and verify that the records are kept in a secure location. ■

— J.D.H.

Privacy

Continued from page 1

facts about what they buy or what hobbies they have, especially if they don't want the companies to do so.

You might not mind getting offers for credit cards in the mail, or hearing about travel opportunities over the phone or by fax. However, many people object to marketers calling them at dinner time, filling their mail boxes with junk mail or sending annoying unsolicited bulk e-mail pitches ("spam").

If telemarketers annoy you, the law gives you the right to ask them to stop calling and to remove your name from their lists. But you can't ask criminals to opt out of their activities. There are many ways that crooks misuse personal information.

Unscrupulous individuals could be accessing information about you in company databases and files and using it to rip you off. Identity theft is a rapidly growing crime. With key facts about you, such as your name, address and Social Security number, impostors can establish credit in your name and charge goods and services.

Thieves create unauthorized credit card transactions and forged checks to steal money from a victim's bank. Employees pilfer records from companies and sell them to criminals. Your personal information can even help burglars find out when you are not at home so they can rob your house. By gaining access to phone numbers or credit card account numbers, unscrupulous companies can make bogus charges to your accounts.

Historically, at times of national stress, First Amendment rights come under pressure. During the "Red Scare" of the early 1920s, thousands were deported for their political views. During the McCarthy period, blacklisting ruined lives and careers. Recently, Americans were appalled to learn that the White House had authorized the National Security Administration to eavesdrop on cell phone calls under the guise of homeland security.

On Jan. 16, 2005, Martin Luther King, Jr. holiday, former Vice President Al Gore delivered a highly acclaimed speech about government privacy invasions before a standing-room-only audience in Washington, DC.

"We … must examine our own role as citizens in allowing and not preventing the shocking decay and hollowing out and degradation of American democracy…," said Gore. "Thomas Jefferson said, 'An informed citizenry is the only true repository of the public will.' America is based on the belief that we can govern ourselves and exercise the power of self-government."

Consumer Action is dedicated to keeping consumers informed about emerging threats to their privacy. The "Take@ction" section of our web site (www.consumer-action.org) lists actions you can take to ensure that our right to privacy remains strong. Please visit often and in, Gore's words, "exercise the power of self government." ■

Join Consumer Action

Consumer Action depends on the financial support of individuals. Members receive a subscription to our newsletter, *Consumer Action News*. New members also receive *How to Complain*. And you'll have the satisfaction of supporting our advocacy efforts, free assistance and referral hotline and distribution of more than two million free educational brochures each year.

• $25, Regular Membership

• $35, Regular Membership (first class mailing)

• $15, Senior or Student Membership

• $10, Low Income Membership

• $50, Corporate Subscription (first class mailing, and all CA press releases)

Or, donate in any amount to our Publications Fund and support free distribution of our materials to consumers.

Mail your check to: Consumer Action, 221 Main St., Suite 480, San Francisco, CA 94105. All donations to CA are tax-deductible. ■

Groups organize to combat online 'phishing' scams

It's time to strike back against the phishers.

With millions of people already victimized by crooks trying to steal personal and financial information, the nation's consumers, corporations and government offices are uniting to take collective anti-phishing actions.

"Phishing" is a massive scam in which identity thieves send e-mails to trick consumers into providing personal information, including bank and credit card account passwords and Social Security numbers. The e-mails are cleverly disguised to appear as if they are legitimate communications from banks, financial service companies, online auctions or government agencies. Once the thieves get the information, they can transfer money out of the accounts or purchase items using credit card numbers or online retail passwords.

The Anti-Phishing Working Group (www.antiphishing.org) says that the word phishing comes from the analogy that Internet scammers are using e-mail lures to "fish" for passwords and financial data from the sea of Internet users.

Phishing attacks are growing quickly in number and sophistication and customers of most major U.S. banks have been hit.

Consumer Action has joined an initiative led by the National Consumers League (NCL), law enforcement, financial services and technical industries to combat this threat. On March 16, the group issued a "call to action," publishing a report filled with recommendations for a comprehensive plan to combat phishing.

The Phishing Report is the result of a comprehensive three-day brainstorming retreat organized last September by NCL, a Washington-based consumer advocacy organization. The report was written by Peter Swire, the C. William O'Neill Professor of Law at the Moritz College of Law of the Ohio State University and former privacy czar under the Clinton Administration.

Consumer Action's Linda Sherry attended the retreat, held on Maryland's Eastern Shore last fall. "This was not a rest-and-relaxation junket," said Sherry. "We were required to adhere to a strict daily schedule. Ideas were flying and enthusiasm was high. The level of expertise in the group was exceptional."

In 2005, phishing scams ranked sixth in Internet complaints to NCL's Internet Fraud Watch program. Phishing attacks are growing quickly in number and sophistication and customers of most major U.S. banks have been hit with phishing attacks. Phishing e-mails that purport to be from brokerages, E-Bay, Amazon.com, Pay Pal and the Internal Revenue Service (IRS) have also duped consumers.

A May 2005 consumer survey by First Data Corp., a retreat sponsor, found that 43 percent of respondents had received a phishing contact, and of those, 5 percent (approximately 4.5 million people) provided the requested personal information. Almost half of the phishing victims (45 percent) reported that their information was used to make an unauthorized transaction, open an account or commit other types of identity theft.

"There is no silver bullet, but there are known responses that need more support and promising new approaches that could help deter phishing," said Susan Grant, director of NCL's National Fraud Information Center.

The report's key recommendations include:

- Create systems that are "secure by design" to make consumers safer online without having to be computer experts;
- Implement better ways to authenticate e-mail users and web sites to make it easier to tell the difference between legitimate individuals and organizations and phishers who pose as them;
- Provide better tools for investigation and enforcement to prevent phishers from taking advantage of technology, physical location and information-sharing barriers to avoid detection and prosecution;
- Learn from the "lifecycle of the phisher" and use that knowledge about how these criminals operate to exploit points of vulnerability and stop them;
- Explore the use of "white lists" to identify web sites that are spoofing legitimate organizations and use "black lists" to create a phishing recall system that would prevent phishing messages from reaching consumers;
- Provide greater support for consumer education with clear, consistent messages and innovative methods to convey them.

The American Express Company, First Data Corporation and Microsoft Corporation sponsored the Phishing Retreat. Retreat participants, who developed the recommendations, represented financial services firms, Internet service providers, online retailers, computer security firms, software companies, consumer protection agencies, law enforcement agencies, consumer and ID theft victim organizations and academia.

To continue the dialogue, NCL is organizing working groups to examine how the anti-phishing strategies in the report can be adopted on a widespread basis.

"There's a role for everyone to play in fighting the bad guys," said Frank Torres, director of consumer affairs at Microsoft.

"The way we get better is through working collectively." ■

Medical records

Continued from page 1

personal health records," said Dr. Deborah C. Peel, chairman of the Patient Privacy Rights Foundation (www.healthprivacy.org), a national consumer medical privacy watchdog group. "Privacy violations will exponentially increase if patients cannot limit which health care businesses and government agencies can access our personal health data over an electronic network."

'Ironclad protections'

Consumer Action joined Patient Privacy Rights and 25 other organizations in a letter to Congress asking for the highest level of privacy protections in the proposed electronic national health care system. The groups held a press conference on Capitol Hill on April 10.

"The intent of the proposed health information technology legislation is to improve health care, reduce medical errors and save money, but we believe that those benefits will be realized only if there are ironclad privacy protections," said Tim Sparapani, legislative counsel for the American Civil Liberties Union. "If we guarantee privacy, it will generate public acceptance, trust and participation in these networks."

The groups cited research that shows people will avoid treatment, be less than truthful about symptoms, omit critical medical data and delay care if they are compelled to share personal medical records over electronic health networks without adequate privacy safeguards.

"We don't want our children to be denied entrance to schools or colleges, be denied their first jobs, be denied the opportunity to own their first home or be denied insurance coverage because businesses have access to their medical records," said Tom McClusky, director of government affairs for the Family Research Council.

The groups urged Congress to:

- Restore patient right of consent.
- Give patients the right to opt-out of having their records in any national or regional electronic health system.
- Give patients the right to segregate their most sensitive medical records.
- Require audit trails of all disclosures.
- Deny employers access to medical records.
- Require that patients be notified of all suspected or actual privacy breaches.
- Preserve stronger privacy protections in state laws.
- Enact meaningful enforcement and penalties for privacy violations.

"2005 is the year that the American public learned that massive security breaches of personal information have made identity theft the number one crime in America," said Marc Rotenberg, executive director of the Electronic Privacy Rights Clearinghouse (EPIC). "We must not allow the most sensitive personal records that exist, our medical records, to go online without adequate privacy safeguards."

EPIC and Patient Privacy Rights have launched an online petition calling for strong medical privacy safeguards. The petition states simply:

- I want to decide who can see and use my medical records.
- I do not want my medical records or those of my family to be seen or used by my employer.
- I should never be forced to give up my right to privacy in order to get medical treatment.

You can sign the petition by visiting www.patientprivacyrights.org on the Internet.

Peel suggests that you do not sign the routine HIPAA privacy notices at your doctor's office. She said that these privacy notices were never meant to constitute consent to share your medical records, as many notices have become. Your signature on the notice should acknowledge only that you were informed about the medical provider's privacy practices, she noted.

According to the Privacy Rights Clearinghouse (www.privacyrights.com), a national advocacy organization based in San Diego, CA, you cannot be denied treatment or health care coverage because you don't sign an authorization. However, you may be prevented from participating in a research trial or enrolling in a health care plan unless you give authorization to share your information. HIPAA requires patients to sign a special authorization to disclose psychotherapy notes and before their health data can be used for certain marketing purposes.

Safeguard your medical history

Your ability to control your sensitive medical information is limited, but according to the Privacy Rights Clearinghouse, you can take steps to guard your medical privacy:

- Read all notices you are asked to sign and question anything you don't understand.
- Talk to your health care provider about the confidentiality of your records.
- Ask how your providers share patient data within the office and with affiliates.
- Read authorizations carefully and don't sign anything if you are not comfortable.
- Ask why your personal health information needs to be disclosed.
- Obtain a copy of your medical records and make sure the information is accurate. Send a written statement to correct any inaccurate information.
- Make sure medical providers understand how you wish to be contacted. For instance, speak up if you don't want to be called at work, or if you prefer that no messages are left on your home phone.
- If you believe your rights have been violated, file a complaint with the medical provider and the HHS Office of Civil Rights. Call 800-368-1019 or visit the Office of Civil Rights web site (www.hhs.gov/ocr/hipaa) to learn how to file a complaint.
- Contact your lawmakers to ask for strong medical privacy laws. ■

Congress eyes electronic health records

Congress couldn't reach agreement on national health care privacy rules under the Health Insurance and Portability and Accountability Act of 1996 (HIPAA). Now the contentious topic is back on the table as government agencies and corporations work to build a national system of shared electronic health records. According to Rep. Patrick Kennedy (D-RI), the nation's health care privacy laws must "at least must be updated to meet the new realities of online, digital clinical health information."

In early April, the House Energy and Commerce subcommittee held a hearing on HR 4157, authored by Rep. Nancy Johnson (R-CT) that would establish an office of "national coordinator for health information technology" in the Department of Health and Human Services (HHS) and require the agency to create a single federal health care IT (Internet technology) privacy standard. The Senate late last year unanimously passed health care IT legislation (S 1418).

Bill Vaughan, a Consumers Union senior policy analyst, told lawmakers at the hearing that the HIPAA privacy provision is "minimalist" and does not do nearly enough to protect patient privacy. Vaughn suggested the federal government should work with states, some of which have higher standards, to set a strong national law.

Rep. Henry Waxman (D-CA) said he is concerned about creating a national health information infrastructure without first setting strong privacy protections.

Rep. Nathan Deal (R-GA), who cosponsored HR 4157, said he believed a health information exchange would be impossible without uniformity in state privacy laws.

Congress also held a recent hearing on legislation that would create electronic health records for millions of government employees and their families. The bill, HR 4859 sponsored by Rep. Jon Porter (R-NV), would use the federal government's purchasing power to encourage the adoption of a national health care IT system.

The Government Accountability Office (GAO) released a report in April calling on HHS to release detailed plans and milestones on health care IT strategy. ■