

Beware of Crooks “Phishing” For Your Personal Information

Classic Telemarketing Scam Making Waves in the Internet Community

Crooks have long used the telephone to “fish” for people’s financial account numbers and other personal information. Posing as well-known companies and counting on the fact that many of the consumers they call may actually have relationships with those businesses, they pretend that there is a problem with their accounts or that they need to confirm their information. If consumers “bite” and provide the information, the thieves can use it to make unauthorized



email brought recipients to a Web site that had the same logo, type style, and colors as the real AOL site — it even had links to real AOL Web pages. But the page on which victims were instructed to enter their personal information was not AOL’s. With the stolen information, the teenager charged online purchases, opened PayPal accounts in the victims’ names, and used their AOL accounts to send scam emails to more consumers. Under a settlement with the **Federal Trade Commission**, he agreed to make restitution and is barred for life from sending unsolicited commercial emails.

Last June, crooks pretending to be from the fraud department of **Best Buy** sent emails to consumers warning that someone was trying to

fraudulently use their credit cards to order merchandise from the retailer and asking victims to click on a link to the company’s Web site — a fake Web site — to confirm their credit card numbers, addresses, etc.

And in another recent case, scammers set up a fake **Massachusetts State Lottery Commission**, complete with the official state seal and picture of the lottery director. They used emails and cellphone text messages to draw people to the site, claiming that they had won the lottery and asking them to provide a credit card number, social security number, and pay a \$100 “processing” fee to collect their winnings.

When you are about to enter financial or other personal information on a Web page, look at the address up top to see if the beginning has changed from “http” to “https” or “shttp.” This indicates that encryption technology is being used to scramble the information so it can be transmitted securely. Your browser may also have security signals such as a padlock that closes or a broken key that becomes whole. But remember, it’s still important to be sure you’re sending your information where you intended it to go!

For a consumer alert from the FTC about “phishing” go to www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm.

charges or debits and impersonate the victims for all sorts of fraudulent purposes.

This type of scam, like many other frauds, has migrated to the Internet. Sometimes referred to as “phishing,” it usually begins with an email that directs the recipient to a phony Web site that looks just like the real thing.

Here is an example: a teenager sent thousands of emails that purported to be from **America Online**, informing consumers that there was a billing problem and that if they didn’t update their billing information they would lose their AOL accounts and access to the Internet. A link in the



How can you avoid being reeled in by a phisher?

- Be wary of emails that come unexpectedly and ask for personal information, especially if it’s information that the sender should already have.
- Contact the company or organization that supposedly sent the email — by phone or by typing in its Web site address, not by clicking on a link provided in the message — to ask if it came from them. If you don’t know the number or Web site address, you can find it by doing an Internet search.
- Report fraudulent or suspicious emails to your Internet service provider.
- Never provide personal information such as credit card numbers by email, even to legitimate companies or organizations, since email is generally not secure.

Dialing Dilemma

Thousands of consumers were surprised to find charges on their telephone bills for access to pornographic Web sites — charges that they never authorized, and that in some cases were made even though no one in their households ever visited the sites. As a result, thirteen states and the federal government have filed suit against **Alyon Technologies**, which provided access to and billing for the Web sites.

The complaints allege that some consumers that were visiting other Web sites were trapped by “pop-up” ads that couldn’t be deleted. Other victims received emails with links to sites that, when clicked on, wouldn’t go away. Once consumers were drawn into the network, a modem dialing program

disconnected them from their regular Internet service providers and reconnected them to the Internet through another phone number at \$4.99 per minute. Investigators with the **New Jersey Division of Consumer Affairs** found that Internet users could download the dialing program without realizing it once they were linked to one of the sites in Alyon’s network.

To make matters worse, the billing system was faulty. It operated by capturing the phone number from which the consumer’s computer was dialing and matching it against telephone subscriber databases that frequently contain errors. According to the **Federal Trade Commission**, many people whose computers never connected to the sites at all

were charged due to billing service errors.

The FTC has obtained a court order requiring Alyon to pay restitution to consumers who file complaints by October 8, 2003. To be eligible, they must show that: the phone number that was billed wasn’t in their name on the date that the service was provided; a minor accessed the site without the permission of the person who is responsible for the phone bill; or the site was otherwise accessed without that person’s authorization. Victims can use the online complaint form at www.ftc.gov or send written complaints to: FTC, Consumer Response Center, Alyon Matter, 600 Pennsylvania Avenue NW, H-130, Washington, DC 20580.

Shielding Yourself from Financial Swindles

The Spring 2003 issue of *Consumer News* published by the **Federal Deposit Insurance Corporation** is devoted entirely to financial fraud — how different types of swindles work and how to defend yourself from them. The FDIC insures deposits at banks and savings associations and supervises banks that are not members of the Federal Reserve System.

There are descriptions of the common cons such as ID theft, advance fee scams, automated payment fraud, and fake cashier checks; ten simple things you can do to fight fraud; and advice about weighing the costs and benefits of buying ID theft insurance. The “Special Report on Fraud” also provides a summary of federal laws that protect victims and a quiz to test your financial fraud savvy.

To get a free subscription to the newsletter: write to FDIC Public Information Center, 801 17th Street NW, Room 100, Washington, DC 20434; call (877) 275-3342; or send an email to publicinfo@fdic.gov.

Bogus Claims for Unclaimed Funds

If you’ve ever lost track of a savings account, an insurance policy, a certificate of deposit, stocks, a security deposit, an inheritance, or other financial account, you’re not alone. Every year property of this type worth hundreds of millions of dollars is abandoned because the owners have moved, passed away, or simply forgotten it. Con artists take advantage of this by offering to help reclaim abandoned property. The **California Attorney General’s Office** recently sued a telemarketing company doing business as **Unclaimed Property Center, Asset Recovery Group**, and several other names, alleging that it falsely promised to find unclaimed property and provide other financial services, and that it obtained social security numbers, mothers’ maiden names, and other sensitive information from consumers that could be used for identity theft.

Fortunately, it’s easy to find lost property yourself. Each state has a law that requires companies to turn forgotten funds over to a designated state agency if the accounts have been inactive for a certain period of time. The state holds the funds in trust — in most cases until the owners are found (the state keeps the interest but the funds themselves don’t go into the general coffers). Items in abandoned safe deposit boxes,

stocks, and bonds may be auctioned off and the proceeds held for the owners.

States try to locate the owners of unclaimed property through publicity — for example, publishing lists of names in newspapers and setting up displays at public events. Some have created searchable databases on the Internet. There are also legitimate companies that help people find their property and inform them about how to claim it. They typically charge a percentage of the total (some states

limit the amount). Look for companies that only charge after you’ve recovered your property and avoid those that demand payment in advance, often a flat fee. Instead of

information about property that belongs to you, they may simply supply you with a list of state unclaimed property offices.

But you don’t need to hire a private company to help you. Contact the appropriate state agency directly, and if you’re entitled to any property, you’ll be given instructions on how to claim it. In most states the process is free; some charge a small handling fee. Since abandoned property is turned over to the state of the owner’s last address, if you’ve moved or you think someone in another state left you property, you might want to

continued, page 3



New Ways to Stop Unwanted Sales Calls

Under new rules by the Federal Trade Commission and the Federal Communications Commission, consumers have more control of their telephones. Starting September 1, 2003, most telemarketers will be required to remove phone numbers that are on the national “do not call” registry from their calling lists. Enforcement begins October 1, 2003.

It’s easy to register your number — and it’s free. You can register now by going to www.donotcall.gov or calling toll-free, 1-888-382-1222. The TTY number for people with difficulty hearing is 1-866-290-4236. To sign up by phone, you must call from the number you wish to register. If you have multiple phone numbers, you can register up to three at a time online; if you’re registering by phone, you must make separate calls from each number. Cell phones can be included. However, business phone numbers can’t be put on the “do not call” registry. There is no charge, and no deadline, to register.

Not all callers are covered. Nonprofit groups, charities, political organizations, and survey companies don’t have to use the national “do not call” list. But there is a special rule for charities that requires them to honor your request if you tell them not to call you again.

Beware of offers to register your number for you, especially for a fee. Con artists use these ploys to get money from consumers or to steal their personal information for illegal purposes. You don’t have to provide lots of personal information to register. The online form asks for your phone number(s) and email address. A response will follow by email providing a link that you must click on within 72 hours to complete the registration. Your email address will be kept secure and not shared with anyone. If you register by phone, you will be asked to enter the phone number you’re calling

from. The system will compare that number with what shows on the “Automatic Number Identification,” a type of Caller ID. If the two match, the number will be registered. No names or other personal information is required. The only information that telemarketers get is the phone numbers to remove from their lists.

Telemarketers that are required to use the registry can call in certain cases even if your number is on it. Companies can call if they have an “established business relationship” with you — if you’ve purchased something from them, received a delivery from them, or made a payment to them within the last 18 months, or if you asked about a product or service or submitted an application for something within the last 3 months. They can also call if they have “personal relationships” with you — friends, relatives, and acquaintances. But you can tell them not to call again. You can also allow companies to call despite the fact that you’re on the registry by giving them written permission. So look at contracts, contest entry forms, and other things you sign carefully to make sure that you’re not giving your OK to call without realizing it.

It may take a while to notice fewer telemarketing calls. Telemarketers that are required to use the national “do not call” registry must check it every three months to remove any numbers that are on their calling lists. If you register before August 31, 2003 you should receive fewer telemarketing calls by October 1. Those who register on or after September 1, 2003 should notice a decline in sales calls within 90 days.

The national registry doesn’t automatically replace state “do not call” lists. Some states plan to transfer numbers on their lists to the national registry, others don’t. You can find out about how the federal rules relate to your state’s law by going to the “do not call” Web site. You can confirm that your number is on the national registry or find out

when your registration expires anytime by going to the “do not call” Web site or calling the toll-free number.

Registration doesn’t last forever.

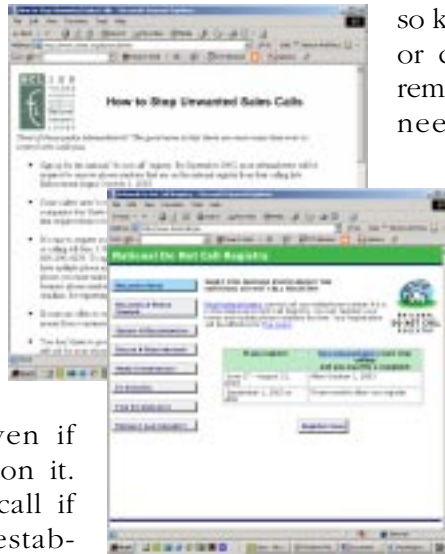
It expires in five years. No notice will be sent to you, so keep your own records or check periodically to remind yourself when you need to renew your registration. You will also need to re-register if you change phone numbers or your number is disconnected. If you no longer want your number on the registry, you can delete it at any time through the Web site or toll-free number. It

may take up to 90 days before telemarketers put you back on their calling lists, if they choose to do so.

Know your rights. If you don’t want to be on the national “do not call” registry, you can still reduce the number of unwanted sales calls you receive by telling companies not to call you again on a case-by-case basis. Keep a record of the company names and the dates of your requests. If you believe your rights have been violated, you can make a complaint through the “do not call” toll-free number or Web site. The FTC and the FCC have both adopted “do not call” rules and will work cooperatively to enforce them. You also have the right to sue telemarketers in your local court for violating the federal Telephone Consumer Protection Act. You can seek up to \$500 per violation, and the court can triple that to a maximum penalty of \$1,500 if the telemarketer knowingly broke the law.

In addition to the information on the “do not call” Web site, more information about your telemarketing rights is available from the FTC at www.ftc.gov/bcp/menu-tmark.htm and its general helpline, 1-877-382-4357, TTY-866-653-4261 (however, if you want to register or complain, you must use the special “do not call” number provided at the beginning of this article). For information from the FCC go to www.fcc.gov/cgb/policy/telemarketing.html or call 1-888-225-5322, TTY 1-888-835-5322.

nclnet.org/donotcall.htm



donotcall.gov

Unclaimed Funds, from page 2

check with the state where you or that person lived. The **National Association of Unclaimed Property Administrators**, an organization of state agencies that hold unclaimed funds, offers advice and links to resources to help you search for your property at www.unclaimed.org.

New Beginning in Fight Against Fraud

The nature and scope of telemarketing and Internet fraud have changed significantly since the **National Consumers League** helped to found the **Alliance Against Fraud in Telemarketing and Electronic Commerce** and launched the **National Fraud Information Center/Internet Fraud Watch** programs several years ago. For example, in 1995, nearly half of all payments in fraudulent telemarketing transactions reported to the NFIC were made by check; by 2002, the most common method of payment had become debits from victims' bank accounts. Another trend is the rising number of fraudulent marketers targeting US consumers from Canada and other foreign countries. New crimes such as online "spoofing" or "phishing" to steal consumers' personal information are proliferating. As a recent report on Mass Marketing Fraud by the **US/Canadian Binational Working Group** stated, we have reached "the end of the beginning." What is the current state of the problem, and what lies ahead?

To help answer those questions, NCL plans a one-day forum on October 28, 2003, in Washington called "A New Beginning: Next Steps in the Fight Against Telemarketing and Internet Fraud." **AARP** is a leading co-sponsor for the forum, which will be held at its Brickfield Conference Center. Participants will be asked to look



with fresh eyes at questions like:

- How do we best marshal our resources to continue to fight telemarketing and Internet fraud?
- Do we know enough about the victims to convey effective anti-fraud messages?
- How does the menace of identity theft relate to telemarketing and Internet fraud?
- How can we deal with the growing problem of cross-border fraud in an increasingly global marketplace?
- As con artists change their methods of operation, how do we need to change our responses?

NCL will present information about emerging trends in telemarketing and Internet fraud. Another highlight of the forum will be the results of new research by AARP designed to improve knowledge about older telemarketing fraud victims and test how well certain educational messages actually help them resist fraudulent pitches. Businesses that facilitate consumer transactions will discuss how these scams impact

them — and what they're doing about it. The important roles of government enforcement action and public education are also on the agenda.

NCL's telemarketing fraud hotline celebrated its tenth anniversary last year, and its Internet fraud program has been operating since 1996. The fraud counselors have given millions of people advice to help them avoid becoming victims and transmitted hundreds of thousands of reports about fraud incidents to law enforcement agencies. And the *www.fraud.org* Web site has received more than 75 million hits.

But while NCL and others have made inroads in the fight against fraud, it's far too early to declare victory. Clearly, new strategies and partnerships are needed. The October forum will provide an opportunity to take stock of our anti-fraud efforts and plan how to meet future challenges. For more information about the forum, go to *www.nclnet.org/aboutforum.htm*.

!!!AAFTEC Alert!!!

The **National Consumers League's Internet Fraud Watch** program warns would-be job seekers about a scam in which they will be both the victims and perpetrators. An overseas company is sending emails to people who use online job posting services proposing a business opportunity to sell expensive items such as plasma televisions through auction sites such as eBay. The company instructs them to set up auction accounts in their names, advertise the merchandise, and direct the buyers' payments to an online payment account that it uses. It promises to pay them \$100 for each item they sell. But the buyers never receive the merchandise, leaving the sellers



Tips for avoiding telemarketing and Internet fraud — including job scams — are online at www.fraud.org.

accused of fraud — and without the promised commissions. These and other Internet scams can be reported to *www.fraud.org*. The information is transmitted to law enforcement agencies.

Membership Info

Want to become a member of the Alliance Against Fraud in Telemarketing and Electronic Commerce? Consumer groups, labor organizations, government agencies, public interest organizations, trade associations and businesses can apply to join. For more information, call the National Consumers League, 202-835-3323 or visit our Web site: *www.nclnet.org*.

Focus on Fraud (ISSN # 1055-4491) is published by the Alliance Against Fraud in Telemarketing and Electronic Commerce. AAFTEC is a coalition dedicated to promoting consumer awareness about telephone and Internet-related fraud. "Focus on Fraud" is published quarterly. Subscriptions are \$9. AAFTEC Chair: Linda Golodner; Writer: Susan Grant; AAFTEC, 1701 K St., NW, Suite 1200, Washington, D.C. 20006.