Don't Take the Bait!

You've probably heard about identity theft — people stealing other people's personal information to use for illegal purposes. In a new scheme called "phishing," ID thieves trick people into providing their Social Security numbers, financial account numbers, PIN numbers, mothers' maiden names, or other personal information by pretending to be someone they're not.

Avoid Getting Hooked by Phishers!

from the National Consumers League

How does phishing work?

- The most common form of phishing is by email. Pretending to be from a legitimate retailer, bank, or government agency, the sender asks to "confirm" your personal information for some made-up reason. Typically, the email contains a link to a phony Web site that looks just like the real thing. You enter your personal information on the Web site — and send it into the hands of identity thieves.
- Phishers also use the phone to hunt for victims' personal information. Some pose as employers and call or send emails to people who have listed themselves on job search Web sites.

How can you tell if the person or company who contacted you is legitimate or a con artist?

- Be suspicious if someone contacts you unexpectedly and asks for your personal information. It's a warning sign that something is "phishy." Legitimate companies and agencies don't operate that way.
- Don't click on links in emails that ask you to provide personal information. To check whether an email or call is really from the company or agency, contact it directly by phone or online. If you don't have the telephone number, get it from the phone book, directory assistance, or the Internet. Use a search engine to find the official Web site;

- Job seekers should also verify the person's identity before providing personal information to someone claiming to be a prospective employer.

What should you do if you got hooked by a phishing scam?

- If you provided account numbers, PINs, or passwords to a phisher, notify the companies with which you have those accounts immediately.
- Put a "fraud alert" on your files at the credit reporting bureaus. For information about how to do that and other advice for ID theft victims, contact the Federal Trade Commission's ID Theft

Clearinghouse at *www.consumer.gov/idtheft* or toll-free, 877-438-4338. The TDD number is 202-326-2502.

- Even if you didn't get hooked, you should report phishing to company or agency that was being impersonated and to the National Consumers League's National Fraud Information Center, *www.fraud.org* or toll-free 800-876-7060. The TDD number is 202-835-0778.

Remember, security tools such as PIN numbers and passwords help keep your transactions safe. Keep them private.

Learn more about how to protect your personal and financial information at ***www.phishinginfo.org***.

National Consumers League
1701 K Street, NW, Suite 1200
Washington, DC 20006

p. 202-835-3323 f. 202-835-0747
email: ***info@nclnet.org***
Web: ***www.nclnet.org***

NCL thanks STAR® Debit and ATM Network for an unrestricted educational grant.

NCL is a 501 (c)(3) nonprofit membership organization.

2004