

# Don't Take the Bait! Avoid Getting Hooked by "Phishers"

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, and other personal information by pretending to be someone they're not.

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 into the hands of identity thieves.

Phishers also use the phone to hunt for personal information. Some, posing as employers, call or send emails to people who have listed themselves on job search Web sites.

- 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, call it directly or go to its Web site (use a search engine to find it);

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

If you provided account numbers, PINs, or passwords to a phisher, notify the companies with which you have those accounts immediately. For information about how to put a "fraud alert" on your files at the credit reporting bureaus and other advice for ID theft victims, contact the Federal Trade Commission's ID Theft Clearinghouse at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) or toll-free, 877-438-4338. The TDD number is 202-326-2502.

Even if you didn't get hooked, report phishing to the company or agency that was being impersonated and the National Consumers League's National Fraud Information Center, [www.fraud.org](http://www.fraud.org) or 800-876-7060, TDD 202-835-0778. More tips about phishing are on [www.phishinginfo.org](http://www.phishinginfo.org).