

Take steps to guard against identity theft

Identity thieves use a variety of schemes to trick people into providing their Social Security numbers, credit card or bank account numbers, passwords, personal identification numbers (PINs), and other personal information.

Once the thieves have this sensitive information, they use it for illegal purposes, such as opening credit card accounts and running up huge, unpaid bills, starting a bank account and writing bad checks, or taking out loans and defaulting on them—*all in your name*.

Anyone with a telephone or email can be a victim, warns the National Consumers League (NCL), the nation's oldest consumer advocacy organization. One of the most common forms of ID theft is called "phishing," which is often done through email. Pretending to be from a legitimate company, financial institution or government agency, the scammer's message asks you to "confirm" your personal information. The message will often use scare tactics—such as saying there is a problem with your last payment, or that your account is about to be closed—to prompt you to respond immediately with the requested information.

Typically, these scam messages contain links to phony websites that look just like the real ones. But when you enter your personal information on the bogus site, the identity thieves now have access to it.

Phishing can also happen by phone. That's why it's important to remember, warns the NCL, that if someone claiming to be from a company with whom you do business contacts you out of the blue, whether

checkmate

News for retirees from

**New York City Comptroller
William C. Thompson, Jr.**

www.comptroller.nyc.gov



by phone or email, and asks for your personal information, it's not likely to be legitimate.

Phishing attempts may be random or may target specific people. For example, some phishers, posing as potential employers, contact people listed on job-search websites to ask for their personal information.

The NCL offers these tips to protect yourself against potential ID theft:

- Be suspicious if someone contacts you unexpectedly and asks for your personal information. 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 website (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 have already provided account numbers, PINs, or passwords to a phisher, immediately notify the companies with which you have those accounts.

In addition to new anti-phishing tips, NCL offers a range of information about other forms of online and telemarketing scams, as well as providing an online form for you to report suspected telemarketing or internet fraud (the information will be transmitted to the appropriate law enforcement agencies), at **www.fraud.org**. You'll also find a toll-free fraud hotline listed.