

## Combating ID theft calls for planning, quick action



Today's technology provides incredible tools for educators and students to improve learning. But the increasing use of the Internet as an educational resource has also led to increasing online use of personal information. Fortunately, you can reduce unauthorized access to personal information with basic counter-measures. And if you become a victim, quick action can limit damage.

- **Use proper disposal techniques**

Old checks, tax returns, credit card statements and similar records should be carefully disposed of, preferably with a cross-cut, fine-size shredder. For hard drives, use a "zero-out" erasure routine to have your computer overwrite deleted data multiple times.

- **Use caution with e-mail**

A strong firewall and related protective software limit attempts to access your PC. So-called malware and spyware may secretly record your online activity or even grant access to your hard drive — exposing credit card numbers, passwords or your Social Security number.

Never open an e-mail from someone you don't recognize. Never click on a link in an e-mail that claims to represent a familiar site. These scams may contain spyware, viruses and other threats. Instead, if you believe the e-mail may be legitimate, open your browser separately and manually enter the known-to-be-valid main e-mail address for the familiar site.

- **Stay alert**

Identity theft may not be obvious for a while. Then you may suddenly receive a surprise warning, such as a "welcome" package in the mail from a company that you normally don't do business with. One overnight shipping company, for instance, recently notified a victim of identity theft that an account had been opened in his name, using one of his credit card numbers.

- **Act quickly if you're a victim**

Contact all companies that granted credit to the ID thief and let them know your identity has been stolen. Cancel all bogus accounts created by the thief. Cancel your credit cards and request new account numbers.

If ID thieves obtained access to your checks or bank accounts, contact the banks, cancel the accounts and open new ones. Place stop-payment orders on the bad checks and let creditors know you've been a victim.

If your driver's license has been stolen, contact the state Registry of Motor Vehicles and request a new driver's license number.

- **Notify credit reporting agencies**

Call the fraud department of at least one of the three major credit agencies to place a fraud alert on your account. By law, the credit agency you contact must inform the other two agencies. Victims are also entitled to free credit reports from the credit agencies.

- **Contact the FTC and police**

Visit the [Federal Trade Commission Web site](#) for practical information on combating ID theft.

Call your local police and report the ID theft. If your local police department doesn't interview you and file a report, contact the state police. A police report furthers your case with creditors.

- **Keep detailed records**

Date and document all events and the names of everybody contacted. This will clearly document a timeline of your actions and may help convince creditors of your innocence.

Because ID theft has increased, there is now insurance to mitigate the effects of the crime. ID theft insurance can cover legal assistance and costs such as time lost from work should you have to visit courts.

With basic precautions and an understanding of how to act quickly if victimized, you can reduce your exposure and potential loss.