



John Bryant
"Your Computer Doctor"
(602) 861-1738
john@helpmedoc.com

Identity Theft Protection

Stay Safe From Phish Tales and Dumpster Dives

Q: "I'm hearing more and more about identity theft, and I'm starting to get nervous. How big of a risk is identity theft and how can I protect myself?"

Clearly, identity theft has become a growing issue of concern. As technology evolves, criminals are creating more and more sophisticated methods of stealing your inner-most secrets ... and your good credit. However, not all identity theft is high-tech. In fact, many of the most devastatingly effective ID theft tactics don't require software, programming skills or even a computer. Here are two very common sources of identity theft, and advice on preventing them from happening.

Dumpster Diving: Dumpster divers use a strategy that is about as low-tech as you can get. They simply pick through your garbage in search of addresses, paperwork, receipts, bank and credit card statements, etc. It's amazing how much personal information gets thrown into the trash.

Defense: Invest \$10.00 - 20.00 into a personal shredder. Shred anything that has your name or address on it before throwing it out. Shred any personal information that is included on solicitation mail or promotion before tossing it into the trash.

Phishing: Online criminals are creating emails that look like an official email from your financial institution. These emails ask you to click on a link and enter your login, password, account information, etc. While they seem very realistic and convincing (often looking exactly like the online website of the real company), these are actually "spoof" emails that are sent out en-mass in order to lure unsuspecting victims. This is called "phishing" because these criminals are casting out "bait" to millions, knowing that a percentage will bite.

Defense: Unexpected emails from your financial institutions are most likely fake. If there is a problem with your account, simply log in to the legitimate website through your browser. Better yet, just pick up your last statement and call the customer service line. *Don't* pass personal information about your account through email and *don't* click on links within suspicious emails. Legitimate financial institutions will never ask for account information by email.

A regular review of your credit report is an excellent way to protect yourself from an unexpected assault on your good credit standing. If you discover a problem with your reports, further damage can be halted by placing a fraud alert through any of the 3 major credit bureaus. Additionally, if you see any unauthorized activity in your financial statements, report it immediately. Fast reporting is a vital step to preventing any long-term damage from identity theft.

Have a question for your Computer Doctor?