Privacy Protection: A 24-Hour News 8 Special Report

Posted: Feb 13, 2008 11:16 PM

Individuals, companies, government and schools are spending more to protect ever-increasing volumes of data. But sophisticated firewalls and encryption might not be enough.

Still, there are things you can do to win the battle against identity theft.

You may be providing information without even thinking about it by using those shopping cards for the grocery, pharmacy, hardware and video store, for sporting goods and books.

Also, for better or worse, access to public records is greater than ever, criminal and civil court records, property records, driver records, and more.

Purdue University information security expert Eugene Spafford believes government and private businesses don't do enough to protect your sensitive information.

"One of the problems with privacy is that once the information's out, it's out," said Spafford.

Indiana University privacy law expert Fred Cate disagrees.

"A lot of data we might think of as sensitive data: Social Security number, credit card numbers or whatever, if you think about it, you provide all the time to other people."

Cate believes Social Security numbers were never intended to be private, just a way to uniquely identify each of us.

But technology has changed how data is collected, how much of it is stored, how it's used and how long it's kept. We want instant access to all our information. That means bad guys are gonna have that type of access too.

Experts say in order to minimize risk watch what you carry in your wallet or purse and ask questions, when you're asked for information.

Also don't give out sensitive information over the phone.

The IRS, your bank, your credit card company won't call you asking for your Social Security number or account information.

Also, don't e-mail sensitive information. Fraudsters send e-mails that tell claim you won the lottery, you got a tax refund or that your bank made an error.

Spafford says to assume that those are fraud.

Don't reuse passwords. Fool the casual criminal by writing the password backwards. Or use a sentence with five or six words with spaces rather than a one-word password.

Also, don't forget to log off your office computer.

"Anyone who comes in your office is you if they can access your computer logged on," said Cate.
Buy a shredder to shred pre-approved credit offers, credit card bills, canceled checks, pharmacy receipts and anything with personal information.

Secure documents like unused checks and other sensitive information in a locked file drawer.

"If we make the data harder to misuse, if we make it harder to use a Social Security number to commit fraud, we make it harder to use a credit card number to commit fraud, that really fights the problem," said Cate.

If you make a mistake or someone steals your information, early detection is critical.

Check your credit card statements and your bank account statements. If someone is making charges or withdrawing money, the sooner you find out about it, the less money you're going to lose. Get your credit report. If you don't check until you need it, you may be too late.

By Rob Youngblood
and Loni Smith McKown
WISH-TV