Stop! ID Thief!

MORE THAN THREE MILLION PEOPLE IN THE United States were the victims of identity-theft-related fraud in the past year, according to a recent survey by the Federal Trade Commission. These people have had accounts opened in their names by scam artists, they've had their names given to the police by crooks stopped for various infractions, and they've had their homes sold out from underneath them. Damages to these victims average more than $10,000 per theft.

Grim as these statistics may be, the growing amount of credit card fraud is even worse: more than five million people had sham transactions dropped onto their credit card statements last year, and more than a million others have had non-credit-card accounts misused, including savings and checking accounts. Fortunately, you can protect yourself using a combination of ingenuity and tech savvy.

The whole foundation of the credit system is fundamentally insecure. A credit card number is really nothing more than a password—a password that's not even secret, because you need to share it in order to use it. Just about the only way that you can detect misuse is to watch your accounts for unauthorized activity.

Keeping such a watchful eye is a lot easier now than it used to be. Credit card companies allow you to view your transactions on secure Web sites. For many people, however, even the few minutes it takes to deal with these sites is a big disincentive. But personal-finance programs like Quicken or Money streamline this process. I use Quicken, which automatically downloads new transactions from my credit cards, bank accounts, and investments with a single mouse click. To use this feature, you first store all of your account numbers and passwords in the program's "PIN Vault." There's no need for you to memorize all those digits: the information is kept encrypted under a master pass phrase.

Getting Quicken set up is only half the battle, of course. You also have to manually review your downloaded transactions every few days to find out if somebody is using your credit card without your authorization. Banks and credit card companies are always looking for fraud as well, but they frequently don't catch it until it is too late. You can nip the problem in the bud by calling up your credit card company and asking for a new account number at the first sign of fraud.

Credit card technology is fundamentally insecure. You can protect yourself by using ingenuity and tech savvy.

Another source of fraud is those "convenience checks" that the card companies send in the mail. Crooks steal them out of your mailbox and go on their own personal spending sprees. Protect yourself by calling up your credit card company and asking them to stop sending the checks. A locked mailbox is a good idea, too. And though it might sound extreme, buy a good crosscut shredder for your receipts; identity thieves have posed as homeless people, rummaging through trash, looking for bank statements and other sources of personal information.

While you have the credit card company on the phone, have them put a password on your account. This replaces your "mother's maiden name" and is much more secure. Finally, ask the credit card companies to stop sharing your personal information with other businesses. This will stop some of the junk mail coming into your house, including those "pre-approved" credit card offers, which are a primary source of identity theft.

Identity theft is generally hard to prevent because it involves new accounts that crooks open in your name, rather than old accounts for which you have the account numbers. Again, the best way to protect yourself is by getting more information. Both Equifax and TransUnion offer credit-monitoring services. For a monthly fee they'll watch your credit file and let you know whenever a new account is opened in your name, or when one of your creditors reports that you're late to make a payment on an already opened account. To notify you, they send an e-mail message that asks you to log in to a password-protected Web site. If you see a suspicious account, you can call up the bank, report the fraud, and try to have the account shut down.

The Equifax service costs $4.95 per month if you want alerts sent within seven days of suspicious activity, $9.95 per month if you want alerts sent within 24 hours. TransUnion charges $10.95 for three months and provides notification within a week. Of course, it is the poor security practices and aggressive sale of credit reports that are largely responsible for the identity theft epidemic in the first place. Still, my advice is to swallow your indignation and sign up for these services.

Finally, don't click on links in e-mail messages from unknown senders. Thieves are sending out messages that look as if they come from PayPal or eBay, then capturing the usernames and passwords of people who attempt to log in to fake Web pages. Avoid this scam by typing the companies' Web addresses directly into your browser rather than clicking on links.

Perils abound on the electronic frontier. Taking a few smart precautions will ensure that you don't have people copping your identity to plunder your bank account and sully your reputation.

Simson Garfinkel is an incurable gadgeteer, an entrepreneur, and the author of 12 books on information technology and its impact.