Steps to protect yourself when your Personal Information has been stolen

No one's immune from the aggravations of potential identity theft.

Last year, millions of employees and consumers were told that their personal information was lost or had been stolen.

When your personal information is stolen, identity theft remains a concern for years. Even if a thief doesn't use your identity as his own, he may, for instance, sell your data to Web businesses that trade in personal information.

The annoying thing is you just don't know. And you never will. But if you are concerned your personal information has fallen into the wrong hands, there are steps you can take to prevent it from being used fraudulently.

Monitor your accounts for any irregularities over the next few years. Sheila Gordon, director of victim services at the Identity Theft Resource Center, recommends that you:

- Check your annual earnings statement from the Social Security Administration and make sure it squares with the money you've earned this year
- Check your 401(k) or other retirement accounts periodically to make sure no one has cashed out or rolled over any of your balance
- Check notices from the IRS that indicate you haven't paid taxes on certain earnings, which may indicate someone is working under your Social Security number
- Check your credit report for any new loans (e.g., home, car, school) taken out in your name or new credit card accounts you didn't open

Put a fraud alert on your credit reports. A fraud alert tells companies that they should call you to verify your identity whenever they check your credit report with the intention of opening an account in your name or making any changes to an existing one.

So, for example, if someone is fraudulently trying to set up a cell phone account in your name, the creditor will call you first.

Put a fraud alert on your credit reports at all three credit bureaus -- Equifax (800-525-6285), Experian (888-397-3742) and TransUnion (800-680-7289).

It's a relatively quick process that you can do by phone via the credit bureaus' automated systems.

You will need to punch in your Social Security number and other identifying information. You'll also be asked to give your phone number. Attorney Mari Frank, author of books on privacy and identity theft, recommends you give your cell-phone number so that creditors can reach you easily.

The fraud alert is free and lasts 90 days. It is recommended you renew that alert every three months for at least a year, since identity thieves may take their time before using your information. A spokesman for Equifax recommends renewing it a couple of weeks before the expiration of the current alert.

Putting an alert on your credit reports should not lower your credit score or prevent you from getting a loan.

The law requires creditors to respond to fraud alerts, but there is no penalty if they don't, that’s why it's important to be vigilant about checking your credit report for suspicious activity every few months.

Order the reports directly from the bureau. Doing so from third parties -- for example, through a lender -- can lower your credit score.
If you live in California, Texas, Vermont or Louisiana, you also are allowed to put a freeze on your credit report -- meaning that no one can view it unless you give them a password to access it, Frank said.

Consider signing up for a credit monitoring service. The service will alert you when there have been major changes in any of your credit reports and may include free access to your credit reports for a period of time.
What it won't do is protect your identity. That is, you will be alerted to changes on your report, but it won't prevent those changes.

Insist on identifiers other than your Social Security number. Request that your health insurer, employer, broker and others use an identifier of randomly selected numbers instead of your Social Security number.

Change your bank account numbers. If you use direct deposit and the data stolen had to do with compensation issues, you might want to change your bank account numbers.
When changing your account, make sure you use a password and Personal Identification Number (PIN) that is not your mother's maiden name, your birth date, your Social Security number or any part of it, or any other easily guessed code.
Once your account is changed, you should receive a new ATM or debit card as well as new checks.
Also, be sure to alert any company whose bills you pay directly from your bank account about the change in account numbers.

Change identifiers on your 401(k), life insurance policy and stock-options brokerage account. Again, if it's primarily HR data that have gone missing, anyone using that information may be able to access your 401(k) account, your life insurance policy or accounts holding your stock options. So it may be worth changing those account numbers and passwords as well.
If it's not possible to change the insurance policy number, ask if it's at least possible to password protect it.

Opt out of pre-approved credit offers. To put a stop to pre-approved offers for credit and insurance -- the majority of which are generated by lenders using information from the major credit bureaus and consumer credit information provider Innovis -- call the Automated Credit Reporting Industry (888-567-8688).