



10 WAYS TO SECURE YOUR INFORMATION

10 WAYS TO SECURE YOUR INFORMATION

1. **Shred All Identifying Documents, Bank Slips, Etc.**

Bank deposit receipts, credit card statements, old documents, anything with sensitive information should be properly disposed of. If you don't have a fireplace, consider investing in a low-cost paper shredder. Identity thieves can learn a lot from rifling through trash -- don't let yours give away your identity.

2. **Shop Online Only on Secure Web Sites**

Shopping online is safe -- when you use secure web pages. Check the bottom of your browser and look for a locked graphic, or look for "https" in the address bar. This means you are on a secure web page and your data is encrypted. Without a secure connection, hackers can eavesdrop on your transaction and grab your private data.

3. **Don't Fall for Phishing Scams**

Phishing is a technique employed by identity thieves through email or online chat services. The thief pretends to represent a company, such as PayPal or your credit card issuer, and informs you that you need to respond with some information or click on a link. The thief may even claim to represent a charity or sweepstakes giveaway. Don't fall for it. Don't respond and don't click the link, even if it appears to be a legitimate link. Responsible organizations will not contact you in this way.

4. **Beware of Telephone Scams**

Never give out personal information over the phone to someone who calls you claiming to represent a bank, credit card company, charity, or other organization. People are not always who they claim to be. You could be talking to a scam artist who is sweet-talking you out of your credit card or bank account number. This is an old scam, but still widely practiced today because it works. Don't let it work on you.

5. **Keep Anti-Virus and Anti-Spyware Software Up to Date**

A computer virus or trojan horse spyware program that sneaks its way onto your computer can compromise your private information. These malicious programs can scan through your entire harddrive and send what it finds out over the internet. To combat this threat, be sure to run an anti-virus program and at least one anti-spyware program, such as Lavasoft's Ad-Aware. These programs will help defend your computer against those who want to compromise it.

6. **Check Your Credit Report**

According to US law every citizen is entitled to one free credit report each year. You can get the free report from the three major credit agencies by going to Annualcreditreport.com. Verify that the information is correct and check for suspicious activity, particularly mysterious new accounts opened. For even better protection, sign up for a service that notifies you when changes occur to your credit report.

7. **Ask About Identity Theft Prevention Procedures**

Ask your bank about what they are doing to combat identity theft. Call your credit card company and find out if you will be liable for fraudulent charges. Ask your employer about what steps are taken to safeguard sensitive employee data. It's your data; you should know how it is managed.

8. Secure Your Important Documents

Your social security card, passport, birth certificate and other identifying materials are highly sought-after by identity thieves and can command top dollar on the black market. Be sure that your documents are safely stored, preferably in a locked box tucked away and out of sight. Do not regularly carry these documents on you. When you travel, pay special attention to securing your passport. Leave it in a hotel room safe at all times.

9. Be Vigilant About Your Social Security Number

Some institutions--insurers, colleges, etc.--prefer to use your social security number as their identification number for you. This is very foolish, as it essentially deprivatizes this number. Because your social security number can be used to gain access to a lot of other private information about you, opt out of allowing institutions to use it. Another number can be substituted instead.

10. Be Careful With Your Mail

Of course tampering with someone's mail is a federal offense, but that doesn't stop people from doing it. Try not to let incoming mail sit in your mailbox for a long time. If you are going to be away, have the post office hold your mail for you. When sending out sensitive mail, consider dropping it off at a secure collection box or at the post office itself.