

Avoiding Identity Theft

Identity theft happens frequently, and it can take up to 18 months to discover you're a victim — and much longer to undo the damage. The following tips will help you avoid becoming a victim of identity theft.

• Data Protection • Privacy • Information Risk Management •
• pragmatic • trustworthy • reliable • secure • dedicated • ethical

1. Vigorously protect your personal information including your credit card, passport, and social insurance numbers, tax information and filings, birth certificate, driver's license, bank and utility account information.
2. Make sure all personal information and photos are deleted from old computers, cellphones and data storage devices before they're discarded, recycled or donated.
3. Limit the amount of personal information you post on the Internet and on social networking sites. Check that photos you post do not contain GPS or geolocation data.
4. Read online privacy policies. Many just indicate how your information will be used.
5. Only carry the identification and credit cards that you really need. Lock the rest away in a safe place.
6. Use strong passwords and encryption on your computers, USB thumb drives, readers, tablets and smartphones.
7. Never give your social insurance number over the phone or by e-mail. Banks and credit card companies don't ask customers to confirm their account or personal information. If you get a call asking that you confirm your personal information, hang up and report it to the police.
8. Buy and use a crosscut paper shredder. Destroy bank statements, receipts, credit card offers, checks and addresses from magazines, envelopes, and packaging.
9. Shred old credit cards and cancel all bank and credit cards that you don't use.
10. Do not give valid personal information to telemarketers, unsolicited sales or marketing contacts, or when completing phone or mail-in surveys.
11. If you make online purchases, use one credit card and reserve it for online activity, and verify that the website is the real thing. Cyber thieves often divert online purchasers to fake websites or use fraudulent security certificates.
12. Do not put your telephone number or home address on personal checks. If a store clerk records your phone number or other details on your check, write a new check.
13. Check your bank statements and credit reports regularly. Promptly investigate any irregularities and transactions you don't recognize.
14. Always maintain detailed financial records — on paper — in case you have to dispute payments you know you did not authorize.
15. Educate your children. Students — carrying their own or their parents' credit and debit cards — often take fewer precautions to protect themselves.
16. Teach children not to discuss personal information or family activities online: Children of all ages divulge personal information about themselves and their families without realizing the potential danger that this creates.