McAfee®

Consumer Threat Notice ** Consumer Threat Notice ** Consumer Threat Notice

Summer Vacation is Prime Time for Identity Theft

- ***While you're away, identity thieves are prowling for your personal information on unsecured wireless networks, at hotels, and in your mailbox, McAfee warns***

Identity theft is a problem that has already affected 11 million adults in the U.S. alone. In fact, by the time you finish reading this sentence, yet another identity will be stolen. But, what many of you may not realize is that summer is a prime season for identity theft since you are often away from home and more lax with your behaviors both online and off.

Identity thieves know that when you go on vacation there's a higher chance that you will logon to unsecured wireless networks at hotels and cafes. They also know that you are more likely to leave sensitive documents at home unattended. Consider this—the most typical methods of identity theft include stealing wallets, rummaging through trash and mail, and stealing information from an unsecured computer. Before you head out of town this summer, learn which behaviors are risky and how to keep your personal information safe year-round.

The Hook: You go out of town and leave your mail piling up at home. Meanwhile, you bring your computer with you and login to banking and other password-protected Web sites from unsecured wireless networks, where cybercrooks can potentially access your personal information. Other vulnerabilities can be accidental when you leave your smartphone or wallet in a cab or unattended hotel room. This is when identity thieves pounce.

The Methods:

1) **Fishing for information in your online and physical worlds**—In some cases, thieves can use online means—such as your social networking status updates—to facilitate their offline crimes. For instance, if you accept friend requests from people you don't know, strangers can potentially find out your address (on your social networking profile page) and see an update that you are "on a two-week vacation" and use that information to steal your mail, including credit card and banking statements.

2) **Watching when you connect**—When you are on the road, you also open yourself up to online threats, such as logging onto unsecured wireless networks where cybercrooks can access personal information stored on your computer, or using unsecured public computers that potentially cache your email and banking passwords, allowing strangers to log into your accounts.

3) **Old-school snooping**—Time-honored methods, such as stealing wallets, rummaging through mail for credit card and banking information, and dumpster diving are still extremely effective. When you are away for home, crooks have greater opportunity to access your at-home possessions, as well as look for opportunities to steal unattended items in hotel lobbies or cafes.

The Dangers: Identity theft can lead to a range of risks, such as loss of money, damaged credit, loss of medical insurance benefits, and even a criminal record if the thief identifies him or herself as you after committing a crime. These dangers are serious and it often takes a long time to clear up the mess—up to three years in the most severe cases.

Bottom Line: Identity theft can happen at anytime—and the risk increases when you are travelling and away from home—so you must take steps to protect your sensitive information both online and offline.

Tips to Avoid Becoming a Victim:

1) If you're going away on vacation, don't post your whereabouts on social networking sites like Facebook and Twitter, where potential identity thieves can learn that you're not at home.

2) Get a friend or family member to regularly collect your mail while you're away from home; when you let your mail pile up, you are making yourself a target for identity thieves.

3) Hotels can be major targets, so make sure to lock up your laptops and smartphones before you leave your room.

4) Be very careful when using unsecured wireless networks in hotels or Internet cafes. Avoid checking your bank account or entering any personal information, and always remember to logout of your email and other password-protected sites. Also, keep in mind that pay-per minute computers in Internet cafes are often infected with malicious software, designed to steal your information.

5) To ensure peace of mind before you travel—and year-round—subscribe to an identity protection service, such as McAfee Identity Protection, which offers proactive identity surveillance, lost wallet protection, and alerts when suspicious activity is detected on your accounts. To find out more, visit http://www.mcafeeidprotection.com

6) For additional tips, please visit to http://www.counteridentitytheft.com

Tips on What to Do If You Have Become a Victim:

You're a victim, now what?

1) If you believe you're a victim of identity theft, place a fraud alert on your credit reports.

2) Contact your bank and credit card companies to let them know that your information has been stolen and close any potentially fraudulent accounts.

3) File a report with the local police and file a complaint with the Federal Trade Commission.

4) Contact the Cybercrime Response Unit at www.mcafee.com/cru, an online help center for advice and technical assistance, if you think you've been a victim of a cybercrime.

###