How to Minimize Your Risk of Identity Theft

On the surface, the TV commercial elicits a chuckle: Two women at the beauty salon sit side-by-side under hair dryers, chatting together. Yet the voices aren’t theirs, but rather those of the thieves who stole the women’s identities.

Ask anyone who has been a victim of identity theft and they’ll tell you it’s no laughing matter. During 2005 alone, 9.3 million Americans fell victim to identity fraud.¹ Most discover it after the fact, when their credit card statements include charges for items they didn’t purchase, or worse yet, when they begin receiving notices from collection agencies.

Although victims usually learn of the crime quickly, it can take a significant amount of time and effort to recover, emotionally as well as monetarily. According to a recent survey of identity theft victims, the emotional impact of identity theft can parallel that of victims of violent crime.²

You Protect Your Patients. Now Protect Yourself.

Identity theft can occur anytime, anywhere—online, in a department store, even in your trash bin. Discarded records often provide an opening for preying criminals. There have been cases in which employees have been bribed to steal information. Thieves have even used camera phones to record personal information while the victim completes a transaction.

Although there is no sure-fire way to prevent someone from stealing your identity, you can reduce the likelihood of becoming a victim by taking steps to protect and monitor your personal information.

Protect Your Electronic Information

Many of the tactics psychologists use for protecting patient information under the Health Insurance Portability and Accountability Act (HIPAA) are also important for protecting your own personal information:

► Use strong passwords on all your accounts. Strong passwords are at least eight characters and include a combination of upper- and lowercase letters and numbers.

► Change your passwords regularly, in your practice and at home.

► Do not use the same password for all of your accounts.

► Update the software on your computer frequently. This includes your operating system, firewall, anti-virus and anti-spam software.

In addition, when you’re online:

► Never open e-mail or download attachments from people you do not know.

► Always use a virus scanner when opening attachments (even if the email comes from someone you know).

► Do not respond to competitions or promotions from random or unfamiliar organizations. This is a ploy that identity thieves often use.

► When making purchases online, look for the site’s privacy policy and a “lock” icon on your browser’s status bar, which tells you that your information will be secure during transmission.

Protect Your Personal Information

► Protect your Social Security number by using it only when absolutely necessary, and never carry your Social Security card with you.

► Do not include your Social Security or driver’s license number on checks.

► Buy a shredder and use it! Your trash could be a goldmine for identity thieves.

► Install a locking mailbox, and take outgoing mail to the post office.

► Monitor your credit report and other public information. There are several ways to do this: You can request your credit report from major credit bureaus including TransUnion, Experian and Equifax. Or you can sign up for identity-theft protection services offered through many banks, financial institutions and independent companies. These services typically help customers protect themselves and assist in recovery efforts should a theft occur. One such company is ID Theft Assist, which offers special discounted pricing to those who purchase a subscription online via APAPractice.org. Check the “ID Theft Assist” section of the APAPractice.org Store for additional information.


By staying alert, taking proactive steps to protect your personal information, and using resources to help with early detection, you can greatly minimize the likelihood of identity theft happening to you.

¹Javelin/Better Business Bureau, 2006
²Identity Theft Resource Center, 2003
How to Minimize Your Risk of Identity Theft

On the surface, the TV commercial elicits a chuckle: Two women at the beauty salon sit side-by-side under hair dryers, chatting together. Yet the voices aren’t theirs, but rather those of the thieves who stole the women’s identities.

Ask anyone who has been a victim of identity theft and they’ll tell you it’s no laughing matter. During 2005 alone, 9.3 million Americans fell victim to identity fraud.¹ Most discover it after the fact, when their credit card statements include charges for items they didn’t purchase, or worse yet, when they begin receiving notices from collection agencies.

Although victims usually learn of the crime quickly, it can take a significant amount of time and effort to recover, emotionally as well as monetarily. According to a recent survey of identity theft victims, the emotional impact of identity theft can parallel that of victims of violent crime.²

You Protect Your Patients. Now Protect Yourself.
Identity theft can occur anytime, anywhere—online, in a department store, even in your trash bin. Discarded records often provide an opening for preying criminals. There have been cases in which employees have been bribed to steal information. Thieves have even used camera phones to record personal information while the victim completes a transaction.

Although there is no sure-fire way to prevent someone from stealing your identity, you can reduce the likelihood of becoming a victim by taking steps to protect and monitor your personal information.

Protect Your Electronic Information

Many of the tactics psychologists use for protecting patient information under the Health Insurance Portability and Accountability Act (HIPAA) are also important for protecting your own personal information:

► Use strong passwords on all your accounts. Strong passwords are at least eight characters and include a combination of upper- and lowercase letters and numbers.

► Change your passwords regularly, in your practice and at home.

► Do not use the same password for all of your accounts.

► Update the software on your computer frequently. This includes your operating system, firewall, anti-virus and anti-spam software.

In addition, when you’re online:

► Never open e-mail or download attachments from people you do not know.

► Always use a virus scanner when opening attachments (even if the email comes from someone you know).

► Do not respond to competitions or promotions from random or unfamiliar organizations. This is a ploy that identity thieves often use.

► When making purchases online, look for the site’s privacy policy and a “lock” icon on your browser’s status bar, which tells you that your information will be secure during transmission.

Protect Your Personal Information

► Protect your Social Security number by using it only when absolutely necessary, and never carry your Social Security card with you.

► Do not include your Social Security or driver’s license number on checks.

► Buy a shredder and use it! Your trash could be a goldmine for identity thieves.

► Install a locking mailbox, and take outgoing mail to the post office.

► Monitor your credit report and other public information. There are several ways to do this: You can request your credit report from major credit bureaus including TransUnion, Experian and Equifax. Or you can sign up for identity-theft protection services offered through many banks, financial institutions and independent companies. These services typically help customers protect themselves and assist in recovery efforts should a theft occur. One such company is ID Theft Assist, which offers special discounted pricing to those who purchase a subscription online via APAPractice.org. Check the “ID Theft Assist” section of the APAPractice.org Store for additional information.


By staying alert, taking proactive steps to protect your personal information, and using resources to help with early detection, you can greatly minimize the likelihood of identity theft happening to you.

¹Javelin/Better Business Bureau, 2006
²Identity Theft Resource Center, 2003