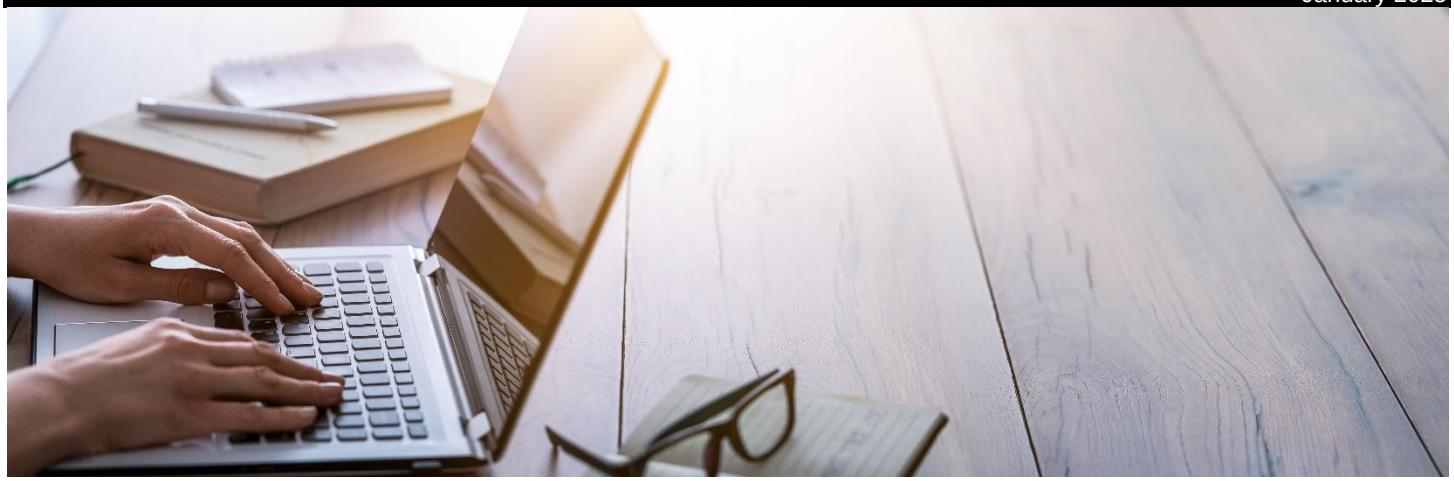
HEALTH ASSOCIATES®
Your Workplace Wellness & EAP Partner

Brought to you by H & H Health Associates

January 2025



Want to Fight I.D. Theft? Be Careful How You Treat Your Information in the Real and Virtual Worlds

Foiling I.D. theft is no longer just a matter of buying a document shredder and keeping track of your receipts - though it helps.

I.D. theft evolves every day and according to security experts, net-savvy thieves are getting more efficient about blending their illegal activity on the ground and online. Here are some examples from Identity Theft Resource Center (ITRC), a non-profit group focusing on the latest I.D. theft trends and assistance for victims:

- I.D. thieves are stealing more paper checks being delivered to homes. Why? Because with the credit squeeze, there are fewer people being approved for checking accounts, so physical checks left in mailboxes are being swiped more frequently so the account numbers can be used to open fraudulent accounts under different names.
- Fraudulent dating, job hunting and social networking Web sites are being used to gather critical data for a host of fraudulent activities. Be careful what you put online.
- Thieves are getting younger since young people are the earliest adapters of online skills. The ITRC notes that arrest records show that younger individuals are getting caught with sophisticated forgery equipment or designing sophisticated online scams.
- Sadly, there are more reports of I.D. theft occurring within families and groups of friends. Individuals are more likely to have their guard down on protection of credit and account data around people they know. Often, such thieves are connected to drugs or other illegal activities being done by their peers.

What can you do? Here are some ideas:

Change your online record-keeping behavior. If you download bank or credit activities to a desktop program like Quicken or Microsoft Money, don't store passwords on that software. It may slow you down but take the time to type in that access data, and then log off as soon as you've completed your transactions and close the browser too. Never put this data on a wireless-enabled computer - I.D. thieves lurk in coffeehouses and other public places to capture data that's traveling through the air. Confine these activities to the desktop and secure terrestrial Internet connections.

Put a lock on your mailbox. If you work long hours or are otherwise not available to grab your physical mail as soon as your letter carrier drops it off, either install a high mail slot on a door with a strong lock (so a thief can't reach in and grab mail that's fallen on the floor), or install an outdoor mailbox with a key lock on it that only you can open. Also, talk to your bank or check printer about secure ways to receive delivery of printed checks.

Shred or cut up any receipts or credit and account documents. A strong, safe paper shredder really is a good investment. What should be shredded: credit solicitations, receipts you're not keeping, line of credit checks that come in your monthly credit card bills (which you shouldn't be using anyway), and tax-related evidence for prior-year returns your tax advisor says you no longer have to keep.

Guard your Social Security number above all. Never, ever share this data unless you are dealing with a recognized financial institution that you trust. Never put it on a check or type it into an online form.

Beware the "Phishermen." Phishing is a process by which scam artists try and get you to divulge your Social Security number, your account numbers, address or other personal information under the guise of a legitimate company you may already be doing business. It's most common over the Internet, but there's no reason why a phishing request couldn't come via direct mail or over the phone. They'll get your attention by saying there's a problem with your account you have to address immediately. Online, the scams are so sophisticated that you'll see e-mails that look exactly like the ones your bank, credit card or even your airline mileage club would send you, right down to the logos and disclaimers. Anytime anyone asks you for personal information, use your own account customer service number (not the one on the mailing) to speak to a live person to verify that the request is real. If it's not, save the evidence - it may help put the con artists in jail.

Change your passwords occasionally. If the only username and passwords you can remember are your e-mail address and your dog's name, you need to develop a schedule for changing those passwords and storing that information in a safe place off your computer. Again, resist storing this information on your computer.

Get each of your credit reports once a year. By law, you're entitled to free copies of your credit report from each of the three major credit rating agencies - TransUnion, Experian and Equifax. Don't get them all at once - stagger them a few months apart so you can see if erroneous data appears throughout the year. Also, if you are on active duty with the military, you can place an active-duty alert on your credit reports to help minimize the risk of identity theft while you are deployed. Active-duty alerts are in effect on your report for one year - if your deployment lasts longer, you can place another alert on your credit report. Couples need to check both reports.

Think twice about I.D. theft insurance. Some companies offer identity theft insurance that will cover lost pay if you have to straighten out your credit but realize they will not do the dirty job of restoring your credit - that's up to you. And since many of the companies selling this insurance are already affiliated with the credit industry, that's good reason for pause. Also, check your home or renter's insurance policy to see if they provide I.D. theft coverage. Most important, be aware that some of the I.D. theft prevention marketers are scams themselves!

Stick with a known ATM. Some of those independent ATMs you see in convenience stores, restaurants and bars may be collecting your data for illegal use. Use ATMs only at established banks.

Watch your wallet and cell phone. Yes, it sounds dumb, but the easiest one-stop opportunity for I.D. thieves to fleece you is sitting in your purse or pocket. Keep only a few necessary items in your wallet and regularly clean out receipts and other data that would identify you. And keep in mind that an Internet- and address book-equipped cell phone is a potential gold mine - they'll not only get your information, but they'll be able to reach all your contacts as well.

What if theft still happens? One of the best resources for a step-by-step guide to fighting identity theft is the Federal Trade Commission and its Web site, www.ftc.gov. The FTC provides a complete listing of contacts and procedures for getting to the bottom of identity theft before the event goes from being serious to devastating.

This column is provided by the Financial Planning Association® (FPA®), the leadership and advocacy organization connecting those who provide, support and benefit from professional financial planning. FPA is the community that fosters the value of financial planning and advances the financial planning profession and its members demonstrate and support a professional commitment to education and a client-centered financial planning process.