By Adam Levin, chairman and co-founder of Credit.com and Identity Theft 911

Your personally identifiable information (PII) is all around you, and much of it is impossible to protect. While your driver's license and Social Security numbers are a significant part of the equation, you can take certain protective measures to keep those from prying eyes. Unfortunately, that's not the case when it comes to more visible forms of PII—like your birthday, email address, home address and even your name. There are criminals out there who see you as their day job, and they know how to use the most gettable pieces of your PII, like your name, to commit crimes.

The fact is, most everyone will experience some form of identity-related compromise during their lifetime. Yes, you most likely will become a victim. The crimes are often hard to detect, but they happen all the time, and there is absolutely no service out there that can give you complete protection from identity-related crimes.

Here are a few ways you can get scammed that only require the clever application of a name, the most basic piece of your PII.

The Grandparent Scam

The first complaints of this scam were logged by the Internet Crime Complaint in 2008, but as the FBI reports, fraudsters working the senior circuit are becoming more sophisticated, using PII gleaned from social media sites to hone their performance.

Typically, a call comes from overseas either late at night or early in the morning, when people aren't thinking as clearly as they might. The caller poses as a grandchild in trouble. There is a request for money, and a plea for secrecy: "Please don't tell mom and dad! They'll kill me." Sometimes an attorney or "an arresting officer" makes the call. Money is wired, and fairly soon after that, the victim comes to realize that he or she has been had.

Variations on the scam include military personnel on leave and friends calling friends. With an increasing number of people oversharing their information on social media, it's not difficult to figure out who will help whom, and when they're away.

What to do: Tighten your privacy on social media; don't share details about vacations, and when anyone asks for money over the phone—even a "family member"— stop, think and don't allow your emotions to drag your good sense and wallet to Western Union.

The Package Scam

Many crimes considered "identity-related" were being perpetrated long before identity theft became part of the national psyche. Stealing mail is one example.

Personally identifiable information has given thievery of mail a real "boost." The latest ploy in urban areas involves the collection of names. Using a notepad, a local thief slipped into a group of condominiums in my neighborhood and started to document who lived where by looking at the junk mail left in the lobby. He used that to gain entry after the courier services made their daily drops. "This is Gary from 2C. Locked myself out. Can you please buzz me in?" In minutes, every package was in his custody and he was gone.

What to do: Don't leave junk mail in your lobby, and urge the building to have a policy that doesn't allow packages to be left unattended.

Will-Call Tickets

I love Broadway and for me there's nothing like being in the stadium to root on my favorite teams—especially when they host my least favorite teams. One thing I try to avoid is picking up tickets at the venue. While many sports arenas are now more careful, requiring ID before handing over tickets, I can't recall the last time I picked up tickets at a theater and was asked for identification. Generally, I give my name, and I get my tickets.

A clever scalper knows you bought tickets for *Aladdin* on Broadway because you tweeted about it. In possession of your name, he or she can grab those tickets and sell them before you arrive.

What to do: Try to avoid will-call tickets by making arrangements to retrieve them in advance or have them delivered digitally or via FedEx/UPS (and make sure they're delivered to a secure location, if not directly into your hands).

Feeling bullied by the specter of such crimes? Don't throw your hands in the air like you just don't care, and never assume that some cure-all service is just a mouse click away. The solution to survive this new reality: Change your behavior.

Identity theft is the third certainty in life, and as such requires vigilance. The solution comes in the form of three M's: Minimize your exposure, monitor for signs of trouble and manage the damage when the inevitable occurs.

Minimizing your exposure comes down to understanding how a thief looks at your information, what that person needs to exploit you, and then making it as hard as possible for them to scam you. Don't overshare information online, on the phone or in your face-to-face interactions.

Monitor your identity in public-facing documents, financial and social networking accounts as well as memberships. Check your credit report as often as you can, use sites like Credit.com to get a free look at your credit scores, and check your bank account and your credit card activity—weekly, if not daily. The more often you do it, the better. Enroll in programs offered by banks, credit unions and credit card companies that notify you of activity in your accounts. Seriously consider buying more sophisticated credit and fraud monitoring programs that give you frequent access to your credit profile.

Manage the damage when you get got. Check with your insurance agent, bank or credit union representative, or the HR department at work to see if you are already enrolled in an identity theft resolution (identity management) program as a perk or at little cost. If you are, take advantage of it. And if you get got, make sure you get on the solution right away, because every moment counts.

In the new landscape of data breaches and ultra-sophisticated criminals, there really is no way to escape all the scams out there. The best thing you can do is keep abreast of the latest trends, be careful, use your head and know how to recognize the telltale signs that you've been had.