Educating the public on the topic of avoiding scams is a priority of the Benton County Sheriff's Office. Thankfully, people can avoid being taken by almost all scams by following the simple rule that states, never give money or personal information to someone who contacts you unexpectedly, regardless of who they say they are. This advice is the equivalent of Preventing Scams 101. The topic of this writing covers those scams that may be a bit more sophisticated and not so obvious. We'll call today's topic Preventing Scams 201.

Most criminals conducting scams work a numbers game. They concoct a thinly veiled reason for seeking money or information from people and contact as many people as possible hoping that they can find that small fraction who will fall victim to their crime. Just as troublesome though are the few criminals out there who employ more crafty methods. They work hard to convince you they are who they purport to be; whether that be a service tech for your cable company, an employee from your credit card company, or perhaps the seemingly nice person you just met online. They are hoping to get you to lower your guard by being friendly, helpful, or perhaps even romantic. However they too are seeking your money or personal information. These criminals fall into one of two categories.

First, we have the information miners. They may begin by asking seemingly innocent questions about your life. What street did you grow up on? What was the name of your first pet? Where did you go to high school? If these questions sound vaguely familiar, you have likely recently registered for an online account somewhere as these are very common challenge questions found online. With the answers to these questions, criminals are one step closer to resetting your passwords and gaining access to your online accounts. While these folks work hard to disguise their personal questions, the best defense against them is to be alert for seemingly out of context personal questions. If you're not sure why the person would be asking for this information, don't give it to them. The next best defense is to have unusual challenge questions in your online accounts. Choose or create questions that are creative and would be unusual for anyone to bring up in conversation. The person you are getting to know might be genuinely interested in what your favorite color is, however, it would be pretty unusual for this same person to ask which compass direction you face in the shower at home. These criminals may also attempt to convince you to divulge personal information such as your Social Security number, credit card number, or banking information. These should be red flag questions regardless of how helpful the person sounds.

Next, we have the long con artists. These criminals are going to work to establish a relationship with their victim and over time steal the victim's money through swindle, lies, and deception. They typically seek to gain the victim's confidence and then spin a sad tale of woe or misfortune. Once they believe they have gained the victim's trust, the criminal will seek the victim's financial help or access to the victim's finances. This criminal will consistently have some problem that needs the victim's attention and financial assistance. Many people have fallen victim to these long con games only to find their bank accounts depleted and their supposed friend or romantic partner suddenly gone. To protect themselves, people should be wary of those who are consistently in need of their financial help and should not give financial information or access to individuals they have only recently met. Also, be on alert for signs that someone you know may be in an exploitive relationship and talk with them about your concerns.

As Minnesotans, it is our nature to be trusting and helpful. While I'm not suggesting we all become cynics and look at everyone as a potential criminal, a phrase made famous by President Regan applies when attempting to discover one of these less obvious scams, "trust, but verify."