

## **Don't Get Scammed**

Kim Flick - MARIELDER'S Transportation Coordinator

04/10/2019

The types of consumer scams and fraud tactics are growing exponentially.

If you feel you'll never be ripped off in one form or another, you're fooling yourself. Your best defense is to arm yourself with information about fraud and scams and follow some basic *do's* and *don'ts* to protect yourself and your family from being victimized.

Seniors are a target simply because they may be less likely to report the crime due to embarrassment, or feeling that it may infer they are no longer capable of managing their own affairs.

So much of our sensitive information is open to hackers online and details of our life are offered up on social media. But even if you do not use a computer or smart phone, you can still be a prime target of door-to-door hucksters, phone scams and even insurance fraud.

Just by opening your door, a crooked contractor can be convincing enough to extract a down payment from you and disappear without doing any work, or do shoddy work that causes even more problems.

Phone scams and robo calls can pressure you into verifying account numbers, wiring money or sending a pre-paid card "right away" to a phony utility rep, fake collections agent or someone posing as a relative in trouble.

Medicare imposters requesting your new 11 digit account number and other sensitive information can lead to identity theft. According to Allianz Life Insurance the average loss to elder victims was \$36,000 – which for many meant financial ruin.

Insurance fraud, involving false claims by policyholders, or unnecessary procedures by providers, indirectly affects consumers through increasing rates to the tune of nearly \$80 billion annually, according to the Coalition Against Insurance Fraud.

“Phishing” is an email cybercrime, but have you heard of “porting”? That’s where your wireless phone gets “hijacked” and your cell phone account gets ported to a new provider, opening your information to the thieves. There are “shimmer” scams that target the chip in your credit cards.

So here are some basics to help you avoid being swindled:

- Do not send money or give out personal information in response to an **unexpected request**. Hang up. Personal information should not be shared freely. If it sounds too good to be true – be wary. Free trials, for instance, can be a set- up for a rip-off. Trust your instincts.
- Do not be **pressured** into making a quick decision. Legitimate agencies will not make such urgent demands.
- Do not automatically click on an email. Check the domain and address. If it doesn’t look genuine or the spelling is off, **err on the side of caution**. By clicking, you may inadvertently download malware onto your computer.
- Be prudent about what you post to social media. Oversharing gives scammers information that can be used to con you.
- Consider lowering credit limits on cards. Close accounts that you no longer use. Check your accounts often to catch suspicious activity.

**The Federal Trade Commission** (FTC.gov/scams) has a list of current scam alerts that is a real eye opener. One of the most comprehensive websites is the **AARP Fraud Resource Center** (<https://www.aarp.org/money/scams-fraud/>), featuring explanations of over forty common scams.

Most of all, keep abreast of what’s going on and enlist the help of a trusted family member or friend to talk about strategies to keep yourself protected.