ARE YOU AT RISK OF FRAUD?

According to a survey by True Link Financial, older Americans are criminally defrauded of **$12.76 billion dollars annually.**

This includes identity theft and all those crazy scams you hear about but smugly think will never work on you.

Do you consider yourself friendly, thrifty or financially sophisticated? If you answered "yes" to any of these questions, then according to that same survey you are more likely to be defrauded because you may give strangers the benefit of the doubt, are more enticed by bargains, and are comfortable moving larger amounts of money around.

1. **Tech Support** – According to Microsoft, last year 3.3 million people were victimized by a tech support con at a cost of $1.5 billion dollars. – Hang up the phone. Neither Microsoft nor their partners make unsolicited phone calls.

2. **Silent Calls**- The phone rings, you pick it up to say "hello" but there is no one on the other line. An automated computer system makes tens of thousands of calls to make a list of humans to target for theft. Put "Caller ID" on your land line, screen your calls and do not pick up the phone if the number is not familiar.

3. **IRS Imposter** - Someone claiming to be from the IRS phones or leaves a message saying you owe back taxes, and threatens that unless funds are wired immediately you will be arrested, or they may say you have a refund waiting but need to verify personal information. Do not return a call from someone claiming to be with the IRS. The IRS opens communication with a U.S. taxpayer only via the U.S. Postal Service.

4. **Cancer Rip-Off** – Last year the Federal Trade Commission (FTC), charged four national cancer charities (Cancer Fund of American, Cancer Support Services, Children's Cancer Fund of America and Breast Cancer Society) with defrauding consumers of $187 million dollars. Before contributing to any charity, check out it's rating on www.charitynavigator.org. Never give cash to door to door solicitors or your credit card number to callers. Ask for information about the charity, (brochures, and websites) so you can investigate the cause first.

5. **ChIp Card** – Bank and credit card companies are currently in the process of issuing customers new "Chip" cards. The FTC is warning that con artists are impersonating card issuers and sending e-mails requesting personal and financial information or asking that you click on a malware laced link before you are issued a new card.

OVER

No credit card company will e-mail or call you to verify personal information it already has on file before mailing a new card. If you are ever unsure, call the number on the back of your credit card.

6. **Medical Identity Theft** - With medical identity theft you can be required to cover the cost of medical services you never received. This can include tests, prescription drugs and even operations. Never surrender your Social Security, Medicare, or health insurance numbers to anyone you do not know. Be wary of free health checks offered at shopping malls, fitness clubs and retirement homes. If they ask to photo copy your medical ID card or sign a blank insurance claim form do not do it.

7. **Counterfeit apps** - In September 2015 news broke that Apple's normally secure App stores had been compromised. Apple said it has purged its stores of these malicious apps but that does not mean it could not happen again. Always read an app's review before downloading and only choose proven popular ones. Be aware that you can limit an apps access to your location by adjusting your devices privacy settings to reduce being spied on.

8. **Gift Voucher** – This rip off involves getting an unsolicited e-mail from McDonald's, Subway, or other popular retailer's offering a free gift card if you click a link to activate it. It's actually a phishing scam where the perpetrator is trying to install malware on your computer or gather personal info by having you complete an online questionnaire. Never click on an unsolicited email or divulge personal info no matter how enticing the offer.

HOW DO SCAMMERS FIND YOU?

1. **Data Purchases** – Scammers buy phone numbers from companies that sell data.

2. **Sucker Lists**-If you have ever been a victim of fraud you are on a so called "sucker" list that are bought and sold among scammers because they are perceived as potential gold mines. Scammers will target victims with a "recovery" scam and pretend to trick you into thinking they will help get your money back.

3. **Volunteered Info**- This is personal information you willing provide by entering giveaways, sweepstakes or when filling our surveys. Scammers use all this data to create profiles for who they want to target. Often they'll target older adults who they perceive as holding the majority of wealth in this country.