

HOW TO AVOID CORONAVIRUS SCAMS

Recently, a “COVID Scams” article was posted, that touched on Robocalls, Social Media Posts, Fake Test Kits, Cures, etc. Sadly, the list of these virus related scams continue to grow . . .

Relief Program Theft: In order to get a piece of government programs intended to help those coping with financial hardships, identity thieves are now stealing unemployment benefits or exploiting small business loan offerings. Additionally, those who receive stimulus payments via debit card, rather than direct deposit, should be aware of scammers who contact you to obtain the card’s information or who indicate there’s a fee to activate the card.

Those small business owners (and their staff) who applied for Paycheck Protection Program loans should be wary of anyone calling or emailing under the guise of a government organization to demand a fee to access the loan or an identifying tax number. REMEMBER, the IRS generally communicates by mail, not by phone or email. Government websites end in “.gov”.

Those currently employed can set up a user name and password at a state employment office website pre-emptively. This means you are using means to begin the process of financial relief if you do lose your job. If a scammer tries to open an account in the name of someone who has already registered, it will set off alarms.

COVID-19 Investment Fraud: Some investors have been duped by companies claiming to offer a product that can detect, prevent, or cure the coronavirus. Cold callers sometimes recommend a medical or drug company stock and suggest that the victim buy it commission free, then dump it once enough people pump up the price. Victims are easier to target more than ever because a relief package approved by Congress in March allows people to withdraw up to \$100,000 from their 401K retirement plans without paying the usual penalty. The best place to check a financial professional’s credentials is on the Financial Industry Regulatory Authority’s BrokerCheck, or the Investment Adviser Public Disclosure website at the Securities and Exchange Commission.

Bogus Meeting Links: Many employees working from home on their personal computers lack the security systems provided by their employers. That makes it easier for scammers to trick people into clicking on faux meeting links as Zoom and other online meeting platforms replace conference rooms. Be wary of these links as they may contain Malware that can be embedded into home computers for the purpose of stealing passwords and other sensitive information. The best protection is vigilance and common sense. Look before you click! The website, virustotal.com can scan links and email attachments to see if there’s anything suspicious about them.

Companionship Schemes: Criminals have preyed on the lovelorn forever, and the pandemic just makes it that much easier. Regulators say that more and more schemers are striking up online romances with the lonely and homebound, with the intent for them to part with their money. Sadly, no consumer-protection website can dissuade someone from draining their life savings in the name of love. Again be wary. If you feel it’s suspicious, and it most likely it is, don’t pursue your quest for companionship on line.

Above information was gleaned from a recent Tampa Bay Times article, “Spot and Avoid Coronavirus Scams”