New COVID-19 Scams Emerging Amidst Uncertainty and Anxiety

As the pandemic escalates, fraudsters have adapted their methods for taking advantage of an anxious and vulnerable population.

One of the newly emerging scams being reported by the Better Business Bureau is a fake "Mandatory Online COVID-19 Test" that looks like it comes from the federal government. A communication is sent via text message or email, impersonating a federal health agency and directing you to a website in an attempt to get your personal information and identifiers like social security number and birth date.

Another scam email takes advantage of the new federal Economic Impact Payment, and tells recipients that they can obtain their stimulus checks faster through the use of an intermediary. Individuals are then directed to a website to enter their personal information. In some cases, the fraudsters actually send a fake check to consumers, asking them to then "verify" their information online in order to cash the check.

In Louisville, Kentucky, the fraudsters took scamming to a new level by erecting a fake COVID-19 testing site in a parking lot, complete with tents and individuals in gowns and face masks testing drive-through customers for \$250 per test.

Be vigilant during these difficult times. Government agencies will not contact you through text, nor will they contact you with .com emails. Be suspicious of any checks you receive in odd increments or requests asking you to verify your personal information. Also, check with your state's Department of Health for the location of authorized COVID-19 testing sites.

Finally, if you feel you have been victimized by identity theft or if you think your banking information was compromised, you should act quickly. Contact www.identitytheft.gov. You can also contact your local police department. You should also reach out to your bank and review your account for any suspicious transactions. The federal Electronic Fund Transfer Act, which applies to consumer accounts, requires banks to conduct an investigation into the suspected fraud if it's reported within 60 days.