



House Budget and Research Office

COVERDELL LEGISLATIVE OFFICE BUILDING, ROOM 412
ATLANTA, GEORGIA 30334
404-656-5050

MARTHA R. WIGTON
DIRECTOR

Consumer Protections: COVID-19 Scams

National and local law enforcement have been warning the public about the infiltration of scams and deceptions related to the Coronavirus (COVID-19) pandemic. The Federal Bureau of Investigation's (FBI) public service announcements are cautioning Americans regarding counterfeit treatments, equipment, and emails appearing from health organizations.¹ The Georgia Attorney General's Office is encouraging Georgians to validate any communications before responding to any suspicious contacts² as hackers are using malicious links or attachments to reveal user names and passwords. The following guidelines help avoid any dangerous exploitation.

Fraudulent COVID-19 Testing

Two types of tests are available for COVID-19: viral tests and antibody tests. A viral test determines if you are currently infected, while an antibody test may tell you if you've been previously infected. Viral tests require laboratory testing to determine results; therefore, any viral test advertising that results can be obtained without the submission of a sample specimen is fraudulent. On the contrary, antibody testing may be performed at home without the request of a sample specimen. The Food and Drug Administration maintains active lists of approved viral and antibody test manufacturers.¹

The FBI has issued warnings for fraudulent COVID-19 antibody testing and has warned the public to be aware of the following indicators of fraudulent activity:

- Claims of FDA approval for antibody testing that cannot be verified;
- Advertisements for antibody testing through social media platforms, email, telephone calls, online, or from unsolicited/unknown sources;
- Marketers offering "free" COVID-19 antibody tests or providing incentives for undergoing testing;
- Individuals contacting in person, phone, or email to inform the government is requiring a COVID-19 antibody test; and
- Practitioners offering to perform antibody tests for cash.²

The FBI is also investigating fraudulent COVID-19 viral test sites and has received reports of such places in Georgia.³ The Georgia Department of Public Health's (DPH) website offers resources to ensure that those seeking a COVID-19 test may do so through reputable sources. Included is a list of testing sites associated with the DPH that provide testing free of charge.⁴

Charity/Donations

Before donating to a charitable organization, review official websites and research how contributions can help affected families or communities. Contact an office for more information on recent projects or programs. At the

Better Business Bureau, the Better Business Bureau Wise Giving Alliance, GuideStar, Charity Navigator, and Charity Watch, criticisms and evaluations are available. It is essential to find the impact of a charity and make sure that donations are helping those who need it most.

Telephone solicitation for contributions should be approached cautiously. If someone is solicited by phone, it is safer to ask for more detailed information about the charity and its services. It is dangerous to give any credit card, debit card, or bank account information to a telephone solicitor. Cash donations or payments to individuals are also questionable. The best way to contribute is by credit card or check directly to the charity, which can be reversed if any suspicious activity is confirmed. The Internal Revenue Service (IRS) has information available on charitable organizations that are eligible to receive tax-deductible contributions.

Stimulus Checks

Georgians should avoid responding to calls, text, or emails asking for personal information or claims offering individuals to receive federal money sooner. The FBI warns of fraud scheme messaging offering cash or a stimulus check from retailers, such as Costco.⁵ The messaging provides a link containing malware, ransomware, or other plans to steal personal data. Any reports that a second round of stimulus checks are now available are false. The IRS will never call to ask for a Social Security number, bank account, or credit card number.

Video Conferencing

While significant strides have been made since the onset of the pandemic, the Federal Bureau of Investigation warns to be cautious when using video conferencing applications. Identified hackers are conducting activities known as "zoom bombing," where cyber scammers hijack online meetings or classes.⁶ Cases have found hackers yelling profanities or displaying inappropriate images during a video conference. Both the FBI and platform software providers recommend sessions should be private and always require a password. Telecommuters should not share links to meetings publicly and should update software regularly. Screen sharing should also have settings to "host-only" to block any uninvited viewers.

Door to Door Deceptions

It is important to remember that most utility companies will work with consumers on payments during the COVID-19 crisis. If someone from a utility company appears at your home demanding payment or threatens to disconnect service, ask for their identification, and call the utility provider. Avoid answering any unsolicited offers or making any payment through mobile applications such as Venmo and Cash App.

Price Gouging

Georgia's price gouging statute (O.C.G.A. § 10-1-393.4) was activated upon the governor's executive order declaring the state of emergency. The law, in conjunction with the executive order, provides that no business or individual may sell any goods or services necessary to support public health at a price higher than the rate at which the products or services were sold immediately prior to the declaration. Prices may only be increased to an amount that accurately reflects the increased cost of the goods or services to the seller or the increased cost of transportation. Retailers may increase the price of products or services if the amount charged is no higher than the value to the retailer of the goods or services plus the retailer's average markup percentage applied during the 10 days immediately before the declaration. Violators may be fined up to \$5,000 per violation.

State Laws Addressing "Phishing"

"Phishing" occurs when bad actors send spam emails, text messages, or links to deceptive websites to steal personal, sensitive, or financial information. The text messages or emails appear dependable, but their purpose

is to collect information for identity theft. Twenty-three states have laws aimed explicitly at phishing schemes. In Georgia, phishing is considered a felony and punishable by no more than 20 years imprisonment, and a fine of no less than \$1,000, nor more than \$500,000, or both.⁸

Financial Crimes Against the Elderly

MetLife Mature Market Institute estimates \$2.6 billion is lost annually by victims of elder financial abuse.⁹ Financial crimes and manipulation included the illegal use of a senior citizen's property or assets. Georgia law establishes adult protective groups to investigate responses of suspected cases of abuse, neglect, or exploitation of the elderly. Fraud or identity theft committed against older adults is not reported often, but 36 states have addressed financial exploitation

Additional information and Resources

The Georgia Attorney General's Office is asking Georgians to continue to stay watchful and only trust reliable sources for updates concerning COVID-19. Scams are occurring that can intrude relief efforts to the pandemic.

To file a complaint with the Federal Trade Commission: www.ftc.gov/complaint

To file a complaint with the Georgia Attorney General's Consumer Protection Division:

- Call: 404-651-8600 inside the metro Atlanta area
- Call: 1-800-869-1123 toll-free outside of the metro Atlanta calling area
- To report suspected scams online, visit www.consumer.ga.gov

References and links

1. Food and Drug Administration, "In Vitro Diagnostics EAUs" September 9, 2020. <https://www.fda.gov/medical-devices/coronavirus-disease-2019-covid-19-emergency-use-authorizations-medical-devices/vitro-diagnostics-eaus>; Food and Drug Administration, "EAU Authorized Serology Test Performance" September 9, 2020. <https://www.fda.gov/medical-devices/coronavirus-disease-2019-covid-19-emergency-use-authorizations-medical-devices/eau-authorized-serology-test-performance>
2. Federal Bureau of Investigation, "FBI Warns of Potential Fraud in Antibody Testing for COVID-19" June 26, 2020. <https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-potential-fraud-in-antibody-testing-for-covid-19>
3. American Association of Retired Persons, "Reports of Fake Test Sites for COVID-19 Emerge Across US" April 9, 2020. <https://www.aarp.org/money/scams-fraud/info-2020/fake-coronavirus-testing-sites.html>
4. Georgia Department of Public Health, "COVID-19 Testing/Direct Patient Lines" September 10, 2020. <https://dph.georgia.gov/covid-19-testingdirect-patient-lines>
5. Federal Bureau of Investigation, Public Service Announcement, "FBI SEES RISE IN FRAUD SCHEMES RELATED TO THE CORONAVIRUS (COVID-19) PANDEMIC," Alert Number I-032020-PSA, March 20, 2020. <https://www.ic3.gov/media/2020/200320.aspx>
6. Federal Bureau of Investigation, "FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic," March 30, 2020. <https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic>
7. Georgia Department of Law, "Carr Warns Georgians about Misinformation Campaigns Designed to Steal, Deceive and Disrupt," March 23, 2020. <http://consumer.ga.gov/news/press-releases/view/carr-warns-georgians-about-misinformation-campaigns-designed-to-steal-deceive-and-disrupt-1>
8. Federal Trade Commission, "Scammers are taking advantage of fears surrounding the Coronavirus," April 7, 2020. <https://www.consumer.ftc.gov/features/coronavirus-scams-what-ftc-doing>
9. GoFundMe, "Helping Our Community During the Coronavirus Pandemic," March 20, 2020. <https://www.facebook.com/gofundme/>
10. Federal Bureau of Investigation, "Protect Your Wallet—and Your Health—from Pandemic Scammers," April 6, 2020. <https://www.fbi.gov/news/stories/protect-yourself-from-covid-19-scams-040620>
11. AL Code § 13A-8-114 (2012).
12. Official Code of Georgia Annotated, 16-9-109.1, (2010).
13. National Committee for the Prevention of Elder Abuse, "The MetLife Study of Elder Financial Abuse," June 2011. <https://www.metlife.com/about-us/newsroom/2009/march/financial-abuse-costs-elders-more-than--2-6-billion-annually--ac/>