

Cyber Scams

Be wary of all emails claiming to be from the Centers for Disease Control and Prevention (CDC), World Health Organization (WHO), and other healthcare organizations, offering to share information about the virus.

Wasden advises residents not to open attachments or to click on links within these emails, as scammers are using phony COVID-19 tracking websites to infect electronic devices with malware, putting residents at risk for identity theft and financial exploitation.

Idahoans should take extra precautions to avoid spoofed or phony websites by only visiting sites with clearly distinguishable URL addresses. Scammers seek to exploit individuals by directing web traffic to similar, but falsely identified website names where they can provide misinformation or attempt to gain consumers' personal information or finances in exchange for pandemic updates.

Be on the lookout for emails asking for the verification of personal data, including Medicare or Medicaid information, in exchange for receiving economic stimulus funds or other benefits from the government. **Government agencies are NOT sending emails asking for residents' personal information in order to receive funds or other pandemic relief opportunities.**

Telephone and Text Messaging Scams

During this difficult time, while working remotely or responding to a larger volume of phone calls, many find it difficult to ignore those from unknown numbers. If you find that you've answered a robocall – **hang up immediately**. Don't press any numbers. Scammers are calling with offers involving everything from COVID-19 treatments and cures, to work-from-home schemes. The recording might say that

pressing a number will direct you to a live operator or even remove you from their call list, but it also might lead to more robocalls.

Similar to email phishing scams, text messages from unknown sources may offer hyperlinks to what appear to be automated pandemic updates, or interactive infection maps. These are just two examples of ways scammers can install malware on your mobile electronic device, putting you at increased risk for identity theft and financial exploitation.

Counterfeit Product Offers & High Demand Goods

Make sure to ignore offers for COVID-19 vaccinations and home test kits. Currently, no vaccines, pills, potions, lotions, medications, or other prescription or over-the-counter products are available to treat or cure the Coronavirus. This applies to offers made online, in stores, by electronic message, or over the phone. The U.S. Food and Drug Administration (FDA) has not authorized any home test kits for COVID-19.

As many have seen firsthand, some consumer products are in extreme demand. Household cleaning products, sanitizers, personal hygiene products, and health and medical supplies may be offered via online or in-person sellers aiming to capitalize on under supplied or unavailable products.

When buying online, be sure to research the seller by searching online for the person or company's name, phone number and email address, plus words like "review," "complaint," or "scam." If everything checks out, pay by credit card as opposed to debit, and keep a record of your transaction. If you are concerned about the pricing of products in your area, contact the Attorney General's Consumer Protection Division by visiting <https://www.ag.idaho.gov/consumer-protection/>.

Bogus Door-to-Door Tests and Virus-related Products

To ensure your personal safety, do not answer the door or allow into your home any unknown individuals or business representatives moving door-to-door offering to sell consumer products, medical kits, vaccines, cures, whole-home sanitization, or in-person COVID-19 testing. Contact local law enforcement to report such activities and, if possible and can be done so safely, alert neighbors, particularly seniors, of these concerning door-to-door offers.

Phony Charities & Donation Requests

Idahoans interested in making charitable donations during the pandemic are urged to be cautious as to where their money is going. Unfortunately, scammers take advantage of generosity by creating fictitious charitable organizations, seeking fraudulent donations by taking money which could otherwise go to those in need.

Be sure to research where a charitable donation is going. Contact the Office of the Attorney General for guidance or verification, or visit the [charities portion of ConsumerResources.org](#) for guidance on charitable giving.

When giving, always do so by credit card or other secure payment processor. **Never** give by gift card, wire transfer, or other anonymous electronic payment processor.

Information & Links

Idahoans can contact the Attorney General's Consumer Protection Division by visiting <https://www.ag.idaho.gov/consumer-protection/> or by calling 1-800-432-3545 (statewide) or 208-334-2424.

For up-to-date information on Idaho's efforts at combating COVID-19, please visit <https://coronavirus.idaho.gov/>. For up-to-date national information on COVID-19, please visit <https://www.usa.gov/coronavirus>.

Additional resources include:

- <https://www.consumerresources.org/>
- <https://www.ftc.gov/>
- <https://www.fbi.gov/>