



City of
Langley Washington

Avoid COVID-19 Scams

Watch out for stimulus payment scams

The federal government is seeing an increase in scams related to federal stimulus payments including phone calls, text messages and e-mails phishing for information. The messaging includes variations of language such as "in order to receive your/your client's stimulus payment via direct deposit, we need you to confirm the banking information" and they are gathering that information via telephone or directing victims to click on a link that takes them to a website where they enter their banking information.

Here are some important things to know:

- The government will not ask you to pay anything up front to get this money.
- The government will not call to ask for your Social Security number, bank account, or credit card number.

If you spot a scam, please tell the [Federal Trade Commission](#). The [Washington State Office of the Attorney General](#) also has information and resources for reporting scams.

COVID-19 Cybersecurity Scams

Cybercriminals are taking advantage of fears surrounding the Coronavirus. Now more than ever, we need to be vigilant looking for online scams. WaTech's state [Office of Cybersecurity is monitoring all activity and is sharing the latest news, updates and resources.](#)

Here are some important tips to follow:

- [Don't respond to texts, emails or calls about checks from the government.](#)
- Ignore online offers for vaccinations and home test kits.
- Beware of emails claiming to be from the CDC or WHO. Use trusted sites like coronavirus.wa.gov and the Washington state [Department of Health website](#) to get the latest information.
- [Be on the lookout for charity scams.](#) Never donate in cash, by gift card, or by wiring money.