Google

How to avoid COVID-19 online scams

Common types of scams

Falsely representing health organizations

Scammers posing as health authorities, such as the WHO or CDC, may offer cures, tests or other COVID-19 information.

Websites selling fraudulent products

Sites might offer hand sanitizer, face masks or other in-demand products that never arrive.

Posing as government sources

Some scams claim to issue updates and payments on behalf of the IRS or local government tax authority.

Fake nonprofit donation requests

Requests for COVID-19 donations to nonprofits, hospitals or other organizations should be checked carefully.

Fraudulent financial offers

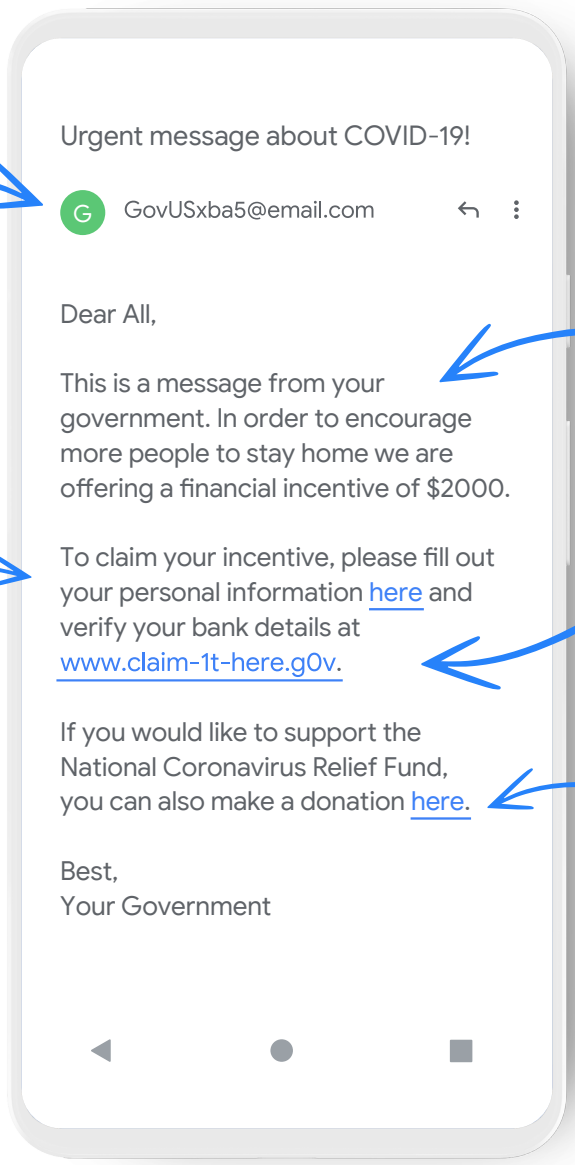
Scammers may pose as banks, investors or debt collectors, with offers designed to steal financial information.

Tips to avoid common scams

Know how scammers may reach you: through email, text messages, automated calls, and malicious websites

Never hand out personal or financial details unless you're sure who you're talking to

Paste portions of suspect messages into search engines to see if they've been reported



Visit authoritative websites directly for the latest updates on COVID-19

Double check links and email addresses before clicking

Donate directly through the charity's website instead of clicking a link sent to you

Add an extra layer of security to your accounts with 2-Step Verification or 2-factor authentication

Report it. If you see something suspicious, report it to justice.gov/coronavirus

For more information on how to avoid COVID-19 online scams visit: safety.google/securitytips-covid19