Google

Helping you avoid COVID-19 online scams

Common types of scams

Stealing your personal data

Scammers who ask for too much information, such as your address, bank account details or even PIN number to “fix” your insurance policy or conduct fake contact tracing

Fake offers of goods and services

Massive discounts on masks or subscriptions to online entertainment services from unknown third parties

Impersonation of authorities

Impersonation of government organisations like MyGov.in or MoHFW offering COVID-19 information

Fraudulent medical offers

Offers of cures, test kits, hand sanitiser or face masks that never arrive

Fake requests for charitable donations

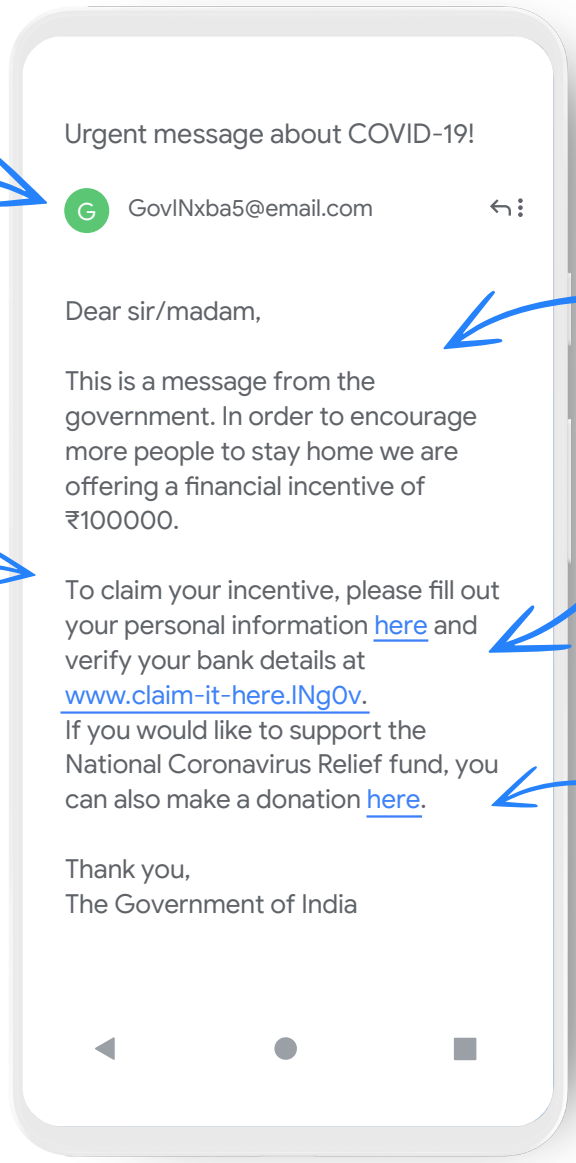
Donations to support COVID-19 relief from non-profits, hospitals, or other organizations should be carefully checked

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, pause and evaluate

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



Check trusted sources directly for the latest updates on COVID-19

Double check links and email addresses before clicking

Donate directly though the nonprofit’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 Authentification

Report it. If you see something suspicious, report it to g.co/ReportPhishing or g.co/ReportMalware

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