



COVID-19 Scams

Tips and Tools to Protect You & Your Loved Ones

April 2020

Learn How to Protect Yourself Against Fraud

Stay Vigilant. From stimulus check scams to phone number spoofing, **scammers are taking advantage of fear surrounding COVID-19.** Remember, neither Apple Bank nor the IRS will call or email consumers and ask for personal account information.



Stimulus Checks: What You Need to Know



Certain U.S. taxpayers will be receiving payments of up to \$1,200 per adult and \$500 per child, with reductions for high earners or other circumstances.

COVID-19 Stimulus Check Scams

Beware of calls, emails, or other communications claiming to be from the IRS Treasury Department offering COVID-19-related grants or stimulus payments. Fraudsters may claim that in exchange for personal financial information, gift cards, or other benefits, they can get you your payment early.

Fraudulent Solicitations: Email, Phone and Text Messages

You should never respond to notifications:

1. Promising a faster stimulus relief payment.
2. Offering vaccinations and/or home test kits.
3. Requesting delivery updates from FedEx, UPS, or the US Postal Service.
4. Asking you to validate/update your personal information, such as
 - Social Security Numbers
 - Account Numbers, Debit/Credit Card Numbers
 - PINs or card expiration dates
 - Billing information
 - Usernames and Passwords.
5. Threatening to close or suspend your account if you do not take immediate action and provide personal information.
6. Requesting payment in the form of:
 - Gift Cards or Bitcoin (Cryptocurrency)
 - Money Transfer Applications (Zelle, Cash App, Venmo, PayPal, or Apple Pay).



Common Types of COVID-19 Scams

- 1. Grandparent Scam:** A fraudster pretends to be a grandchild or other family member who is sick or in the hospital, and convinces the Elder to send money for treatment, or to provide access to their bank or credit card account.
- 2. Email Phishing or Social Engineering:** Scammers pretend to be from the IRS, or other official entities, and send fraudulent emails that request personal information using a fake website link or attachment.
- 3. Health Care Scams:** Scammers pose as Medicare representatives and provide unnecessary/fraudulent services at mobile clinics to try to steal seniors' personal information and bill fraudulent Medicare claims.
- 4. Charity Scams:** Scammers call victims to solicit for fake COVID-19 related charities and pressure them to donate on the spot.
- 5. Tax/IRS Scams:** Scammers claim to be employees of the IRS or another official entity. They advise the victim that money is owed or personal information is needed before receiving a stimulus check.

Protecting Yourself or Your Loved Ones: What Can You Do?

- Avoid clicking on links in unsolicited emails and be wary of email attachments.
- Use trusted sources such as legitimate government websites for up-to-date, fact-based information about COVID-19. Report unsolicited emails to <https://www.ic3.gov/>
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.
- Verify a charity's authenticity before making donations. Review the Federal Trade Commission's page on [Charity Scams](#) for more information.
- Stay informed to avoid COVID-19 scams. Review the [FTC website](#) for more information and examples.
- Know that the federal government, including the IRS, will **NEVER** call you on the phone and ask for personal information or financial information (including your Social Security Number or account numbers).
- If it sounds too good to be true, it probably is.

COVID-19: How We Can Help



- Identify a trusted contact person that the Bank can contact, in the event that we see unusual account activity in your account.
- If you see unusual activity or believe you were a target of a scam and may have provided sensitive information, report it to your Bank immediately.
- For more details and tips, visit Apple Bank's Education Center at <https://www.applebank.com/service/support/education-center> and the Federal Trade Commission website at <https://www.consumer.ftc.gov/features/coronavirus-scams-what-ftc-doing>

COVID-19 Scams: Report Issues and Review Important Information

Agency	Website
Federal Bureau of Investigation Internet Crime Complaint Center (Report Internet crime)	https://www.ic3.gov/default.aspx
Federal Trade Commission (FTC Complaint Assistant)	https://www.ftccomplaintassistant.gov/#crnt&panel1-1
Federal Trade Commission (Consumer Information)	https://www.consumer.ftc.gov/features/coronavirus-scams-what-ftc-doing
Internal Revenue Service (IRS)	https://www.irs.gov/

