

## Banking Tips for Seniors

In response to the COVID 19 pandemic seniors are encouraged to isolate at home to protect their health. However, this arrangement can make them more vulnerable to financial scams. Below are some tips to remind seniors to remain vigilant and avoid scams.



- ❖ **Watch out for phishing scams.** Phishing scams use fraudulent emails, texts, phone calls and websites to trick users into disclosing private account or login information. Do not click on links or open any attachments or pop-up screens from sources you are not familiar with, and NEVER give your password, account number or PIN to anyone.
- ❖ **Keep your computers and mobile devices up to date.** Using the latest security software, web browser and operating system is the best defense against viruses, malware and other online threats. Turn on automatic updates so you receive the newest fixes as they become available.
- ❖ **Change your security settings to enable multi-factor authentication for accounts that support it.** Multi-factor authentication (MFA) is a second step to verify who you are, such as a text with a code.
- ❖ **Recognize and avoid bogus website links.** Cyber criminals embed malicious links to download malware onto devices or route users to bogus websites. Hover over suspicious links to view the actual URL where you will be routed.
- ❖ **Before you make any investments, remember the high potential for fraud right now.** You should be wary of any company claiming the ability to prevent, detect, or cure coronavirus.
- ❖ **Help others by reporting coronavirus scams.** Visit the FBI's Internet Crime Complaint Center at [ic3.gov](https://ic3.gov) to report suspected or confirmed scams. You can also stay up-to-date on the latest scams by visiting the FTC's coronavirus page at [ftc.gov/coronavirus](https://ftc.gov/coronavirus).

If you have any questions please call our Customer First Contact Center at (203) 462-4400  
(Mon – Fri 8:30 a.m. to 4:30 p.m.)

June 29, 2020