First County Bank
It's where you belong.

CustomerFirst
CONTACT CENTER
Weekdays 203.462.4400
Touch Tone 203.462.4300

Elder Financial Fraud in the Digital Age

Each year millions of elderly adults fall victim to financial fraud. While contacting potential victims by phone has been a successful approach, many scammers have branched out to cybercrimes, taking advantage of increasingly sophisticated technology, and growing digital use by seniors. Common scams include:

- Government Imposter: Scammers call pretending to be from the IRS, Social Security Administration, or other government agency and "spoof" the agency's actual phone number.
- Robocalls: Robocalls use automated phone technology to dial large numbers of households from anywhere in the world. One common robocall is the "Can you hear me?" call. When the person answers "yes," the scammer records their voice and uses the recording to authorize unwanted charges.
- Computer Tech Support: A pop-up message or blank screen appears on a computer or cell phone indicating that the device is damaged or infected with malware. When the victim calls the "support number" for assistance the scammer requests remote access and infiltrates the device and/or demands a fee be paid for repairing it.
- Internet Fraud: Pop-up browser windows that look like anti-virus software can fool victims into either downloading a fake anti-virus program (at a substantial cost) or an actual virus that exposes information on the user's computer to scammers.
- Email and Text: Phishing emails and text messages that appear to be from a well-known bank, credit card company, or online store request that an older adult share personal data, such as a log-in, account number and/or Social Security number, to verify that person's account.

PROTECT YOURSELF

- Be extremely cautious of unsolicited contacts. Recognize scam attempts and end all communication with the scammer immediately.
- Search online to verify the contact information (name, email, phone number, addresses) provided by the scammer. Other people have likely posted similar information online.
- Resist pressure to act quickly. Scammers create a sense of urgency to produce fear to lure victims into immediate action. Call the police immediately if you feel there is a danger to yourself or a loved one.
- Never give or send any personally identifiable information, money, jewelry, gift cards, checks, or wire information to unverified people or businesses.
- Make sure all computer anti-virus and security software and malware protections are up to date using only reputable anti-virus software and firewalls.
- Disconnect from the internet and shut down your device if you see a pop-up message or locked screen. Enable pop-up blockers to avoid accidentally clicking on a pop-up.
- Be careful what you download. Never open an email attachment from someone you don't know and be wary of email attachments forwarded to you.

If you have any questions, please call our Customer First Contact Center at (203) 462-4400
(Monday – Friday (excluding bank holidays) from 8:30 a.m. to 4:30 p.m.)

September 11, 2023