Citizens

Protect today, plan for tomorrow.

A fraudster can access your sensitive accounts, perform transactions, and steal money from your accounts. Learn about the latest scams, including those targeting the elderly, and how to avoid them.

What to look out for:

Unsolicited phone calls, text messages, voicemails or emails

Fraudsters might impersonate people you know, trusted companies (like your bank), tech support, investment opportunities, or authorities (with threats of punishment or harm).

Requests for personal information

A common sign of a scam is being asked for sensitive information (such as card numbers, bank details or password information) over the phone, on social media, via text messages or email.

Pressure to act fast on urgent matters

Impostors often fabricate emergency situations (for example, a family member in dire financial need) to get you to act quickly without thinking twice.

Unusual payment requests

Be cautious when asked to send gift cards, make wire transfers or use payment applications because they are difficult to trace and are often favored among scam artists.

Citizens can help protect family finances now and in the future.

Schedule an appointment to speak to a banker.

Reminder: Citizens will never call, text or email you asking for your full account number, username, password, or to initiate a transaction.

2346257_CV25_Elder-Financial-Protection

Citizens

Stop crime: Tips for preventing fraud and scams

Cybercriminals often rely on elaborate lies and manipulation rather than sophisticated technology. Use these tips and tools to help you stay ahead of cybercrime.

Identifying elder financial abuse scams:

Impersonation

The scammer identifies as a grandchild asking for help.

Charity

A scammer pretends to need help with medical or education bills.

Romance

A scammer is looking for love ... and your money.

How to stay safe:

- **Calls:** Always double check with family or call back the person you know directly.
- **Email:** Don't click on suspicious links or attachments.
- **Tech:** Avoid public Wi-Fi when using or reviewing account information.

Cyber security tips and tools:

- **Device Security:** Protect your devices with virus scans and make sure your apps are updated.
- **Passwords:** Refresh your passwords and try not to use one password for multiple accounts.
- **Multi-Factor Authentication (MFA):** Enable MFA on all eligible accounts or devices for an extra layer of security when you log in.
- **Account Management:** Monitor your accounts for any unauthorized transactions or suspicious activity.
- **Payments:** Consider safer ways to pay with Citizens Online℠ Bill Pay or Zelle®. Your Citizens debit card and Citizens Credit Card can also offer protection features.[1]

Notice unusual activity on your account?

Report unauthorized transactions:

For checking, savings, or money market accounts, contact our Fraud Customer Service Center at ***800-922-9999 (option 1, 9, 2).***

For credit card accounts, contact our Credit Card Customer Service Center at ***888-333-0114.***

Scan for more info:

[1]Speak to a banker about secure payment options.

Zelle® and the Zelle® related marks are wholly owned by Early Warning Services, LLC and are herein under license.

2346257_CV25_Elder-Financial-Protection