## WHAT YOU NEED TO KNOW ABOUT ELDER FRAUD



## Criminals will pose as...

- interested romantic partners on social media or dating websites
- technology support representatives and offer to fix non-existent computer issues
- a relative usually a grandchild claiming to be in in immediate financial need.
- a debt collector or IRS representative and threaten to arrest/prosecute unless you agree to pay
- a charitable organization, or claim you have won a lottery or sweepstakes
- a contractor or handyman who charges homeowners in advance for services they never provide
- a Medicare representative asking for your personal information

## How to protect yourself.

- **NEVER** give out your social security number, credit or debit card information over the phone. OFCU and other financial institutions will never call requesting your account numbers, PINs or passwords.
- **Resist the pressure to act quickly!** Fraudsters create a sense of urgency or produce fear to override your common sense.
- If you are not expecting the call, or don't recognize the number, **don't answer the phone.** Let it go to voicemail fraudsters don't leave messages.
- **Don't open attachments or click on links** in emails that you do not recognize. Look for the red flags!
- **Check your account activity** regularly and look for unexpected transactions. Contact your financial institution immediately is you spot suspicious activity.