BETTER CYBER SAFE THAN SORRY

The internet provides opportunities for fun, learning, connectivity and more. But the web also creates a playground for fraudsters. The best defense against scammers is to stay in-the-know about scams and red flags.

PRIMIS

WHAT IS PHISHING?

Phishing is when you get emails, texts, or calls that seem to be from companies or people you know. But they're actually from scammers who are attempting to get you to click a link or share personal information.

KNOW THE RED FLAGS

It can be difficult to recognize phishing scams so look out for these clues.

TEXT	EMAIL	PHONE CALLS
Sharing a special code	Misspelled words	Asking for addresses
Asking for your social security number or account number	Prompts to download an attachment	Using scare-tactics or urgency
Asking for a PIN	Asks to fill out a form	Asking for birthdays

COMMON SCAMS FOR SENIOR CITIZENS

- **Grandchild Scam.** A fraudster calls senior citizens acting as a grandchild or family member, or pretending to call on their behalf. They establish a rapport and ask for money under the guise of helping family.
- **Healthcare Scam**. The scammer may pretend to be a rep from an insurance company or Medicare and attempt to pull personal information. They may press for information claiming benefits are at stake.
- **Romance Scam.** Scammers may prey on older adults, especially if they live alone. Even if the victim is not part of a dating site or service, the scammer may use information on social media to build a phony romantic relationship, and ultimately ask for money.
- **Sweepstakes or Lottery Scam.** Fraudsters call an older adult to tell them they've won a lottery or prize of some kind, but tell the "winner" that in order to claim the prize they must send over money or gift cards up front to cover supposed taxes or processing fees.
- **Government Impersonation Scams.** Scammers call unsuspecting senior citizens claiming to be from a government agency, like the IRS (Internal Revenue Service), Medicare or Social Security Administration. They make false threats, often saying the senior citizen owes money, like unpaid taxes. They solicit money, or information that may be used for identity theft.
- **Tech Support Scams.** Hackers pose as tech support agents that spot a fake virus on the senior's computer or mobile phone. They convince the victim to install a virus protector that actually enables identity theft.

SCAMMERS MAY TRY TO IMPERSONATE PRIMIS REPS!

REMEMBER:

Primis will never send you a text or email asking for account or PIN numbers, social security numbers, or passwords.

HOW TO REPORT FRAUD

VIRGINIA

Consumer Protection Hotline
1-800-552-9963

MARYLAND

Protection Division Hotline
410-528-8662

PRIMIS

MEMBER FDIC