## Stop Scams Now

# Recognize, reject, and report scams at: Meuser.House.Gov/Scar



#### Resist the click

Don't respond to suspicious emails texts or calls.

#### Keep your personal info to yourself

Never share usernames, passwords, card numbers, or codes with strangers.

#### Be careful about public WI-FI

Use a secure connection or VPN when logging into accounts on public networks.

#### Use multi-factor authentication (MFA)

When creating accounts on apps or websites, choose this option and you will always be asked to verify your login with an additional step, like a security code which is texted to you to your cell phone or emailed to your address on file.

#### Monitor your credit score frequently

Sudden drops may signal fraudulent accounts opened in your name.

#### Freeze your credit reports

Stop criminals from opening new loans or accounts in your name.

#### Check more than money accounts

Identity theft can target benefits, medical records, or even your child's information. Be sure to monitor all of the accounts that may have your personal information.

#### Stop using weak passwords

Create strong, unique passwords, or use a password manager.

### If You Think You've Been Targeted, Start Here: These trusted resources can help you recognize, reject, and report scams:

- My Fraud & Scams Page: <u>meuser.house.gov/scams</u>
- PA Attorney General's Office: 800-441-2555
- PA Veterans Scam Assistance: 800-547-2838
- PA E-ZPass Customer Service: 877-736-6727
- Elder Fraud Hotline: 833-372-8311
- FBI Internet Crime Complaint Center (IC3): IC3.gov
- FTC Fraud Reporting: <u>ReportFraud.FTC.gov</u>
- Report Scam Texts: Forward messages to 7726

