# CAPE COD 5 Identifying and Avoiding Financial Scams

## 5 Quick Tips

1. Any unsolicited calls and emails requesting money or gift cards, offering large sums of money or demanding immediate action should be considered a red flag – confirm the information using known contact information for the person or organization.
2. Review the controls you have in place to secure your physical documents and online activity.
3. Empower yourself – stay current by visiting Federal Trade Commission (FTC) and AARP websites.
4. Protect your credit – sign up for a security freeze and check your credit report at least annually.
5. Be an ambassador – share this information with others.

## Best Practices to Protect Yourself from Fraud

### Slow Down

- Urgency and secrecy ("don't tell anyone!") are the scammer's best friend.

### Confirm All Unsolicited Requests

- Be suspicious of unsolicited requests for money, gift cards or personal information, or large offers of money. Confirm all stories, offers or charities independently. Guidestar is one way to confirm legitimate charities (**www.guidestar.org**)
- Never give out your online banking user name/password or other account information – your credentials are just as valuable as money to fraudsters.

### Do Not Trust Your Caller ID

- Phone number spoofing is rampant. Fraudsters can easily mask their number to look like it is coming from someone you trust – a family member, a government agency or even your bank. Do not trust your caller ID to verify a caller.

### Computer Security/Online Activity

- Use up-to-date anti-virus and malware protection – this includes installing the latest software update from your cellular carrier on your mobile phone.
- Create strong, unique passwords for each account (a passphrase is best).
- Never share your passwords.
- Never give unknown people access to your computer.
- "Think before you click" – Advertisements and pop-up windows can be loaded with malware.
- Do not use public wireless for secure transactions such as banking or online shopping.
- Online shopping: log in as a guest and do not save payment information for future use.
- Always log out of a secure session before closing page.
- Back up your system.

*Continued on back*

# CAPE COD 5 Identifying and Avoiding Financial Scams

*Continued from front*

**Social Media/Emails**

- Know the signs of a "phish": Unsolicited emails with generic greetings, embedded hyperlinks or attachments and grammatical inaccuracies can all be phishing indicators.
- Limit personal information shared on social media sites. Fraudsters use everything you post to piece together the 'puzzle' to perpetuate identity theft.

**Physical Documents**

- Pick up home mail delivery as soon as delivered and drop outgoing mail at post office
- Invest in a shredder
- Sign up for USPS Informed Delivery

**Protect Your Credit**

- Order your free annual credit report: **www.annualcreditreport.com**
- Place a free security freeze on your credit report:

**Equifax: www.equifax.com/personal/credit-report-services or call 800-349-9960**
**Experian: www.experian.com/freeze/center.html or call 888-397-3742**
**TransUnion: www.transunion.com/credit-freeze or call 888-909-8872**

## How to Respond to Fraud

If you do become a victim of fraud or identity theft, first – don't be embarrassed – it happens to thousands of Americans every year. Take immediate action; you could potentially recover some money if you act fast!

**Contact:** Your bank, credit card issuer, local police and credit agencies to place a fraud alert or security freeze.

**Report Identity Theft:** IdentityTheft.gov

**Report Fraud:** Federal Trade Commission (FTC)**: www.ftccomplaintassistant.gov** or Federal Bureau of Investigation (FBI): **www.ic3.gov**

## Notes:

.....

.....

.....

.....

.....

.....