## Twelve Simple Steps to Protect Yourself From Cyber Elder Abuse



1. Request a copy of your free credit report at: www.annualcreditreport.com

877-322-8228

- 2. Remove your name / email address from direct mail lists, internet or email adds. Mail a request to: DMA Mail Preference Service, P. O. Box #643, Carmel, NY 10512 / Or log on to: www.dmachoice.org
- 3. Place your name on the **"Do Not Call"** list ~ this will need to be updated quarterly. From the phone number you are registering, call: www.donotcall.gov 888-382-1222
- 4. Remove the name of deceased individuals from mailing lists. Sign up at: <a href="https://www.ms-dm.com/cgi/ddnc.php">www.ms-dm.com/cgi/ddnc.php</a>
- 5. Opt out of pre-approved credit offers <a href="https://www.optoutprescreen.com">www.optoutprescreen.com</a>

888-567-8688

- 6. If using social networking sites, such as *FaceBook*, read the *privacy policy* and avoid posting personal and private information that may inadvertently alert scammers to your family information, whereabouts, income level or possessions.
- 7. Regularly apply *system updates* on all of your devices when you are prompted by your device to do so. This adds another level of security to your phone, computer, tablet, etc.
- 8. Don't give control of your device to a third party who calls you out of the blue to tell you "something's wrong".
- 9. Do not rely on Caller ID alone to authenticate a caller. Criminals can spoof caller ID numbers and they may appear to be calling from a legitimate company or local number when they may not even be in the same country as you are.
- 10. <u>Never</u> provide your password, credit card, Social Security Number, personal or financial information to someone who calls and claims to be from tech or fraud support. No legitimate organization will ask you for this information.
- 11. Lastly, criminals routinely rely on fear to deceive and manipulate you.

  Immediately suspect a crime if you feel confused or wary about a cyber or internet device communication ~ Trust Your Instincts ~ CHECK IT OUT

  Before You Respond!
- 12. If you or someone you know may have been victimized by a cyber fraudster, <a href="mailto:please">please</a> submit a complaint to the Federal Bureau of Investigation IC3 (FBI Internet Crime Complaint Center) at: <a href="https://www.ic3.gov/">https://www.fbi.gov/scams-and-safety/common-fraud-schemes/telemarketing-fraud">https://www.fbi.gov/scams-and-safety/common-fraud-schemes/telemarketing-fraud</a>

WHEN IN DOUBT . . . REACH OUT!