Have you experienced any of these things that affect your vulnerability to fraud?

- Answered the phone, and waited through 3 seconds of silence for someone at the other end to speak?

  Hang up!

  That delay, or the hum of multiple voices in the background, is a sign of computer-dialed calling. At best, it is someone wasting your time or trying to sell you something you don't need, at worst, a scam. Beware assurances that they are not selling anything. If it was someone you would have wanted to speak to, he or she will call you back. We have all been trained to call 9-1-1 in case of a true emergency, so you won't be abandoning a friend or family member. Getting Caller ID can help you to screen out calls. Sign up on the www.DoNotCall.gov list to reduce solicitation calls of all kinds. Since scammers ignore the list, you'll then know you are more likely to be hanging up on a con artist than an ethical business. Get an unlisted phone number for a family member who may have trouble fending off phone solicitations.

- Clicked on something in an email or a screen popup you're not expecting, to investigate it further?

  Take your hand off the mouse or screen, Click on nothing!

Look with your *eyes* first: If an email, look at the sender. Move your cursor over the name without clicking, to see what shows up. Is it exactly the correct full email address of a known person, and not something convincingly similar? Check it against your own separate email address lists. If not a perfect match, don't trust the email! Check it out with a phone call using a number you already had, not by emailing back or using a number supplied in the email in question. If a popup, can you get it to go away by pressing the Escape button on your keyboard or by clicking only the small "X" at the corner of the popup and nothing else? Don't trust anything based on a convincing company or software logo -- they are easy for scammers to copy. Look up the company's contact information using a different resource such as a statement or invoice you already know is real and ask whether the item you received was legitimate.

- Felt unsure about an incoming phone call or email?

  Maybe it seems to be from the IRS, the FCC, Microsoft, Apple, a credit card company, etc., warning you that something is wrong, and you must call or email, or click a link, or else risk a negative outcome?

  Hang up! Delete!

  These entities do not contact their customers or the public in this manner. If you visit their legitimate websites, you will find their assurances that they do not. Tech companies do not reach out or generate popups on your computer originating from their tech support. *Never* respond to an incoming request to "remote in" or be given access to your computer "to help you". Scammers use this technique to steal account information or work you toward eventually giving them credit card or account information in the guise of collecting payment for bogus amounts owed or "support" fees. Tread carefully with items that seem to coincide with something you just did or bought recently, such as upgrading software or a phone, shipping, filing taxes, or donating to disaster relief. Because they are events many people are doing around the same time, it's ripe for a scammer to exploit because when they refer to it, it seems familiar to you. Finally, ***never*** put financial or credit card account numbers, social security numbers, or Medicare numbers in an email!

- Entertained a charitable solicitation or any offer over the phone or via email?

  Extract yourself from the situation! The harder they push, the more suspect they are!

  You deserve time to deliberate; the charity's not going to shut down in the next five minutes; they can move to the next person on the list.

  1. Remember that you should never give your credit card or account information over the phone for a purpose you did not yourself initiate at that moment, even if it sounds vaguely familiar.

2. Check the charity's legitimacy and effectiveness in using donations at charitywatch.org or charitynavigator.org. Ask solicitors whether they are paid to solicit and how much, along with the tax ID of the charity. If they can't tell you, hang up. Be sure to pause and consider any request within your overall plans for giving this year before doing anything.
3. Think first whether you truly are interested in a product or service. Find another way to research it from an independent and legitimate source, off the phone.
4. Hang up on, delete, and shred any credit card offers. When you need one, you will comparison shop for it at your own pace using better resources.

- Forwarded an email that contains pictures, video or links in it that you didn't put there personally?
  Got it as a member of an email group?

  Wait! First always examine it. Clean it up for the safety of anyone about to get it next. Don't forward any bogus email itself as your way of warning someone about it -- you may just have passed to them an embedded virus or a scammer headache.

  Mouse/move your cursor over, without clicking, the entire email from top to bottom to see where there are active links and whether you can tell where they go. If what they do is unclear, or they are not needed, delete anything that's a link or not needed. Better still, copy and paste only what you want into a brand-new email rather than forwarding.

  If someone sent you a link to something you want to share further, try to send the browser address for the item in a new email instead. (Right-click on the link, Select Copy Hyperlink, click in the body of your new email, Right-click and select Paste-Keep Text Only.) The recipients will copy and paste that URL address string into their browsers.

  Be sensitive to others' need for privacy and protection against email fraud – Avoid letting group email addresses be visibly broadcast unnecessarily: consider using BCC "blind carbon copy" when you address an email to a group; remove addresses from the email string when you forward content to someone outside of the earlier group.

- Went for months without looking carefully at your financial account, bank, or credit card statements for anything that looks "off"?

  Consider whether procrastination may have gotten out of hand, or maybe you need occasional assistance from a trusted family member or appropriate professional such as lawyer, accountant, or financial adviser.

- Got a check with an offer to become a Secret Shopper, or from an online sale?

  If you get a check in the mail for being a secret shopper, and then are told to wire or send money back, it's a scam! Scammers might send you a check in the mail with a job offer as a secret shopper. You deposit the check and the funds

become available. Your first assignment may be to “test the money transfer service” in a store by sending some of the money you deposited. In many cases, when the bank finds out the check is a fake, the scammers will be long gone. When selling items online, watch out for bogus checks – have them checked at the bank before sending the item to the purchaser.

- Thought about checking on your credit report this year, but didn’t?

  These are now free, so that reason to put it off is gone.

  Even if you don’t anticipate needing any credit, a review can allow you to see fraudulent credit activity committed in your name.

For more information, visit www.consumerfraudreporting.org.