Online Safety for Everyone

Unfortunately, there are lots of criminals who prey on naïve people to steal their money. Here are some simple guidelines for avoiding trouble when you are using computers and the Internet.

1. **Phone calls asking for money**
   a. Explain that you are not donating money to politicians or organizations on a phone call to you. You can write down the name of the organization and then donate online once you learn more.
   b. Use the *Better Business Bureau's* evaluation of the organization before donating. Type < bbb name > in GOOGLE to find the BBB evaluation; e.g., <bbb dav >.
   c. Find the organization's website yourself before donating.
2. **Using e-mail safely**
   a. Do not open e-mail messages from complete strangers unless you are a public figure.
   b. Do not open attachments from anyone unless you are expecting them; if you are in doubt when you receive a cryptic message from someone you know that has an attachment, ask them personally if they actually sent it and what it is.
   c. Discard all messages that warn you of terrible things but have no specific date or source, that urge you to send them to everyone you know, or which promise you money for nothing.
   d. Do NOT click on ANY links in suspicious messages.
   e. Even if a message seems to be from a friend and it includes a link, hover your mouse cursor over the link to see exactly where it goes. If it's supposed to go to YouTube, be sure it does – not to some random address that may be controlled by criminals who are faking the origin of the e-mail.
3. **Advance-Fee Fraud**
   a. These frauds are called also called Nigerian 4-1-9 Scams based on a law in Nigeria.
   b. Messages from strangers ask you for help supposedly from people who have stolen or inherited or are distributing large amounts of money and want to share it with you. These are all scams. No one gives away millions of dollars to random strangers!
   c. The victims are pressured to send hundreds of dollars (usually using money cards they buy at a store) to the criminals – and they lose it all.
   d. Sometimes the victims give the criminals access to their bank accounts, Social Security numbers and so on. Awful! **Don't do that!**
4. **Refund scams**
   a. Start with e-mails supposedly from Paypal, VISA, MasterCard, Geek Squad, McAfee, Norton, Amazon and so on but actually coming from a GMAIL, HOTMAIL, or other non-business account claiming that you have been charged hundreds of dollars for nonexistent purchases. They include a phone number you can call to "cancel the charge."

Online Safety for Everyone

b. If you get such a message call the supposed company yourself using the phone number you FIND BY YOURSELF (e.g., on the back of your credit card, on a previous statement, or by looking it up using GOOGLE). NEVER CALL A PHONE NUMBER IN A SUSPICIOUS MESSAGE
c. The criminals will tell victims to allow *remote access* to the victims' computer, whereupon the criminals can do anything they want, including copying bank information, logging into a bank account, and so on.
d. The criminals will ask for your password(s). **NEVER GIVE ANYONE YOUR PASSWORD**. If a legitimate helper or technician YOU CALLED needs access, change your password yourself, give them the new one, then change it again to a new one after they finish their work.
e. Sometimes the criminals will falsely show the victim that they have "accidentally refunded more money than intended" by using an image they have modified and tell the victim to go personally to their bank immediately to order a wire transfer to the criminals to refund the nonexistent deposit.
f. Anyone yelling at you on the phone to get money to them is a criminal.

5. **Do not forward e-mail warnings** about *anything computer-related* – especially warnings about stuff you don't have any technical knowledge about such as new viruses.
6. **So what should you do to protect your system?**
   a. First, find someone in your family or friends who is technically knowledgeable.
   b. Make sure that you (or your helper) install a good antivirus program and keep it up to date all the time (pay the modest yearly license fee and get over it!). Examples include BitDefender, McAfee, Norton and others.
   c. Install *only one* antivirus program: having more than one can cause problems.
   d. Activate the *firewall* program (possibly with help) on your computer and be sure that all your ports are closed and invisible using a tool such as GRC.COM's ShieldsUp test (free) < https://www.grc.com/x/ne.dll?bh0bkyd2 >.
   e. Lock your computer *automatically* when you are away for more than a reasonable period (e.g., 20 minutes) so that no one can pretend to be you online and do bad stuff in your name which can get you in trouble.
7. **Ignore threats to reveal your non-existent porn habit – it's a scam**
   a. Criminals send email at random claiming that they have recorded the recipients watching porn.
   b. They demand blackmail money – or they will spread the "info" around.
8. **TELL YOUR [GRAND]KIDS NEVER TO SEND NUDE PICTURES OF THEMSELVES TO *ANYONE*.**
   a. It's a Federal crime to make, send or receive child pornography.
   b. Kids who have sent their nude pics to their friends have found those pics on the Internet or used to blackmail their families.