Technology Dos and Don'ts

Dos

Be suspicious – Don't trust any email that you receive without taking a close look at it first. Poor grammar and vagueness are good clues that an email might be a fake. Some can be very convincing though. When you have even the slightest doubt, please contact the sender to make sure the email is legit. Google also has a nice Phishing quiz here…

https://phishingquiz.withgoogle.com/

Sign up for credit monitoring – A lot of credit card companies are now offering free credit monitoring with their cards. Personally I use Discover Card's . Anytime I apply for a new credit card I always get an email from Discover letting me know somebody used my Social Security Number to apply. If you don't have a credit card that provides that service for free, there's a good chance you're eligible for 10 years of free credit monitoring due to the Equifax breach. They're also offering up to $125 if you turn down the monitoring service. Unfortunately, that amount will most likely drop as more people sign up. You can check your eligibility here…

https://eligibility.equifaxbreachsettlement.com/en/eligibility

Consider Freezing your credit – If you do have concerns about somebody opening accounts in your name it is possible to freeze access to your credit reports by contacting the 3 major credit bureaus. The downside is if you need to unfreeze them to open a new line of credit, it will take a few days to go into effect.

Sign up for USPS Informed Delivery – A relatively new scam involves the US Post Office. You can now sign up for Informed Delivery. Every day they'll send you a picture of what mail you'll be receiving that day. That's good because if something is missing you'll know it. It's bad because crooks have been signing up as other people. So if something valuable will be arriving at your house, they'll know before you do. The good news is once you sign up as yourself nobody else can.

Backup your files – I can't tell you the number of times the people have brought me a computer with a dead hard drive or a flash drive that's be run over by a car. At that point it's usually too late to save the files. Please make copies of any files that are important to you. The best practice is to keep the backup detached from your computer, that way if your computer gets a virus it won't spread to the backup device.

Don'ts

Click on links in emails if you don't have to – Better safe than sorry on this one. For example, if you get an email that says you have a message from a Chase Bank and it tells you to click a link, don't click on the link. Instead, type chase.com in the address bar of your browser.

"Unsubscribe" from Spam – Unless you're sure an email is from a legit company, don't unsubscribe. That's just letting them know you really exist and they'll bombard you with even more spam.

Text "stop" – Same thing with the ever-increasing text message spam. The last thing you want them to know is that you read the last one.

Log in to accounts on public computers – If you need to print something at a hotel/library/store, be prepared with an extra email account just for that purpose. You can just forward what you need to be printed to that email address and delete it after you print. If the account is hacked due to the public PC being compromised, no harm is done.