Security / Phishing

Phishing:
Attempt to obtain information such as username, password or credit card details to steal your money or sensitive data by disguising a link in an email, on a website, on an ad, or by instant messaging.

Email Spoofing:
An email with a forged email address. No sure way to know if the From, Reply-to or Sender is actually who it appears to be. Must use judgement in determining if email can be trusted. If not sure, contact the person, but do not contact using the questionable email's reply-to or forward.

Note:
'bankofamerica' is an example, this could also be 'yourbank' (replace your bank's domain in these examples)

Notice misspelled URLs:
correct: http://www.bankofamerica.com/
incorrect: http://www.bankofamerlca.com/ (notice the lowercase L in amerlca)

Notice use of subdomains (www.subdomain.domain.com) in URLs:
The domain comes right before the '.com'. There can be many valid subdomains that divide up a larger domain. To deceive users, a scammer's domain (securelogin) will add a subdomain (bankofamerica) that looks like a reputable domain (bankofamerica).
correct: https://www.securelogin.bankofamerica.com/
incorrect: https://www.bankofamerica.securelogin.com/

Notice displayed text for link:
displayed: button 'Click to go to Bank of America'
actual: http://www.scammersfakebankofamerica.com/ (hover over)

Do not click on links to a secure site:
Never click on a link from your email, a webpage, or an ad, to go to a secure site like your bank. Your bank and other secure sites are **NOT** going to send you an email with a link to a secure login. Type the site into a search engine if you don't know the url. Save the link as a bookmark for re-use.

Use Ad Blockers:
Recommend Adblock Plus and uBlock Origin Install using your browser's add-ons options. Some ads are malicious and clicking on them may enable damaging downloads to your computer. Ad blockers will block most of those, will not block all ads, but do block those that they already know are malicious.

Backup your data:
Ransomware will ask you for money to get use of your computer again. If you have personal data that is stored elsewhere, documents, photos, etc, then you can just reinstall your operating system and restore your data. Else, you will have to pay the ransom or lose the data. Ransomware can come from ads, letting someone remote into your computer, or a flash drive.

Do not give out your password:
The IRS, credit card company, or bank will not ask for your ID, password, Social Security number, or drivers license number. They will not ask for payments. Don't use a debit card online. Credit card online is normally safe when using a secure site.