The purpose of this PSA is to reduce the amount of scam communications you receive as well as make you a harder target to scam. While doing this you protect others from cyber crime and phishing. Here are some signs that you are being cyber attacked through a spam email. Possible scammers may use a bogus or fake email account. Sometimes two “@’s” will be in the email and this is usually a tell tale sign. Other times the phising attack will come from a random company you have never heard of. If the name on the “To:”, line doesn't have it addressed to you specifically this is another sign. Additionally the email may enter a “time pressure”, meaning to respond in a certain time to validate a certain offer. Sometimes a company will single you out meaning somehow you are the winner of a brand new Iphone for a raffle you never entered or a free trip to Disneyland. Then the email will ask for your name and credit card information and possibly social security. Do not fall for this. Additionally, never click on any links to read a privacy policy and never call a phone number listed as safe. Some of these are typical ways scammers will gain your information. Avoid phishing at all costs or any supsected phishing, it may save you a major headache. Any number that isn’t a toll free number or a valid email this is another sign. PSA: Phishing scams as well as cyber attacks can be found in a place you feel is safe to you and you're family but it is not. Down below I have constructed four government websites that are all here to benefit us in stopping these attacks. Many attacks will happen through email but can also be through text, calls, and website links. Just this morning I received such an email through my UTSA account so they will do everything to try and make you feel safe while launching their attack. Be careful whose WIFI you connect too as well and only connect or share passwords with who you absolutely trust. Do not click on promises for easy money or cash prizes these are some of the more common attacks that are designed to steal funds from you and information. You can protect yourself by usig multi factor authentication so that nobody but you can access your accounts. UTSA has a multi authentication system called ‘Duo’, that is designed to send a text code to your phone or email. Or it will call you from a 1-800 number and you can verify through that. This is one way to protect yourself. You can update our computer and phone to have security software. There are plenty of different options on the web, obviously use one that has been used by others before with success. Also backup the data you want to save on your computer or onto a hard drive. Like we learned earlier, sometimes USB’s are not a safe option. Buy extra data space on your hardware or find another alternative that cannot be easily lost or misplaced. If you do come across a phishing attempt report it right away. For an email send the report to ‘reportphising@apwg.org’. For a text report it to ‘SPAM 7726’. You can also report it to ‘ReportFraud.ftc.gov’.