

## Popular Scams

### IRS Scam

People when they hear IRS tend to panic and the scammers are well aware of this. Callers claim to be employees of the IRS, victims are told they owe money to the IRS and the money must be paid promptly through a pre-loaded debit card or wire transfer. If the victim refuses to cooperate they are threatened with arrest. Or the victim may be told that they have a refund due them and the scammer tricks them into sharing private information. If the phone is not answered, scammers often leave an urgent call back number which is usually a number from a prepaid non traceable number. The IRS will NEVER call to demand immediate payment about taxes owed or require you to use a specific payment method for your taxes. Nor will they threaten to bring in law enforcement to have you arrested. If the IRS would need to contact you regarding your taxes, they will do so via US mail, not by telephone, and ask that you contact them. If you receive a phone call regarding the above, just hang up the phone and do not attempt to initiate a conversation.

### IRS Email Phishing Scam

The IRS will never attempt to contact you via email. The phony email may say something along the lines of, "update your IRS e-file now." This email appears to come from the IRS and includes a link to a fake website intended to mirror the official IRS website. These emails direct you to update your IRS e-file immediately. The email mentions USA gov and IRS gov. DO NOT RESPOND OR CLICK ON THE LINK. Again, the IRS will never attempt to contact you via email. Forward the scam email to the IRS at [phishing@irs.gov](mailto:phishing@irs.gov) to report it.

### Computer Virus Scam

They sound very professional; they claim to be tech support from Windows, Microsoft, Virtual PC Doctor to name a few. They will tell you that a virus has been detected in your computer. You are given directions on where to look on your computer, they will tell you that yes there is a virus. They give you directions to download a piece of software, sign up for a service that is meant to keep your computer safe. This gives the scammer remote access to your computer and your computer may have been hacked.

### Utility/Work-Order Scams

If someone professes to be from a utility company, cable company and you are not expecting anyone, do not give them access to your residence. Or if they tell you that they just moved in down the street and they just want to introduce themselves, do not let them in. Or they tell you that they are doing work at your next door neighbor's residence and need to have you come out to your back yard, do not leave your residence. Close and lock your door immediately call 911 and if the police are able to locate them, let us determine if they should be in the area. Also, anyone doing any type of soliciting must first register at the village hall and will have a permit.

If you live in an apartment complex or condo, and someone knocks on your door stating that they need to get into your residence to work on a problem and you have not received notification from your apartment manager and/or condo association regarding work to be done, do not let them in. Most apartment management and associations will advise you in advance of any work being done.

These are just a few of the more popular scams, there are numerous other scams out there, too numerous to mention. Just remember, if you did not initiate contact with anyone, and something does not seem right, hang up the phone or close and lock your door and call 911.