

Millions of people lose their money, privacy and sense of security every year due to online scams. These scams come in many forms and are often designed by career criminals making them difficult to detect. See real scam examples below and learn the signs!

The “Helpful” Computer Technician

A caller pretends to be from a reputable company that notices something wrong with your computer. They pretend to call out of concern to help you fix a problem. Their intention is to talk you into giving them access to your computer so they can take it over.

Hang up and block the caller. Run an anti-virus scan.

“If it seems too good to be true, it probably is” has never been more important to remember. Cyber criminals are clever and they will pull on your heart-strings, promise money and even befriend you.

The Stranded Traveler

Convincingly appears to be coming from a family member or a friend that desperately needs financial help due to a crisis.

Don’t respond. Call the family member or friend to verify they are not in need of help.

The Rich “Prince”

Convinces you that, in return for sending money, you will receive an even larger sum of money.

Don’t respond and block the sender.

Ransomware

A scare tactic that takes control of your device or files; designed to threaten you into paying a fine to get your access back. There is no guarantee that paying the fine or doing what the data kidnapper tells you will give access to your PC or files again.

Do not pay fines, run an anti-virus scan and contact police if you were deceived into paying fines.

SCAM SIGNS

Crisis or emergencies	
Offerings of money or prizes	Time limits or countdowns
Extremely urgent requests	Threats or accusations



VICTIM? Go through all of your online accounts whether you believe they have been compromised or not and change the passwords. Make a list of all information that you unsuspectingly gave to the criminal. Track all communications, especially if the scammer is still trying to exploit you. Obtain a copy of your credit report or confidential financial records and review them. Notify your financial institutions about the situation and they will advise you. Contact your local law enforcement.