

# TIPS TO AVOID GETTING SCAMS



#### USE CAUTION WHILE OPENING EMAIL ATTACHMENTS

Spamming emails are frequently used by cybercriminals to distribute viruses. They transmit infected attachments through emails to a large number of victims. When the virus is opened and run, it might install itself in the background and begin its activity.

### YOU SHOULD NOT BELIEVE EVERYTHING YOU SEE

Scammers are skilled at impersonating government seals, typefaces, and other characteristics. Just because a website or email appears to be official does not guarantee it is. Caller ID is frequently faked. Learn more about how to avoid impostor scams.

#### BEFORE YOU CHECK OUT, BE SURE YOUR ONLINE PURCHASE IS SAFE

Look for "HTTPS" in the URL (the additional s stands for "secure") as well as a little lock icon in the address bar.

Better better, before you buy on the website, double-check that you are on the correct page.

# WHEN INTERACTING WITH SOMEBODY YOU'VE MET ONLINE, EXERCISE EXTREME CARE.

Never give out your personal information to someone who has approached you unexpectedly, whether by phone, email, social media, or even at your front door.

## RESIST THE NEED TO RESPOND QUICKLY

Shady actors will usually try to make you believe that something is rare or only available for a limited period. They urge victims to make a choice straight away rather than thinking about it or consulting with family, friends, or financial consultants.