

# 5 Tips To Recognize & Combat Social Engineering Scams



**TurnKey Solutions**

**01**

## EXAMINE ALL LINKS & ATTACHMENTS

You may receive innocent-looking links or attachments which actually contain malware; examine carefully & don't click unless you're certain it's safe

If a message might be from an impostor, contact the real person or organization through a known, safe method, such as a public phone number

**02**

## DON'T USE THEIR CONTACT METHODS

**03**

## ESCALATE

If someone's story sounds fishy or they can't prove who they are, pass the issue - and your concerns - up the chain of command

Social engineering may try to intimidate, emotionally blackmail or threaten you. Don't let it faze you

**04**

## DON'T LET YOURSELF BE BULLIED

**05**

## DON'T SHARE INFORMATION AN ATTACKER COULD USE

If you share personal or sensitive information online, an attacker can harvest it for use in impersonation or attacks