5 Ways to Engage Your Shield Against SOCIAL ENGINEERING ATTACKS

Resist the Rush

Social engineers often create a tremendous sense of urgency, such as telling you there is a tight deadline, to trick you into making a mistake. If someone pressures you to bypass or ignore our policies, it is most likely an attack.

Recognize the 'Bag of Tricks'

Social engineers use emotions, such as fear, intimidation, curiosity, or excitement, to get you to do what they want. If something sounds suspicious or too good to be true, it probably is.

Think Before You Click

Social engineers want you to carelessly click on links and not think twice before opening attachments. Be cautious: one wrong move could infect your device and spread it to others.

Don't Just Download It or Plug It In

Social engineers count on you to download unapproved software or plug in infected USB drives or external devices. Only use authorized hardware and software. If you are not sure if something is authorized, just ask.

Ask Questions, and If It Feels Odd or Suspicious, Contact Security

If you are feel you are experiencing a social engineering attack, hang up the phone (or do not respond to the email), and contact security right away.

To contact the CWRU Information Security Office (ISO): security@case.edu

[U]Tech Service Desk
help@case.edu
216.368.HELP (4357)
help.case.edu

SANS SECURITY AWARENESS

UNIVERSITY TECHNOLOGY
CASE WESTERN RESERVE UNIVERSITY