

Social Engineering Tips

One of the greatest risks remote workers will face, especially in this time of both dramatic change and an environment of urgency, is social engineering attacks. Here are ways to better recognize and report such attack efforts.

- **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, please contact TTUHSC IT Solution Center at 806-743-1234 or itsolutions@ttuhsc.edu.
- **Ask Questions, and If It Feels Odd or Suspicious, Contact TTUHSC IT Solutions Center:** If you feel you are experiencing a social engineering attack, hang up the phone (or do not respond to the email), and contact TTUHSC IT Solutions Center right away.