Social Engineering

Some of the greatest financial and reputational damage can be caused by social engineering. It is important to protect yourself from related cyber threats, including phishing via email, text message, and phone calls.

Tips

Numerous tips can be provided to protect yourself against social engineering. Below are a few key tips:

1. If it seems too good to be true, it probably is. Trust your gut. Don't provide sensitive information or perform a financial transaction unless you have the utmost confidence in the person with whom you are transacting.

2. If you are contacted for financial transactions or to obtain other sensitive information, reach out through a different communication channel. Spoofing of phone numbers and email addresses (making it appear to come from a trusted source) is a common scam tactic. When someone contacts you, including "your bank, law enforcement, IRS," or another trusted source, always contact them by looking up their contact information on the source's website. Don't rely on the number or other information provided by the original sender.

3. Except for your trusted IT provider or friend, no one needs remote access. Don't let someone talk you into providing remote access to your computer unless you have complete trust in the person you are talking to. Scammers sometimes impersonate big company names to gain remote access to your computer, which can be used to cause significant financial and/or reputational harm to you and your family.

For more information and to learn how to identify a scam, refer to this link: How to Identify a Scam

STAR is committed to your financial security and privacy. For more tips and information, please visit STAR's security page. STAR also has a dedicated Fraud team ready to assist with any fraud-related matter.