Social Engineering

LEVEL UP YOUR DATA DEFENSE

98% OF CYBER ATTACKS ARE CAUSED BY SOCIAL ENGINEERING

IT TAKES AN AVERAGE OF 277 DAYS FOR A SECURITY TEAM TO IDENTIFY AND CONTAIN A BREACH

KNOW YOUR ENEMY - THE TYPES OF SOCIAL ENGINEERING

EXECUTIVE FRAUD - Attacker pretends to be an executive to cause a sense of urgency and familiarity.

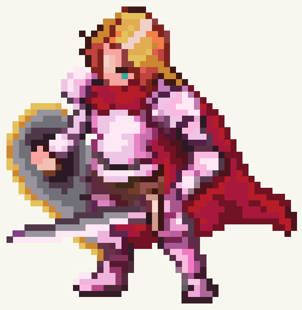
TAILGATING - Attacker tricks an employee with access to enter a restricted area.

PHISHING - Attacker sends malicious emails designed to trick users to give up sensitive information.

PRETEXTING - Attacker uses a fabricated story to gain a victims trust to gain sensitive information.

DUMPSTER DIVING - Attacker searches through the trash for useful information to do cyber crime.

BE HEROIC - TAKE STEPS TO PROTECT CNP DATA



- **Know what data being released** - Know your data classification level and protect your data.
- **Use Multifactor Authentication** - Take advantage of MFA tools at work and at home.
- **Secure physical device** - Always lock your mobile devices and keep them in your procession.
- **Know CNP policies** - All CNP polices are found on CNP Today! (Utilize key word search).

Cyber Security Operations Center (CSOC)
xxx-xx-xxxx (redacted for submission)
redacted@centerpointenergy.com

START GAME

Help Desk
xxx-xxx-HELP (redacted)
1-xxx-xxx-Help (redacted)

Cyber Security Awareness
redacted_for_submission@centerpointenergy.com