Social Engineering

The easiest way to breach security is to obtain credentials, and the easiest way to get that information is to ask for it. The technique of tricking an individual into revealing secure information is known as social engineering, the basic goal of which is to gain unauthorized access to systems or information. Social engineering is used to commit fraud, network intrusion, industrial espionage, identity theft or simply to disrupt and compromise computer systems.

Social engineering is often successful because most targets instinctively want to trust people, and provide as much help as possible. Victims of social engineering are usually unaware they have been conned.

Common Techniques

- Social engineering by phone – pretexting
- Online social engineering
  - Phishing (email)
  - Vishing (voice phishing – automated phone calls)
  - SMiShing (text messages on cell phones)
  - Pharming (redirect website traffic to a bogus site)
- Persuasion
- Reverse social engineering
- Dumpster diving
- Shoulder surfing (looking over a shoulder to see information)
- And many more...

Tips to Avoid Social Engineering

- Never share your username or password with anyone
- Always be aware of your surroundings
- Reputable companies will never ask you for your username or password.

If you have any questions, please contact your nearest Busey branch, or report suspicious activity to Busey immediately at 1.800.67 | Busey (1.800.672.8739), option 2.