First County Bank
It's where you belong.

CustomerFirst
CONTACT CENTER
Weekdays 203.462.4400
Touch Tone 203.462.4300

Social Engineering Awareness

How Social Engineering Works

Social engineering is essentially the art of gaining access to buildings, systems or data by exploiting human nature. Social Engineers prey on our human tendency to trust others, our desire to be helpful, and our respect for authority. Rather than by breaking in or using technical computer hacking techniques to obtain information, criminals take advantage of human nature to deceive their victims into voluntarily providing sensitive information that can be used to commit fraud.

Common Social Engineering Techniques

Many times Social Engineers will use small pieces of illicitly obtained information to gain trust or access so that they can fully carry out their cons. Some of the common techniques of a social engineer include:

- ***Pretexting***: Fraudsters create a detailed storyline to manipulate their targets into providing sensitive information. The pretext may involve false emails, websites, names, identities, and even clothing. The criminal may use a sob story, intimidation, flattery, and/or charm.
- ***Impersonation:*** Fraudsters pose as an employee or authority figure in order to obtain information.
- ***Phishing:*** Information such as login credentials and account numbers is collected by fraudsters by sending emails or text messages that appear to be legitimate.
- ***Dumpster Diving:*** Sensitive information is collected by going through the trash looking for documents and/or portable storage devices (for example: a flash drive) containing sensitive information.

How to Avoid Being the Victim of Social Engineering

Your best defense against social engineering is to be aware of the threat and embrace a healthy skepticism.

- Slow down. If you are pressured to provide information by a sense of urgency, or high-pressure sales tactics be skeptical; never let their urgency influence your careful review.
- Never give out confidential (or seemingly non confidential) information over the phone or in person unless you can first verify the person asking and the need. First County Bank will ***never*** ask for your password or other confidential information over the phone or in person.
- Be suspicious of unsolicited offers of and requests for help. Legitimate companies do not contact you to provide help. Seek out charitable organizations on your own to avoid charity scams.
- Never respond to unsolicited email messages and never click on a URL or attachment in an email unless you can verify the source. Type out the URL in the browser bar instead.
- Avoid tossing sensitive information directly in the trash. Use your shredder and dispose of paper and digital data properly.

If you have any questions, please feel free to call the
CustomerFirst Contact Center at (203) 462-4400 *(Monday - Friday from 8:30 a.m. to 4:30 p.m.)*