

## Social Engineering

Technology is deeply embedded in our daily lives, making it an attractive target for fraudsters. One common tactic fraudsters employ is social engineering, which is a method used to manipulate individuals into divulging confidential information or performing actions that benefit the attacker. Fraudsters often exploit current events such as natural disasters, political elections, and holidays to carry out their schemes.

Staying informed of social engineering tactics and recognizing red flags can help protect you and USF from these scams:

### **Phishing, Vishing, and SMSHING**

Fraudsters pretending to be from a trusted source use a fake email, call, or text message to ask for sensitive information or install malware.

### **Pharming**

Fraudsters redirect individuals to a fraudulent website that mimics an official one, with the goal of stealing sensitive information. USF Office of Internal Audit web site:

### **How can I report general USF fraud or abuse?**

Notify your supervisor

 \_\_\_\_\_

 \_\_\_\_\_

 \_\_\_\_\_

 \_\_\_\_\_

 \_\_\_\_\_