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.

Vendor Impersonation Fraud

- Fraudsters pose as a vendor to deceive organizations by sending fake invoices or directing future payments to a fraudulent bank account.

Pharming

- Fraudsters redirect individuals to a fraudulent website that mimics an official one, with the goal of stealing sensitive information.

Charity Fraud

- Fraudsters impersonate a legitimate charity or create a fake charity to deceive individuals into donating money to them.

Red Flags of Social Engineering

- A sense of urgency or pressure
- Unsolicited information requests
- Unusual or generic greetings
- Grammatical errors
- Requests to install software
- Suspicious links or attachments
- Unexpected payment requests
- “Too good to be true” offers

Where can I find more information?

- USF Regulation 5.001: Fraud Prevention and Financial Detection
- USF Office of Internal Audit website: https://www.usf.edu/audit/

How can I report general USF fraud or abuse?

- Notify your supervisor
- Contact the USF Office of Internal Audit at (813) 974-2705
- Report general USF fraud & abuse through the EthicsPoint hotline at (866) 974-8411