Social Engineering

In a **social engineering attack**, an attacker uses human interaction to manipulate a person into providing them information. People have a natural tendency to trust. Social engineering attacks attempt to exploit this tendency in order to steal your information. Once the information has been stolen it can be used to commit **fraud** or **identity theft**.

Criminals use a variety of social engineering attacks to attempt to steal information, including:

- **Website spoofing**
- **Phishing**

This brochure explains the meaning of these common attacks and provides tips you can use to avoid being a victim.

To learn more about information security, visit any of the following websites:

- OnGuardOnline.gov
- StaySafeOnline.org
- BBB.org/Data-Security
- US-CERT.gov

First Century Bank, National Association
http://www.myfirstcenturybank.com
Toll Free: (866) 343-9497

FIRST CENTURY BANK, N.A.

Avoiding Social Engineering Attacks

Common Attacks

❖ **Website spoofing** is the act of creating a fake website to mislead individuals into sharing sensitive information. Spoof websites are typically made to look exactly like a legitimate website published by a trusted organization.

Prevention Tips:

- Pay attention to the web address (URL) of websites. A website may look legitimate, but the URL may have a variation in spelling or use a different domain.
- If you are suspicious of a website, close it and contact the company directly.
- Do not click links on social networking sites, pop-up windows, or non-trusted websites. Links can take you to a different website than their labels indicate. Typing an address in your browser is a safer alternative. Only give sensitive information to websites using a secure connection. Verify the web address begins with "https://" (the "s" is for secure) rather than just "http://".
- Avoid using websites when your browser displays certificate errors or warnings.

❖ **Phishing** is when an attacker attempts to acquire information by masquerading as a trustworthy entity in an electronic communication. Phishing messages often direct the recipient to a spoof website. Phishing attacks are typically carried out through email, instant messaging, telephone calls, and text messages (SMS).

Prevention Tips:

- Delete email and text messages that ask you to confirm or provide sensitive information. Legitimate companies don't ask for sensitive information through email or text messages.
- Beware of visiting website addresses sent to you in an unsolicited message.
- Even if you feel the message is legitimate, type web addresses into your browser or use bookmarks instead of clicking links contained in messages.
- Try to independently verify any details given in the message directly with the company.
- Utilize anti-phishing features available in your email client and/or web browser.
- Utilize an email SPAM filtering solution to help prevent phishing emails from being delivered.
- Do not open attachments received from unknown senders or unexpected attachments from known senders.
- Be cautious of the amount of personal information you make publicly available through social networking sites and other methods. The more information publicly available about you, the easier it is for attackers to craft more convincing phishing messages.

Report Fraudulent or Suspicious Activity

Contact us immediately if you suspect you have fallen victim to a social engineering attack and have disclosed information concerning your First Century Bank, N.A. accounts.

Call us at (866) 343-9497 or visit your local First Century Bank, N.A. branch location.

Regularly monitoring your account activity is a good way to detect fraudulent activity. If you notice unauthorized transactions under your account, notify First Century Bank, N.A. immediately.