Social Engineering -

A collection of techniques used to manipulate people into performing actions or divulging confidential information.

- **Pretext Calling:** A perpetrator uses an invented scenario to target victims such as pretending to be computer support and asking for passwords or other confidential account information.
- **Phishing:** A form of criminal activity where individuals pose as legitimate entities to try to obtain or "fish" personal information. Typically come as official looking emails, instant message, text message or fax that appear to be from legitimate businesses requesting verification of confidential information so you can "update" or "verify" credit card numbers, bank account information, Social Security numbers, passwords and any other sensitive information. They like to target account holders to try and establish what financial institution you use and send an official looking email from your bank to gain that confidential information.
- **Pharming:** Pharming is a criminal activity where a website's information is acquired and traffic on that website is directed to another location to obtain personal information. The individual trying to obtain information illegally will set up a fraudulent website to look like a real website in almost every detail. They then use "phishing" tactics to entice people to the website to divulge confidential information such as pin numbers, account numbers and passwords. When looking at the Bank website, be and sure notice the secure "https://" and secure "padlock" or "lock" icon in the web browser status bar. A fraudulent website will not have these details. Banks invest extra in these areas to help keep the site and customer accounts secure.
- **Skimming:** when you pay with credit or debit card know where your card is going. The person taking the payment may run it through a skimming device and copy the information on it.
- **Old fashioned stealing:** stealing cards and account information to create ways to copy cards and commit fraud! Breaking into homes, cars, buildings; not securing items on your desk

Please Note: Spring Hill State Bank will *NEVER* send an unsolicited email or text message requesting you to verify your personal information.

HOW CAN I PROTECT MYSELF?

1. Don't reply to emails from people or companies you don't recognize. Misspelled URL's are common deceptions as well as the @ symbol in web addresses.
2. Contact the company cited in the email requesting your information by using a web address you know to be genuine.
3. Do not click on links in websites unless you trust who they are from. Typing in the web address for the company in a separate browser is the safest.
4. Avoid emailing personal and financial information. If you must, make sure you see the "lock" icon on your web browser's status bar before submitting any personal data. This "lock" icon signals that your information is secure during transmission.
5. Be sure your virus protection software is current. The extra expense of virus protection is important to protect your computer from would be hackers.
6. Perform updates to your system as required.