CONSUMER ALERT

A new type of FRAUD has found its way to our area and it's designed to steal your money or your identity. It's known as "phishing" and the big catch is your personal information.

Customers of local banks have already been targeted by automated phone systems asking for debit card numbers and live callers asking customers to "verify" the information on a check. The threat also often extends to unsolicited email asking you to verify your Social Security number or online banking credentials.

HOW CAN YOU PROTECT YOURSELF ?
BE SUSPICIOUS OF ANY REQUEST FOR INFORMATION AND IF YOU FEEL UNCOMFORTABLE, DON'T CLICK THE EMAIL LINK OR PROVIDE ANY INFO OVER THE PHONE. SIMPLY HANG UP AND CALL ANY OF OUR FIRST SOUTHERN BANK BRANCH OFFICES.

REMEMBER THAT FIRST SOUTHERN BANK WILL NEVER:
- **Email you asking for information to "verify" or "correct" anything**
- **Try to pressure, intimidate, or scare you into giving out your info**
- **Be able to PREVENT this type of fraud because the thieves will always target you, THE CUSTOMER, without the bank's knowledge**
- **Ask you for information that we should already have unless we are trying to resolve a problem or issue that YOU CALLED US ABOUT**

REMEMBER THAT THIEVES WILL OFTEN:
- **Initiate the communication**
- **Ask for information that the bank already has**
- **Try to scare or intimidate you with an "urgent" message**
- **Target your home computer, mail, telephone number, or email**
- **Pretend to be from the government (IRS, Federal Reserve, etc)**
- **Have some piece of "PUBLIC" information (Bank's routing number, etc.)**
- **Be EXTREMELY convincing**
- **Say that fraud has already occurred and they're trying to help you**
- **Offer to pay you for help in collecting money from a foreign country**

FIRST SOUTHERN BANK

Member FDIC

EQUAL HOUSING LENDER