What is An Online Phishing Scam?

The term "phishing" is a term derived from "fishing." It refers to the process used by criminals to steal your confidential information. It is a type of deception designed to acquire your valuable personal data, such as credit card numbers, passwords, account data, social security numbers or other information. Con artists might send millions of fraudulent e-mails messages that appear to come from Web sites you trust, like your bank or credit card company. These fraudulent emails request that you provide personal information to a website that looks legitimate but is actually not the true website of your bank.

Where these fraudulent e-mail messages may claim to be from Southern Heritage Bank, always check the Web site's address. These messages usually take an urgent tone asking you to "update" or "validate" your ATM, debit card, credit card, or other personal account information immediately or face consequences. They often include official-looking logos from real organizations and other identifying information taken directly from legitimate Web Sites.

You can avoid being taken in by these scams by keeping in mind these important points:

- Southern Heritage Bank **DOES NOT** send urgent, time sensitive or contest e-mails, or ones that ask you to provide, update, or confirm sensitive data. We already have this information on file and would not request it from you.
- We **DO NOT** send e-mails that ask you to provide personal information using a link or input fields in the e-mail *except* in response to an inquiry **YOU** initiated.

If you suspect that you have responded to a phishing scam with personal or financial information or that you have entered this information into a fake Web site, take these steps to minimize any damage.

- Report the incident to Southern Heritage Bank and/or your credit card company. Contact the organization directly that you believe was the front for the scam along with the Federal Trade Commission. FTC: National Resource for Identity Theft at www.consumer.gov/idtheft;
- Change the passwords on all your online accounts;
- Set up a schedule to routinely review your Southern Heritage Bank statements and those from your credit card companies;
- Use the latest products and services to help warn and protect you from online scam, by installing phishing filters or up-to-date antivirus and spyware software.

Southern Heritage Bank in an effort to educate the consumer on steps to take for protecting themselves would like to direct you to a brochure available in a downloadable form through the FDIC's Web site at www.fdic.gov/news/news/press/2004/pr9304b.pdf . Remember Southern Heritage Bank's website is www.shbnet.com .