MeridianBank

PHISHING SCAM.
DON'T TAKE THE BAIT!

WHAT IS PHISHING?

Phishing is one of the latest cons used by high-tech criminals to facilitate one of America's leading forms of fraud—identity theft. Basically, the scam uses spam (unsolicited e-mail) to bait consumers into disclosing sensitive personal information—such as social security numbers, account and routing numbers, credit card numbers, personal identification numbers, passwords, and other private data.

According to the Federal Trade Commission (FTC), the unsolicited e-mails give the appearance of being from legitimate businesses. In fact, fraudsters usually pick a business that the potential victim actually does business with, such as a financial institution, credit card company, or insurance company. The fraudsters tell the e-mail recipients they need to "update" or "validate" their billing information to keep their accounts active. To help set the hook, they even direct their potential victims to a web site that imitates the look of the legitimate web site—with logos, colors, and designs to match. Unwittingly, consumers then submit their information to the impostor, who then uses the personal data to commit identity theft.

TO AVOID GETTING REELED INTO ONE OF THESE SCAMS, THE FTC OFFERS THE FOLLOWING GUIDANCE:

• If you get an e-mail that warns you—with little or no notice—that an account of yours will be shut down or interest suspended unless you reconfirm your billing information, do not reply or click on the link in the e-mail. Instead, contact the legitimate company cited in the e-mail using a telephone number or web address you know to be genuine.

• Avoid e-mailing personal and/or financial information.

• Look for the "lock" icon on the browser's status bar before submitting financial information through any web site. It signals that your information is secure during transmission.

• Review credit card and account statements as soon as you receive them to determine whether there are unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or financial institution to confirm your billing address and account balances.

• Report suspicious activity to the FTC— send the actual spam e-mail to **uce@ftc.gov**. If you believe you've been scammed, file your complaint at **www.ftc.gov**, then visit the FTC's identity theft web site at **www.ftc.gov/idtheft** to learn how to minimize your risk of damage from identity theft. To help fight fraud, the FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel® — a secure, on-line database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

• Visit **www.ftc.gov/spam** for other ways to prevent and avoid e-mail scams and to learn how to deal with deceptive spam.

As your financial institution, we want to help you combat identity theft. One of the best ways to fight fraud is to educate yourself and be aware of a possible scam before it happens to you. Be cautious when providing information, and learn the steps you can take to help protect your sensitive, personal information in an attempt to stay ahead of these criminals.

To file a complaint or get fee information on consumer issues, visit ***www.ftc.gov*** *or call toll free to* 1-877-FTC-HELP (1-877-382-4357) or TTY: 1-866-653-4261.