BOUNDARY WATERS BANK

Your Financial Outfitter

CONSUMER ALERT: DON'T LET INTERNET PIRATES STEAL YOUR PERSONAL FINANCIAL INFORMATION. YOU have the POWER to stop them. An Identity Theft scam called "Phishing" (pronounced "fishing") is significantly on the rise.

In a typical case, you might receive an e-mail that appears to come from a reputable company such as your financial institution. The e-mail would warn you of a serious problem that requires your immediate attention, It may use phrases, such as “Immediate attention required,” or “Please contact us immediately about your account: The e-mail will then encourage you to click on a button to go to the institution’s Web site. In a phishing scam you could be re-directed to a site that may ask you to update your account information or to provide information for verification purposes.

How to Protect Yourself:

1. **Never provide your personal information in response to an unsolicited request.** Whether it is over the phone or over the Internet, E-mails and Internet Pages created by phishers may look exactly like the real thing. They may even have a fake padlock icon that ordinarily is used to denote a secure site. If you did not initiate the communication, you ***should not*** provide any information.

2. **If you believe the contact may be legitimate, contact the financial institution yourself.** You can find phone numbers and Web sites on the monthly statements that you receive from your financial institution, or you can look the company up in a phone book or on the Internet. The key is that ***you*** should be the one to initiate the contact, using contact information that you have verified.

3. **Never provide your password over the phone or in response to an unsolicited Internet request.** A financial institution would never ask you to verify your account information online. Thieves armed with this information and your account number can help themselves to your savings.

Review account statements regularly to ensure all charges are correct. If your account statement is late in arriving, call your financial institution to find out why. If your financial institution offers electronic accounts access, periodically review activity online to catch suspicious activity.

If you fall victim to an attack, act immediately to protect yourself. Alert your financial institution. Place fraud alerts on your credit files.

* Report all suspicious contacts to the Federal Trade Commission through the Internet at Consumer Information or by calling 1-877-IDTHEFT.