FS First State Bank

Online Security Tips

Beware of Phishing Attempts and Internet Scams

Phishing (fishing) is a social engineering technique often used by criminals to trick individuals into providing personal information such as: ATM card numbers, account numbers, Social Security numbers, access Ids and passcodes.

Phishing maybe performed over the telephone through SMS texting or through email and redirection to a fraudulent website that appears to look just like the legitimate site.

Some of these fraudulent websites and even compromised legitimate sites may be virus laden and can be used to download malicious software (also known as mal-ware or crimeware) to your computer. Below we have listed a few tips to help protect your personal information on the Internet:

- Always be wary of any email requesting your personal information: such as your account number, ATM card number, PIN number, or social security number.
- Do not click on links or download attachments in email unless you are expecting the email.
- Bookmark financial websites and use these bookmarks every time you visit the website.
- Whenever you enter personal information on a website always look for the lock symbol, or https: in the address bar. Always click on the lock symbol and review the certificate details.
- Keep your Internet browser and computer operating systems updated! Most browsers also now offer free anti-phishing tool bars that can help alert you of fraudulent websites.
- Always use anti-virus and anti-spam software and keep it updated.
- Change passwords to your online accounts regularly.
- If you frequently surf the Internet, consider using a dedicated computer strictly for online banking.
- If you send us an email, please do not include any confidential, personal or sensitive information in the email message, as email messages are not secure. We do offer secure messaging through our Online Banking service and you may use this secure messaging feature if you need to send us sensiztive or confidential information.
- If you receive an e-mail that you think could be a scam, social engineering or a phishing attempt, delete it immediately or forward the email to spam@uce.gov.
- If you have any questions about the legitimacy of an email, especially an email from this Institution, you can your local branch at the number below:

Buxton	Grand Forks	Mayville	Portland	Thompson
423 Broadway	2500 32nd Ave. S.	124 Center Ave. S.	509 Parke Ave.	612 Broadway
701.847.2600	**701.746.7766**	**701.788.9030**	**701.788.3791**	**701.599.2600**

EQUAL HOUSING LENDER Member FDIC

firststatebanks.com