Security Statement

The Bank of Dixon County is committed to protecting your privacy and security. We will never initiate a request for sensitive information, such as Social Security numbers, account numbers, or PINs from you via email. We strongly suggest that you do not share your personal ID, PIN, or account numbers with anyone. Below are some of the safeguards we have in place to protect against security breaches in the online environment:

Call the Bank of Dixon County at (402) 755-2224 or email them at pam@bankofdc.com with any questions or concerns.

Fraudulent Emails
Beware of emails that contain the following:

- Request that you click a link to a spoof website – one that looks like a real company website, including the real company's graphics and design. Since fraudulent emails may even use exact wording from the real company's website. It's difficult to determine a spoof website. If you have any doubts, please contact us at (402) 755-2224.
- Ask to give, confirm, or update sensitive personal information, such as Social Security Numbers, usernames, passwords, PIN numbers, or account numbers
- Use Pop-Up windows for entering or confirming personal data (see below for more on pop-up screens on secured websites).
- Have a sense of urgency to give the information immediately, citing a specific thing that might happen. For example, your account may be closed or temporarily suspended.
- Have spelling errors and/or bad grammar. Intentional spelling errors may allow the email to get through spam filters used by Internet Service Providers (ISPs).

Even if you don't enter your personal data, by clicking on a link embedded in a fraudulent email, you may inadvertently download tracking software or viruses that track your keystrokes to gain your personal information.

Some people "test" for online fraud by entering incorrect information. If the information is accepted, then they feel they can determine that it's an email fraud. Criminals are now aware that people perform this test, and may not accept the information entered first. The best defense is not to enter any personal information at a website you link to from an unsolicited email.

Online Banking User ID and Password
Our system is designed to limit online account access to those possessing the User ID and Password associated with your account(s). Unsuccessful logins are limited to three tries to further deter unauthorized access.

Encryption
We have encryption technology in place that allows for the protection of data in transit between your computer and ours. A secure website address will begin with the https://(the s signifies secure). The closed lock icon will usually indicate whether a communication session is encrypted also.

Firewalls
Our computer systems include firewalls that are monitored and designed to protect against unauthorized access to our systems.

Timeout
Our online banking system is designed to log you off after 20 minutes of inactivity.

Log Off
When you are done online, click the log off button. We suggest you do this before you shut your computer off and before you surf to other websites.

Security for your Computer:
- Keep your operating system and browser up to date
- Install a personal firewall
- Install anti-virus software and keep it up to date
- Scan your computer for spyware on a regular basis
- Don't download programs or files from unknown sources
- Install a pop-up blocker from a trustworthy source
- Disconnect from the internet when you are not online

Safeguarding your Information (from the American Bankers Association):
- Don't give your Social Security number or other personal credit information about yourself to anyone that calls you.
- Tear up or shred receipts, bank statements, and unused credit card offers before throwing them away.
- Keep an eye out for missing mail.
- Don't mail bills from your own mailbox with the flag up.
- Review your accounts regularly for unauthorized charges.
- Order copies of your credit reports once a year to ensure accuracy.
- Do business with companies you know are reputable, particularly online.
- Don't open email from unknown sources and use virus detection software.
- Protect your PINs (don't carry them in your wallet) and passwords; use a combination of letters and numbers for your passwords and change them periodically.
- Report any suspected fraud to your bank and the fraud units of the three credit reporting agencies immediately.
    - TransUnion – (800) 916-8800
    - Experian – (800) 301-7195
    - Equifax – (800) 525-6285

If you become a Victim - contact the following:
- The fraud department of the three major credit bureaus (see listed above)
- The creditors of any accounts that have been misused
- The local police to file a report
- The bank to cancel accounts held in your name and reopen new accounts with new passwords