FNBC BANK&TRUST

Commercial Banking Customers

Safeguarding Your Information

Tips on a secure online banking experience

At **FNBC Bank & Trust,** the security of customer information is a priority. We are strongly committed to the safety and confidentiality of your records. Every day, unscrupulous individuals are busy developing new scams targeting the unsuspecting public. One of the best ways to avoid fraud is to become an educated user.

Small to Medium sized business and government banking accounts are being targeted by criminals every day.

Every security system in place today can and has been compromised by criminals. No system that the bank has put in place can catch 100% of fraudulent attempts.

***** Commercial Accounts and Government Accounts are not covered under Regulation E. *****
In most circumstances you will be responsible for assuming the loss on fraudulent transactions. It is vital that you following best practices:

What we expect of you:

- Establish a separate account for the origination of each type of transaction. ACH origination / Wire Transfer etc.
    - Ideally only fund those accounts with enough funds to cover the planned transactions on a daily basis.
- Establish dual control over the setup and creation of new user accounts on the system.
- Establish dual control over the setup of new payees on the system.
- Run summary reports of all transactions to ensure they are accurate.
- Review your transactions the next business day to determine if fraudulent activity has occurred.
- Maintain up to date anti-virus on your computer systems at all time that access financial websites.
- Patch your operating system weekly and ensure that you are updating Java and Adobe applications weekly as well. Vulnerabilities in these applications are utilized by criminals constantly.
- Ideally, dedicate a single PC for online financial transactions and prohibit any other form of web surfing and email access on this PC.
    - Have the firewall specifically restrict access for the workstation to only the IP Addresses of the financial institutions systems. This will prevent individuals from surfing the internet on the PC.
- Utilize a unique complex password (Upper Case, Lower Case, Special Characters) at least 8 characters long.
    - DO NOT RE-USE PASSWORDS THAT YOU HAVE REGISTERED FOR AT OTHER WEBSITES!
        1. Websites can be compromised and your password will be exposed.
    - Change your password every 30 days.
    - Do not utilize words in your password such as Password1.
- Never provide your account number or username / password in any written communication to the bank. This is especially true of email.
- Watch out for copycat Web sites that deliberately use a name or Web address very similar to, but not the same as the real one. The intent is to lure you into clicking through to their Web site and giving out your personal information, such as a bank account number, credit card number or Online Banking login information.
- Always use your pre-established link to access web sites. Never click on a link contained in an email.
- Utilize Security and Balance Alerts to be notified via phone, e-mail and or SMS text messages when activity occurs on the account.

What the Bank does:

- On at least an annual basis the bank examines its controls that it has implemented for online banking access.
- Based on that review that bank will determine if changes are necessary and will implement required changes on an ongoing basis.

FNBC BANK&TRUST

- Reviews the current fraud trends at least quarterly to determine if changes are required in regards to current security controls and provide alerts to our customer base.
- Monitor ACH transactions for suspicious activity on your account.
- Monitor Wire transactions for suspicious activity on your account through a rules based online system.
- We utilize multi-factor authentication that is in guidance of federal guidelines for online banking.
- We may on occasion call to verify other information regarding your online activity should we see something of concern in your login patterns.

What the Bank does not do:

- We will never ask you for your online banking password.
- We will not contact you via email requesting you click on a link inside the email.
- All electronic communication is done through the secure email system provided within the online banking system.
- We will never send your non-public information via email unless it utilizes our secure email system.

While these layered process are designed to prevent fraud. They will not catch fraud 100% of the time. You are responsible for losses incurred on commercial and government accounts. Be vigilant and monitor your account at all times.

In case of errors or questions about your electronic transfers, call or write us at the telephone number or address listed, as soon as you can.

If at any time you have questions regarding security or possible fraud, please contact our customer service representatives at your local branch office.