

## **To our Business Internet Banking Customers,**

We are constantly striving to make our online banking product as secure as possible, but internet safety requires your involvement also. Therefore, we are providing the following information to help you keep your account information and your money safe from internet fraud. If you have any questions about this matter please call Candace Lauby at 920.206.9480.

## **PREVENTION**

### **1. Educate everyone on this type of fraud scheme**

Don't respond to or open attachments or click on links in unsolicited e-mails.

If a message appears to be from your financial institution and requests account information, do not use any of the links provided. Contact the financial institution using the information provided upon account opening to determine if any action is needed. Financial institutions do not send customers e-mails asking for passwords, credit card numbers, or other sensitive information. Similarly, if you receive an email from an apparent legitimate source (such as the IRS, Better Business Bureau, Federal courts, UPS, etc.) contact the sender directly through other means to verify the authenticity. Be very wary of unsolicited or undesired email messages (also known as "spam") and the links contained in them.

Be wary of pop-up messages claiming your machine is infected and offering software to scan and fix the problem, as it could actually be malicious software that allows the fraudster to remotely access and control your computer.

Teach and require best practices for IT security.

### **2. Enhance the security of your computer and networks to protect against this fraud**

Minimize the number of, and restrict the functions for, computer workstations and laptops that are used for online banking and payments. A workstation used for online banking should not be used for general web browsing, e-mailing, and social networking. Conduct online banking and payments activity from at least one dedicated computer that is not used for other online activity.

Do not leave computers with administrative privileges and/or computers with monetary functions unattended. Log/turn off and lock up computers when not in use.

### **3. Use/install and maintain spam filters**

- Install and maintain real-time anti-virus and anti-spyware desktop firewall and malware detection and removal software. Use these tools regularly to scan your computer. Allow for automatic updates and scheduled scans.
- Install routers and firewalls to prevent unauthorized access to your computer or network.
- Change the default passwords on all network devices
- Install security updates to operating systems and all applications, as they become available. These updates may appear as weekly, monthly, or even daily for zero-day attacks.
- Block pop-ups.
- As recommended by Microsoft for users more concerned about security, many variants of malware can be defeated by using simple configuration settings like enabling Microsoft Windows XP7, Vista, and Data Execution Prevention (DEP) and disabling auto run commands. You may also consider disabling JavaScript in Adobe Reader. If these settings do not interfere with your normal business functions, it is recommended that these and other product settings be

considered to protect against current and new malware for which security patches may not be available.

- Keep operating systems, browsers, and all other software and hardware up-to-date.
- Make regular backup copies of system files and work files.
- Encrypt sensitive folders with the operating system's native encryption capabilities. Preferably, use a whole disk encryption solution.
- Do not use public Internet access points (e.g., Internet cafes, public wi-fi hotspots (airports), etc.) to access accounts or personal information. If using such an access point, employ a Virtual Private Network (VPN)
- Keep abreast of the continuous cyber threats that occur.

#### 4. **Enhance the security of your corporate banking processes and protocols**

- 1 Initiate ACH and wire transfer payments under dual control using two separate computers. For example: one person authorizes the creation of the payment file and a second person authorizes the release of the file from a different computer system. This helps ensure that one person does not have the access authority to perform both functions, add additional authority, or create a new user ID. If, when logging into your account, you encounter a message that the system is unavailable, contact your financial institution immediately.

#### 5. **Monitor and reconcile accounts at least once a day**

Reviewing accounts regularly enhances the ability to quickly detect unauthorized activity and allows the business and the financial institution to take action to prevent or minimize losses. ***For all ACH transactions done on a Business Account you only have a 24 hour (1 day) return (reject) time.***

#### 6. **Note any changes in the performance of your computer such as:**

- A dramatic loss of speed.
- Changes in the way things appear.
- Computer locks up so the user is unable to perform any functions.
- Unexpected rebooting or restarting of your computer.
- An unexpected request for a one time password (or token) in the middle of an online session.
- Unusual pop-up messages.
- New or unexpected toolbars and/or icons.
- Inability to shut down or restart.

#### 7. **Pay attention to warnings**

Your anti-virus software should alert you to potential viruses. If you receive a warning message, contact your IT professional immediately.

#### 8. **Be on the alert for rogue emails**

If someone says they received an email from you that you did not send, you probably have malware on your computer. You can also check your email "outbox" to look for email that you did not send.

## **RESPONSE**

- 1. If you detect suspicious activity, immediately cease all online activity and remove any computer systems that may be compromised from the network**  
Disconnect the Ethernet cable and/or any other network connections (including wireless connections) to isolate the system from the network and prevent any unauthorized access.
- 2. Have a plan**  
Your employees need to know who should be notified when they suspect a problem, and that go-to person needs to know what steps to follow.
- 3. Immediately contact Bank of Lake Mills so that the following actions may be taken:**
  - Disable online access to accounts.
  - Change online banking passwords.
  - Open new account(s) as appropriate.
  - We will review all recent transactions and electronic authorizations on the account. If suspicious active transactions are identified, we will attempt to cancel them immediately.
  - Ensure that no one has added any new payees, requested an address or phone number change, created any new user accounts, changed access to any existing user accounts, changed existing ACH template profiles, changed PIN numbers or ordered new cards, checks or other account documents be sent to another address.
  - Contact the appropriate law enforcement agencies.
- 4. Maintain a written chronology of what happened, what was lost, and the steps taken to report the incident to the various agencies, financial institutions, and firms impacted**  
Be sure to record the date, time, and contact telephone number, person spoken to, instructions, and any relevant report or reference number.
- 5. Have a contingency plan to recover systems suspected of compromise**  
Your contingency plan should cover resolutions for a system infected by malware, data corruption, and catastrophic system/hardware failure. A recommended malware removal option is to reformat the hard drive, then reinstall the operating system and other software on the infected computer(s). There is no preservation of data using this method – all your data will be permanently erased. Do not take this step until you determine if a forensic analysis of the computer is needed. For additional recommendations on steps to take following a compromise, see the section “What if I am Compromised” on page 6 of the US CERT document, *Malware Threats and Mitigation Strategies* available at [http://www.us-cert.gov/reading\\_room/malware-threats-mitigation.pdf](http://www.us-cert.gov/reading_room/malware-threats-mitigation.pdf)
- 6. Consider whether other company or personal data may have been compromised**