First Bank of Berne
Depend On Us

CONSUMER AWARENESS INFORMATION GUIDE

First Bank of Berne Consumer Awareness Tips

First Bank of Berne will never ask for sensitive information such as account numbers, debit/credit card numbers, or passwords via email or phone. Please review the following tips for safeguarding your information.

- Do not give out your Social Security number or other personal information if requested to do so via email, phone, or mail unless you have initiated the contact.
- Do not open emails from unknown sources.
- Install and frequently update virus detection software.
- Conduct business with companies that you know and trust, especially when doing business online.
- Enhance password security by using a combination of letters, numbers, and special characters.
- Regularly review account statements for any unauthorized charges.
- Properly dispose of documents containing sensitive information (i.e. shredding of documents).
- Send documents containing sensitive information in a secure manner (i.e. do not place in a mailbox with the flag up).
- Review options for ordering a copy of your credit report. A review of the credit reporting agencies and options available can be found at ***www.annualcreditreport.com***.
- Contact First Bank of Berne and other financial partners immediately if you have reason to suspect fraud on your account(s) and/or misuse of your personal information.

First Bank of Berne Identity Theft Tips

Identity theft occurs when someone obtains personal information and uses that information to commit fraud or theft. Please review the following tips to assist in minimizing the chances of becoming a victim of identity theft.

- Do not give out your Social Security number or other personal information if requested to do so via email, phone, or mail unless you have initiated the contact.
- Minimize the amount of documents you keep with you that contain personal information.
- Properly dispose of documents containing sensitive information (i.e. shredding of documents).
- Secure personal information in your home making it available to only those that need to see it.
- Promptly remove mail from your mailbox.
- Prior to providing personal information for business purposes, inquire as to how the information will be used and secured, and whether it will be shared with others.
- Safeguard your debit and credit cards knowing where they are at all times; if you happen to lose one, report it as soon as possible.

CONSUMER AWARENESS INFORMATION GUIDE

- Choose a personal identification number (PIN) for your ATM and debit card that is different from your address, telephone number, Social Security number, or birth date.
- Keep and compare your receipts for all types of Electronic Funds Transfer (EFT) transactions with your periodic statement.
- Make sure you know and trust a merchant before sharing any bank account information.

If you become a victim of identity theft:

1. Order a copy of your credit report. A review of the credit reporting agencies and options available can be found at ***www.annualcreditreport.com***. Place a fraud notice with the credit reporting agencies.
2. Contact the creditors of any accounts that have been misused.
3. Contact the local police to file a police report.
4. Contact First Bank of Berne and other financial partners to cancel existing accounts held in your name and reopen new accounts.

First Bank of Berne Online Banking Tips

Online banking offers the convenience of accessing account information 24/7. With this convenience comes an additional responsibility to safeguard your personal information. Please review the following tips to maintain a safe and user friendly customer experience.

- Avoid using personal information in your password such as birth dates, or names of family members and pets.
- Avoid using the same password for multiple websites.
- Avoid using the password auto-save feature on your browser.
- Keep your password secure and avoid sharing your password with others.
- Log out of your First Bank of Berne online banking session when you are finished with your transaction(s).
- Review your account information often. Report any unusual activity to First Bank of Berne immediately.
- First Bank of Berne has implemented several control features pertaining to password safeguards. These include the requirements for an effective password and duration. Please access the First Bank of Berne online banking system for more information.

Protecting Yourself from Online Banking Fraud

While most companies that do business on the Internet, including First Bank of Berne, are very diligent in providing online protection for their customers, the first line of defense is knowledge about what you, the end-user, can do to protect yourself. The two most prevalent types of fraud, “Keylogging” and “Phishing” occur from viruses on your computer. In both cases, the end result is the fraudster capturing your login credentials.

CONSUMER AWARENESS INFORMATION GUIDE

Keystroke Logging or Keylogging

Keylogging is a method by which fraudsters record your actual keystrokes and mouse clicks. Keyloggers are software programs that target your computer's operating system (Windows, Mac OS, etc.) and are "installed" via a virus. These can be particularly dangerous because the fraudster has captured your user ID and password, account number, Social Security number, and anything else you have typed. If you have the same ID and PIN/Password for many different online accounts, you've essentially granted the fraudster access to any company with whom you conduct business.

Here are some ways you can prevent yourself from being a victim of keystroke logging:

- Use Anti-Virus Software. This is the single most important thing you can do to protect your computer from viruses. There are many on the market today. If you opt to use a free version, make sure it is being offered by a reputable company and do research on the company and its product before installing.
- Keep your Operating System up-to-date with the latest security patches.

Phishing

Phishing is a scam where Internet fraudsters request personal information from users online. These requests are most commonly in the form of an email from an organization with which you may or may not do business. In many cases, the email has been made to look exactly like a legitimate organization's email would appear complete with company logos and other convincing information. The email usually states that the company needs you to update your personal information or that your account is about to become inactive, all in an effort to get you to click the link to a site that only looks like the real thing. If you click on the link to go to the phony website and enter all of your information, you've just been the victim of a phishing attack. The fraudsters have just captured all the necessary information to access your accounts online. **No reputable business will ever email you requesting that you update your personal information, including account numbers, system passwords or Social Security numbers via a link to their site.**

Follow these guidelines to protect yourself from phishing scams:

- Never click on a link from a business requesting that you provide them with personal information.
- Pay close attention to the URL (Internet address) behind the link. Often in phishing attempts, if you move the cursor over the link the fraudsters want you to click on, it has nothing to do with the actual company they claim to be.
- Do not log in unless you see the correct watermark or personal image on the screen.
- Report any phishing attempts to First Bank of Berne.

If you are unsure that the request is valid, open a new Internet session and manually key in the business' web address. If the business genuinely needs information from you, they will have you log in to your online account to see the request. In most cases, you'll just be greeted with a message indicating that the business will never email you requesting personal information.