Security Center

Educate Yourself

In order to help our customers protect themselves and have access to helpful data regarding information security, we've provided some important information and resources. As security concerns can be an evolving matter, we'll make periodic updates and changes to this information as needed. We'll help you get there.

Scams

Malware is any software that is intended to be harmful to a computer. Malware could be a virus, worm, Trojan horse, spyware or adware.

Pharming is a form of online fraud that redirects a website's traffic to a bogus website. The fraudulent website will look very similar to the legitimate website.

Phishing is a fraud scam that attempts to collect personal information such as usernames and passwords by an attacker claiming to be a trustworthy source. Phishing scams are generally initiated through an official-looking email that asks the victim to urgently click on a link and provide personal information. Other phishing scams originate in an email that asks the recipient to call a phone number to verify information. Often times the caller reaches an automated voice response system that asks them to provide personal identifying information.

If you think your computer system may have been compromised by one of the above, you should close your programs, conduct a scan of your PC with anti-spyware and anti-malware software and you should also clear your cache (go to Tools then delete Browsing History).

For more information about pharming or phishing, please visit http://www.bos.frb.org/consumer/phishpharm/index.htm.

Social engineering is a way of manipulating people to share their personal information.

For additional information on common scams, please visit http://www.fbi.gov/scams-safety/fraud.

Stay Informed

The U.S. Government has many resources available to consumers to help them stay informed of security issues, especially when it comes to cyber-related threats. One such tool is available through the United States Computer Emergency Readiness Team (US-CERT). Please visit http://www.us-cert.gov/ to subscribe to the US-CERT security alert email tool.

Protect Yourself

First National Bank North will never initiate an email or text requesting your bank credit or debit card number, account number, Social Security Number, Personal Identification Number (PIN), password or other personal identifying information. If you receive an email or text requesting information that appears to be from First National Bank North, do not respond to the email or text and contact your local First National Bank North branch immediately.

Do not share your personal identifying information with anyone who is not authorized to have access to your accounts. Personal identifying information includes your:

- ✓ Birthdate
- ✓ Social Security Number
- ✓ Credit or Debit Card Numbers
- ✓ Personal Identification Numbers (PINs)
- ✓ Password

- You can change your password as often as you like online and we encourage you to do so regularly. Do not use birthdays, phone numbers, or names that others can guess.
- Promptly review your account statements and immediately report any discrepancies or unauthorized transactions to your local First National Bank North branch.
- Always be suspicious of offers made by telephone, email or on a website that seem too good to be true.
- Do not respond to unsolicited email and do not click on links or open attachments within unsolicited email. If the email appears to be coming from First National Bank North go directly to our website to login.
- Always be suspicious of emails that use urgency or scare tactics.
- Always be suspicious of proposed transactions that require an advance payment by wire transfer.
- It is essential for you to install, frequently update, and regularly run anti-virus and anti-spyware protection programs on your computer. Keep account numbers, Personal Identification Numbers (PINs), credit and bank cards and checks in a secure location.
- Check your credit report regularly.

For additional information about protecting yourself from identity theft, visit http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/deter.html

How First National Bank North protects you

Federal regulations provide consumers with protection from fraudulent or deceptive electronic fund transfers. See the Electronic Fund Transfer disclosures that were provided at account opening for more information on this protection. For a current copy of these disclosures contact your local First National Bank North branch and we will be happy to provide one for you. For example, these federal laws establish limits on a consumer's liability for unauthorized electronic fund transfers. They also provide specific steps you need to take to help resolve an error with your account.

First National utilizes industry-standard security measures when it comes to protecting your information when using online and electronic services.

How to respond if you're a victim of fraud

If you believe that any of your personal identifying information has been lost, stolen or compromised, contact your local First National Bank North branch immediately!

- If your ATM/Debit card was stolen, have the existing card closed and a new card and PIN issued.
- Request to close the accounts that you believe have been compromised and open new accounts.
- Monitor your statements for any fraudulent activity. If found, contact your local First National Bank North branch immediately.
- Contact one of the major credit reporting agencies to place a fraud alert on your credit reports.

  - ✓ Experian: 1-888-397-3742 http://www.experian.com/
  - ✓ Equifax: 1-800-525-6285 http://www.equifax.com/home/en_us
  - ✓ TransUnion: 1-800-680-7289 http://www.transunion.com/

Notify the issuers of the credit cards you carry. If unauthorized charges appear on your credit cards or if unauthorized cards have been issued in your name:

- Request new cards with new account numbers.
- Monitor your credit card bills for fraudulent activity. If found, contact the credit card issuer immediately.

Contact your local police department to file a report.

Document the names and phone numbers of everyone you speak to regarding the incident. Follow up your phone calls with letters, and keep copies of all conversations.

For additional information about responding to identity theft, please visit http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html.

For more information about protecting yourself from identity theft and what to do if you are a victim of identity theft, visit http://www.consumer.gov/idtheft

Lost or Stolen Debit or ATM Card?

If your ATM / Debit card is lost or stolen it's important to act quickly!

If you discover your card is missing during regular bank hours, call your local bank immediately and report the loss or theft. If your bank is not open, call 1-800-264-5578.