Enhanced Login Security
FAQ

What is Enhanced Login Security?

Enhanced Login Security requires online users to provide something additional beyond today's username and password to login. This enhanced security means that even if a user has their password stolen in a phishing attack or by malicious software, the fraudster cannot access online accounts because they do not possess the additional factors needed, which are harder to steal.

Why is First National Bank implementing the Enhanced Login Security?

Protecting customers' personal information is our top priority. Enhanced Login Security provides you extra protection from fraud and identity theft. In addition, on October 12, 2005, the Federal Financial Institutions Examination Council (FFIEC), the regulators overseeing the banks and credit unions, communicated that passwords alone will no longer be acceptable as the sole means of achieving online security. The regulators now require that two forms of verification are used to access Internet Banking. The options include: 1)something you KNOW i.e. password 2)something you HAVE i.e. PC 3) something you ARE i.e. biometrics such as a thumbprint. This is a mandatory regulation that all banks and credit unions must adhere to by December 31, 2006.

Multifactor Authentication (MFA) is the recommended solution. Enhanced Login Security is one form of MFA and uses the password AND PC for verification.

How will Enhanced Login Security improve security?

Enhanced Login Security identifies you as the true "owner" of your accounts. Now, not only will your password be recognized, your computer will be recognized as well. If the bank doesn't recognize your computer where you've logged in, you will be prompted to provide information that only you will know. This new layer of security will act as an additional line of defense against unauthorized access to your accounts.

What changes will I see with my Internet Banking Account once the Enhanced Login Security is implemented?

Once Enhanced Login Security is set up on your computer, it is business as usual. Your online banking experience will remain the same.

What other precautions can I take to protect myself from identity theft?

- Don't give your Social Security number or other personal credit information about yourself to anyone who calls you. **The bank will never call you to ask for this information.** Criminals use this information to open new charge accounts posing as you.
- Be suspicious of any email with urgent requests for personal financial information (phishing scams)
- Tear up receipts, bank statements and unused credit card offers before throwing them away. Criminals can collect bits of information about you by going through your trash.
- Watch for missing mail. An identity thief may steal your mail and file a change of address form with your credit card company or the U.S. Postal Service.
- Review your monthly accounts regularly for any unauthorized charges.
- Order copies of your credit report once a year to ensure accuracy.
- When conducting business online, make sure the site is secure. Make sure your browser's padlock or key icon is active.
- Don't open email from unknown sources and use virus detection software.
- Protect your PINs and passwords and change them frequently.