Blissfield STATE BANK

Blissnet™ Online Banking
Fast / Convenient / Secure

The following are security features employed by Blissnet™ Online Banking to help protect your identity and transactions:

1. **User IDs—**When you apply for Blissnet Online Banking, you are given a 12-digit user ID number. This number never changes and you can use it for the first login screen. Optionally, you can give yourself a more user-friendly Alias to use in place of the number by clicking on the Options tab and then the Personal tab under that. In the Enter New window for Blissnet ID, enter what you would like to use. The requirements for this are specified on the screen. If you try to use an alias that another customer of ours is already using, you will receive an error message and will need to try something else.
2. **Passwords:** We encourage strong passwords by requiring them to be a minimum of 8 characters in length. Passwords use letters, numbers, and special characters. (Available special characters are shown on the password change screen.) Passwords may be changed at any time using the Options and Personal tabs.
3. **Personal Image/Icon:** When you first use Blissnet, you will be asked to choose a Watermark (picture). The watermark is an anti-phishing measure that shows you that you are using the legitimate Blissnet Online Banking site.
4. **Security/Challenge Questions:** You are required to establish three security questions, chosen from drop-down lists, and type in answers (not case-sensitive). These questions are used to challenge you when your session risk score exceeds a given threshold* or you generate a Bill Pay transaction with a dollar amount of $1000 or more. You are also required to change your security questions every 6 months.

***About Session Risk Scores:**
Every time you login to Blissnet Online Banking, you session will be given a risk score based on a variety of factors including: current IP address, type of device used, and Browser version. A higher session risk score indicates a greater possibility of unauthorized access. For example, if you typically login from a Windows PC using Internet Explorer 8 and suddenly change to a browser such as Firefox or login from a completely different device such as a smartphone, you may be required to answer two of your security questions in order to continue with your session.

Additional information:

- When you call our Blissnet support or we call you (solicited or not), we may ask you for information to verify your identity—ex: last 4 digits of your social security number, your birthdate… We will not ask you for your Blissnet user ID or Alias since we can access this information ourselves. We also will not ask for your password as this is not available to us for your protection.
- Commercial (business) users of Blissnet are advised to periodically perform risk assessments of their use of Blissnet and evaluate their controls over Blissnet access (ex: which employee(s) have the user ID and password).
- Protect yourself from online fraud and identity theft. Here are some helpful tips and resources:
    1. Use common security tools such as a computer firewall and reputable antivirus software to protect your computer from malware and hackers.
    2. Keep your computer operating system and security software up to date with the latest security patches and virus definitions.
    3. Be wary of possible email and online scams. Never click on links or open attachments in unsolicited or unexpected email messages and only visit websites hosted and maintained by trusted, reputable companies. For more information on email and web scams, visit the following website: http://www.microsoft.com/security/online-privacy/phishing-scams.aspx
    4. Use strong passwords, change them periodically, and keep them private. For tips on how to create strong passwords, visit the following website: http://www.microsoft.com/security/online-privacy/passwords-create.aspx
    5. Monitor your credit and view your credit report at least once a year. You can get one free credit report per year online at https://www.annualcreditreport.com/cra/index.jsp
    6. Also visit OnGuardOnline.gov and FTC.gov for more information on protecting your information and your identity online.
- If you notice suspicious account activity or experience customer information security-related events, call the bank and ask for Andrew Beal, Daniela Yovanov, or David Robertson.