For All Online Banking Customers

Safeguarding Your Information

Type **your Internet Banking URL**

Always access our Internet banking by typing the correct web address (http://www.fsbanks.com) into your browser. Do not click on a link in an email to take you to a website, or enter personal details either in the email or website.

Password Security

You should always be wary if you receive unsolicited emails or calls asking you to disclose any personal details or card numbers. This information should be kept secret at all times. Be cautious about disclosing personal information to individuals you do not know.

Please remember that we will never contact you directly to ask you to disclose your password information.

If it sounds too good to be true...

It probably is. Don't be conned by convincing emails offering you the chance to make some easy money. As with most things, if it looks too good to be true, it probably is. Be cautious of unsolicited emails from overseas - it is much harder to prove legitimacy of the organizations behind the emails.

PC Security

It is important to use up-to-date anti-virus software and a personal firewall. If your computer uses Microsoft Windows, it is important to keep it updated via the Windows Update feature. If you use another operating system you should check regularly for updates.

Ensure you also regularly patch Java and Adobe products. These items are frequently updated because of vulnerabilities and hacker use of those vulnerabilities to install malware on your computer.

Consider using a single computer for your online banking and restrict other uses on it. The more that Internet surfing is done on the computer used for financial and other important transactions, the more risk that you are taking.

Avoid Public Wireless Internet Access

You should be vigilant if you use Internet cafes, or a computer that is not your own and over which you have no control, such as computers supplied in hotels. Hackers and identity thieves often monitor these networks or may install malware to capture your login credentials.

Keep your identity private

Your identity can be as easily stolen offline as it can online. It is important that you comply with instructions about destroying expired bank cards. Do not write down your Username and Password and leave it next to your computer.

Do not use the same password for online banking that you use for any other website. Then if those other sites are hacked and your password is stolen, at least it won't be the same as your online banking password. First State Bank of Blakely has other login credentials other than just a password, but the argument for using a unique password just for online banking remains the same.

You should also consider using a shredder (preferable a cross-cut shredder) to destroy bank and other statements that may contain sensitive personal information.

It is advisable to store important documents in a suitable locked and fire-resistant container.

For all website applications, use a complex password that is not easily guessed. It should not contain full names or words and include special characters and be at least 8 characters long.

Check your statements
It is important to check your statements regularly; a quick check will help identify any erroneous or criminal transactions that might have been performed on your account without your knowledge.

Check for Spyware/Malware
In addition to being protected by using up-to-date antivirus software you should also regularly use software to remove spyware from your computer, as these programs record information about your Internet use and transmit it without your permission. In some circumstances this can compromise your PC security. Remember current anti-virus software does not catch 100% of every virus. Consider utilizing multiple programs to regularly scan your computer.

Ensure you log off properly
It is important to completely log off from your Internet banking session; simply closing the window you performed the transaction in may not close the banking session. If your computer is infected with a Trojan, your session may become hijacked by a criminal and financial transactions may be performed without your knowledge. It is also advisable to disconnect from the Internet if you are not planning to use it.