First United
Bank & Trust

First United Bank & Trust Security Provisions

Security / Protecting Online Applications First United Corporation is committed to protecting the security of your personal information, including when it is transmitted online. Therefore, we utilize advanced Internet security technology to protect your personal financial information against unauthorized access.

First United Corporation will never request personal information by means of e-mail or a pop-up window. User IDs and Passcodes are used to help safeguard access to your information through the website. As always, we strongly encourage you to assist us in that effort by not sharing your User ID and Passcode with anyone.

When you choose to apply for a loan or deposit product using an online application, you will be required to provide personal information that is necessary to process your request. To ensure that your information remains confidential, it is sent to First United Corporation in a "secure session" utilizing Secure Socket Layer (SSL) technology. SSL is a security protocol for transmitting information via the Internet. Internet Explorer, as well as other internet browsers such as Firefox, Chrome, and Safari support SSL. In addition, other web sites SSL technology scrambles or "encrypts" information as it moves between your computer's browser and our computer systems.

We want to help keep you and your money safe.

At First United we hold the security of your confidential information in the highest regard. We make every effort to ensure that your non-public data is secure and that your information will not be compromised.

However, there are steps you can take to help protect yourself against the potential threats that we all face, every day, online. By following a handful of simple, common-sense steps, you can help ensure that you are safe in your journeys on the Internet:

- Be sure that you are running the latest browser technology. You can find the latest versions of these browsers here: Internet Explorer | Firefox | Chrome
- Be sure that your operating system is current; you can check the Windows Update center on your PC to see available updates.
- Use strong passwords for your various logins.
- Use a firewall to protect your computer.
- Set up Mobile or Internet Banking account alerts.
- Exercise caution when posting information on social media.

Looking for information about current security topics? Check out our Security Briefs. We are committed to informing you of topics that may impact your online security, but please remember this information is not all inclusive. You should take time to check for alerts and information from your hardware and software providers. These are general briefs for

informational purposes only. For further assistance with any of these suggestions, please contact your computer support personnel.

Security Tips to Remember

- It is a best practice to never give out personal information in response to an unsolicited call or email. There are fraudsters who will use our public information to try to attain personal information from you.
- Unless you initiate the contact or we are completing an application for you, First United will NEVER request your personal information (e.g., account number, Social Security number or mother's maiden name) through email, U.S. mail, text or phone.
- Various types of information will be requested by First United to identify you on the phone; however, we will NOT request your online banking passcode. This should be kept safe and secure by you and not written or shared with anyone.
- First United will never send an email or text requesting that you click on a hyperlink and enter your login credentials or personal information. If you receive this type of email or text, please forward it **abuse@mybank.com** or contact our **Customer Service Center at 1-888-692-2654**.
- Always remember, it is a best practice to verify any suspicious emails by calling the supposed sender (at a phone number) before following any email requesting information or financial transactions (such as wire transfers), and to not visit un-trusted websites or follow links provided by unknown or un-trusted sources that may be included in those same emails.