Online Banking Security

Commercial Trust Company takes this matter very seriously. Your connection to Online Banking uses the best commercial data encryption available. Other "behind the scenes" mechanisms are in place to assure the security of your financial information. You may have also noticed that at no time does your account number, or Tax ID number appear on screen over the Internet. Security is not a one-time effort with our Online Banking system. As security improvements are available in the future, our specialists will continue to make any needed enhancements to assure that your account information is safe and secure.

Commercial Trust Company will never request your User ID and password when sending a non-secure email to your personal email address. We want you to be aware that customers of a few banks have recently reported receiving an e-mail message that directed them to a fraudulent login page to "reactivate their account" by entering their access information. Neither the message nor the login page was from the actual bank. Rather, this was an illicit attempt by a third party to gain access to the customer's login and personal information. The messages are sent to a number of people to try to reach a few that actually have an account at that bank. If you ever receive such a message, you should delete it immediately.

It's easy to protect yourself against such schemes. Whenever you go to a secure login page, double-click on the lock that appears in the lower right corner of your browser. The certificate information will appear, and for Commercial Trust Company, it should read www.banno.com.

Here are a few other points to keep in mind to help keep your electronic banking safe and secure:

Best Practices for Online Banking Security

- Use strong, complex passwords that contain:
    - alpha/numeric characters and symbols
    - upper and lower case characters
    - minimum of 8 characters but longer is recommended
    - no real words or names of family/friends/pets
    - use entire keyboard; avoid strings of identical characters
- Change your passwords regularly and use a different password for each website you access.
- Never reveal your confidential Online Banking login ID, password, PIN or answers to security questions to anyone.
- Never reveal your confidential Online Banking login ID, password, PIN or answers to security questions by e-mail.
- Never bank online using computers at kiosks, cafes, unsecured computers or unsecured wireless networks.
- Prohibit the use of shared user names and passwords for your online banking accounts.

Tips to Avoid Identity Theft by Phishing, Spyware and Malware

- Don’t open e-mail from unknown sources.
- Never respond to a suspicious e-mail or click on any hyperlink embedded in a suspicious e-mail:
    - Call the purported source if you are unsure who sent an e-mail.
    - If an e-mail claims to be from your bank, call a customer services representative.
- Educate your staff about current scams and loss- prevention steps.
- Make sure all of the computers you use for work-related business, at the office and at home, have the latest versions and patches of both anti-virus and anti-spyware software.
- Maintain updated and patched systems and software.
- Install a firewall between your computers and the Internet.
- Check your settings and select at least a medium level of security for your browsers.
- Clear the browser cache before starting an online banking session to eliminate copies of Web pages that have been stored on the hard drive.