PEOPLES TRUST Company

Security Statement

The security and protection of your accounts and our systems are of the utmost importance to us, whether it's through traditional banking methods or through Peoples Trust Company Online Banking Services. We take extraordinary care in an attempt to provide a safe and secure online banking delivery system. We maintain physical, electronic and procedural safeguards that comply with federal guidelines to guard your nonpublic personal information against unauthorized access or use. Please read our Security Statement outlined below.

1. Your Responsibilities

The use of our Peoples Trust Company Online Banking Services is for authorized users only. Access to these services requires an Access ID and Password to authenticate with our systems. We utilize additional layers of security to verify your identity and protect your information. It is your responsibility to protect your Access ID, Password and other security data e.g. image, pass phrase, challenge questions and answers with the same degree of care and secrecy that you would use to protect other sensitive nonpublic personal information.

Any individual using this system is subjected to having all activities monitored and recorded by us. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, we may provide the evidence of such monitoring to law enforcement officials.

2. Peoples Trust Company Security Measures

Peoples Trust Company's Online Banking Services combine a variety of industry standard and customized security technologies, methodologies and best practices to protect our customer's information. The system's architecture and design is professionally assembled to control and monitor authorized access to customer and account information from the Internet. Some of these measures are outlined below:

- Data encryption between the customer and our Online Banking Server. We utilize Secure Sockets Layer (SSL) 128 bit Encryption via digital certificates issued by Verisign. Encryption is a technology that "scrambles" or alters the content of information transmitted between the customer and our systems in such a manner that only the customer and our systems can decipher or "unscramble" the information. This measure is used to ensure that it is virtually impossible for anyone other than the customer and our systems to read the information that is being transmitted.

- We utilize multiple firewalls to control, direct and authenticate communication from the Internet. This measure is used to ensure that only appropriate and authorized communication is allowed between the customer and our systems.

- Access to your account(s) is authenticated by the validation of an Access ID and Password as well as the use of other security data to authenticate who you are. This measure is used to validate the customer that is attempting access to our systems.

- Passwords are required to be changed every six months or more frequently. This measure is used to reduce the exposure associated with the length of time that a password exists. Changing passwords frequently is considered an excellent practice that creates an unknown randomness which enhances Access ID security.

- Passwords are required to be generated using a combination of upper & lower case characters, alpha & numeric characters, as well as the use of special characters. This measure is used to reduce the possibility of someone compromising a password that could otherwise be considered as “simple” or “guessable”.

- Access to Online Banking is restricted to (4) attempts before the account is locked-out. If this occurs, you will need to contact Peoples Trust Company in order to have the account unlocked. This measure is used to reduce the possibility of someone “guessing” a customer’s password by having too many attempts without locking the account. If an account was repeatedly locked out, it may suggest inappropriate access attempts.

- We have dedicated resources that provide a variety of monitoring techniques to detect unusual or unauthorized activity. This measure is used to ensure that we can quickly and efficiently respond to potential inappropriate use our systems or unauthorized access attempts.

3. Virus Protection

Peoples Trust Company is not responsible for any electronic virus or viruses that you may encounter. We suggest that you use “up-to-date” antivirus software to protect your computer(s). Viruses can corrupt and destroy your computer programs and files and could possibly disclose unintended nonpublic personal information about you. We also strongly recommend that you keep your computer(s) updated with current software patches and service packs as recommended by the developer of your computer operating system (e.g. Microsoft) and that you do not open e-mail attachments that might be considered suspicious or of an unknown origin. Following these recommendations will aid in the protection of your computer and transactions that you conduct through our Peoples Trust Company Online Banking Services as well as other businesses.

4. Hyperlinks

Hyperlinks to other Internet resources are used at your own risk. The content, accuracy, opinions expressed and other links provided by these sources are not investigated, verified, monitored or endorsed by Peoples Trust Company. Other websites’ security statements may be different from ours. Please read them when you visit their websites.

Although Peoples Trust Company has taken these reasonable and appropriate measures to mitigate any foreseeable risks and to ensure that your personal information is secure, we cannot guarantee that the nonpublic personal information that is exchanged will not be intercepted by others and possibly decrypted. We are not liable for a breach of security that occurs for reasons outside of our control.