WOODTRUST BANK
BANKING | INVESTMENTS | TRUST

BUSINESS BANKING - ONLINE SECURITY

WoodTrust Bank is committed to protecting your account information and ensuring that WoodTrust Bank's Online and Business eBanking Web sites are secure. We use the latest technology available including Advanced Login Authentication and 128-bit encryption. Additionally, the security of your computer system and passwords is also critical to your online bank safety.

COMMON WAYS CYBER CRIMINALS OBTAIN BANK INFORMATION INCLUDE:

- **Phishing** – phishing attacks use fake emails containing links to counterfeit Web sites that look like the authentic sites. Often the emails state that there is a problem that needs to be fixed with the account. When the user enters their bank account information on the spoofed Web site, the fraudster has what they need to gain access to the bank account. Under no circumstances will WoodTrust Bank ever email you and request confidential information such as your account number, user name, or password.
- **Malware** – Malicious software can be installed on a computer, such as spyware or keystroke loggers when an email attachment is opened or a pop-up ad is clicked on. Malware can capture keystroke information and other data. The software can also generate Web pages that look legitimate but are not; the Web address will vary in some way. Once the bank information is entered, the criminal has what they need to access the account.

Fortunately, there are ways to help protect you and your business against online bank fraud. The best defense is to ensure that you have current anti-spyware, firewall and virus protection software, and that you avoid clicking on unknown emails or Web site links.

Below are some safety tips for online banking. Use this as a guide to help you safeguard passwords and your account information.

IT Safeguards

- Install Firewall, Virus Protection and Intrusion Protection Software
- Update your anti-virus software daily
- Regularly download vendor security patches for all of your software
- Change the manufacturer's default passwords on all of your software
- Monitor, log and analyze successful and attempted intrusions to your systems and networks
- Select at least a medium level of security for your browser
- Business customers should limit administrative rights on users workstations
- Business customers should perform a risk assessment and controls evaluation periodically

Password Protection

- Make your passwords complex. Use a combination of numbers, symbols and letters. Use symbols or numbers in the middle of a word to make it harder to decode. Never use the word "password" or a series of numbers such as 1234.
- Change your passwords regularly (every 45 to 90 days)
- Do not give your user name or password to anyone
- Never save your password online if you are prompted, or use a password saving program to save your password on your computer. If needed, write it down and store it in a secured area.

General Online Safety

- Conduct Internet Banking activities only on those computers you know to be safe and secure. Do not use public or other unsecured computers. If possible, dedicate a PC solely for financial transactions (no web browsing, emails, or social media).
- When conducting financial transactions online, make sure the browser screen displays a locked icon and the website URL begins with “https:”. The “s” means that it is secure.
- Never conduct banking transactions while multiple browsers are open on your computer.

Log In/Log Out Recommendations

- Confirm last sign on date on the Internet Banking “Home Page”
- Log out when you have completed your banking activities and close browser

Business eBanking User Controls

- Do not use account numbers when providing nicknames for your account(s)
- Establish separate user names and passwords for each user
- Create a new User to replace Admin User functions and lock default Admin User ID
- Establish dual control measures for all financial transactions
- Set-up multiple user roles. Limit the number of users with approval authority
- Create multiple user thresholds and user dollar limits
- Use system email alerts to notify you when:
    - an ACH template has been modified
    - transactions have been processed
- Review history files daily such as ACH, Funds Transfers, and Bill Payment
- Delete User access when employees leave your company

Remember, you are responsible for protecting your password and account information in order to prevent online bank fraud. If you notice any unauthorized transactions, contact us immediately.