Protect Yourself Online

Online Banking

Do not use public or other unsecured computers to log into Online Banking

Check your last login date/time located under the Account Summary section on the left-hand panel

Review account balances and detailed transactions (preferably daily) and immediately report any suspicious transactions to your financial institution

View transfer history available through viewing account activity information

Whenever possible, use Bill Pay instead of checks to limit account number dissemination exposure and to obtain better electronic record keeping

Take advantage of and regularly view system alerts including balance alerts, transfer alerts, and password change alerts

Do not use account numbers, your social security number or other account or personal information when creating an account alias or nickname

Whenever possible, register your computer to avoid having to re-enter authentication information

Review historical reporting features of your online banking application on a regular basis to confirm payment and other transaction data

Choose a current browser version that will identify secure sites by highlighting all or part of the URL in green

Never leave a computer unattended while using online banking

Never conduct banking transactions while multiple browsers are open on your computer

When you have completed a transaction, ensure that you log off properly to close the connection

Username and Passwords

Create a strong password with at least 8 characters that includes a combination of mixed case letters, numbers and special characters

Make your password unique and change it frequently

Do not use the same username and password for every online account

Never store you username and password where others could gain access to it

Never share username and password information with third-party providers

Avoid using an automatic login feature that saves usernames and passwords

Email Security

Do not open e-mail from unknown sources Be suspicious of e-mails purporting to be from a financial institution, government department or other agency requesting account information or verification, or banking access credentials such as usernames, passwords, PIN numbers and similar information. Opening file attachments or clicking on web links in suspicious e-mails could expose your system to malicious code that could hijack your computer. Chattahoochee Bank of Georgia will never ask for your username and password via email.

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 claiming to be from Chattahoochee Bank of Georgia seems suspicious, check with us by calling 770-536-0607 or visit the bank at 643 E. E. Butler Parkway.

Install anti-virus and spyware detection software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product

Update all of your computers regularly with the latest versions and patches of both anti-virus and anti-spyware software.

Ensure computers are patched regularly, particularly operating system and key applications

Install a dedicated, actively managed firewall, especially if using a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to your network and computers

Check your settings and select, at least, a medium level of security for your browser

Clear the browser cache before starting any Internet Banking session to eliminate copies of web pages that have been stored on the hard drive. How the cache is cleared depends on the browser and version you are using. This function is generally found in the browser's preferences menu

Be advised that repeatedly being asked to enter your user ID or password are signs of potentially harmful activity

Do not use unsecured wireless connections or public/shared computers to access accounts or to perform financial transactions

Additional Tips for Wireless Network Management

Business Customers: Wireless networks can provide an unintended open door to your network. Unless a valid business reason exists for wireless network use, it is recommended that all wireless networks be disabled. If a wireless network is to be used for legitimate business purposes, it is recommended that wireless networks be secured as follows:

- Change the wireless network hardware (router /access point) administrative password from the factory default to a complex password. Save the password in a secure location as it will be needed to make future changes to the device
- Disable remote administration of the wireless network hardware (router / access point).
- If possible, disable broadcasting the network SSID
- If your device offers WPA encryption, secure your wireless network by enabling WPA encryption of the wireless network. If your device does not support WPA encryption, enable WEP encryption
- If only known computers will access the wireless network, consider enabling MAC filtering on the network hardware. Every computer network card is assigned a unique MAC address. MAC filtering will only allow computers with permitted MAC addresses access to the wireless network