Account Authentication & Online Banking

Things We Do To Protect You Online

- **Never ask you to send us confidential information online** – You will not receive emails from us requesting information such as your Social Security Number, account number or passwords.
- **Verify certain transactions by text message -** For certain high risk transactions (typically large bill payments and external transfers) we may request a verification passcode before processing your transaction. If you register a mobile number within online banking the passcode will be sent to your mobile device. If you do not register a mobile number you can call us during regular business hours and we will assist you.
- **Send you alerts** – For business customers with Cash Management you'll receive alerts when orders for new wires are submitted, ACH batches are initiated, when new users are added, and when changes are made to users.
- **Ask you challenge questions** – Our system may ask you challenge questions when it sees "out of pattern" or "high-risk" transactions. This includes signing on from a computer you're not normally associated with when you're traveling.
- **Contact you** – For ACH and wire transactions we require an "offline" verification (phone or fax) before we will process them. We may also contact you if we suspect suspicious activity on your online account.
- **Assign dormant status** - If you are not using your Online Banking access, our system applies a dormant status (after 6 months of no use) to protect you from fraudulent activity. You can call to speak with a bank representative to reactivate your account when needed. Accounts that have no online activity for 12 months, will be deleted from the system to further protect you.

Things You Can Do To Protect Yourself

- **Protect your online passwords** – Don't write them down or share them with anyone.
- **Change your password at least 2-3 times annually** – Changing your password frequently helps protect you from fraud.
- **Use updated anti-virus software and a personal firewall on your computer.**
- **Protect your answers to security questions** – Do not write down your security questions or answers or share them with anyone.
- **Use secure websites for transactions and shopping** – Shop with merchants you know and trust.
- **Always log off from Online Banking.**
- **Be cautious when using public hotspots and consider your Wi-Fi auto-connect settings.**
- **For Cash Management users, use a dedicated PC without email to access your accounts and facilitate transactions** – The vast majority of account takeovers come from viruses and malware that are planted within an email – so try using a computer just for banking if you're utilizing our more complex services.

Community BANK
Member FDIC

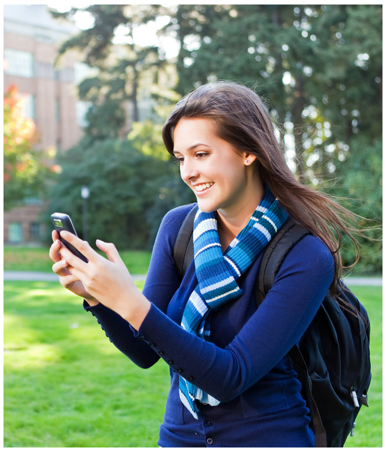
See additional tips
on the reverse side

Email Security Tips

- Be wary of suspicious emails. Never open attachments, click on links, or respond to emails from suspicious or unknown senders.
- If you receive a suspicious email that you think is phishing (an attempt to steal your information), let us know immediately.

Mobile Banking Security Tips

When you use a mobile device for browser or text-based account access, keep these tips in mind:



- Use the keypad lock or phone lock function on your mobile device when it is not in use. These functions password-protect your device to make it more difficult for someone else to view your information. Also be sure to store your device in a secure location.
- Frequently delete text messages from us or any bank, especially before loaning out, discarding, or selling your mobile device.
- Never disclose via text message, phone call or email your personal or financial information, including account numbers, passwords, Social Security Number or birth date.
- If you lose your mobile device or change your mobile phone number, remove the old number from your mobile banking profile at www.communitybanknet.com.

Learn more about online security by visiting any of these websites:

www.staysafeonline.com
www.idtheft.gov
www.usa.gov
www.ftc.gov

Community BANK

Member FDIC