Frequently Asked Questions
INTERNET BANKING

JACKSON COUNTY BANK
8 Main Street, Black River Falls, WI 54615
(715) 284-5341 Member FDIC
jacksoncountybank.com

ABOUT INTERNET BANKING

Q: What is Internet Banking and how much does it cost?
A: Internet Banking enables you to access your accounts electronically through a computer via the Internet. There is no charge for this service.

Q: What do I need to bank online?
A: To bank online you will need:
- A Jackson County Bank deposit or loan account
- Internet access
- A browser with the proper encryption capabilities (See *Internet Banking Support – Which browser can I use?* page 3.)
- You must successfully enroll in Internet Banking

Q: How do I enroll?
A: You may enroll in Internet Banking online (online enrollment not available for businesses) or by completing an enrollment form.

Online Enrollment

Go to jacksoncountybank.com and in the login area click on "Enroll" and then click on "Enroll Online" (Option 1). To enroll online and begin using Internet Banking immediately, you will need to have an email address on file with the bank and have access to it, know your social security number, account number and contact information as recorded with the bank. If you do not have all of this information, you can still enroll online and we will mail you the information you need to begin using Internet Banking.

Complete an Enrollment Form

You may also enroll by completing an Internet Banking Enrollment Form. This form can be accessed online by visiting jacksoncountybank.com/sign-up and downloading the Consumer Enrollment Form or Business Enrollment Form. You may also pick up a form at any location; or a form can be sent in the mail if requested.

Q: How soon will I be able to access my account information after I sign up for Internet Banking?
A: If you have a valid email address on file with the bank, and the required additional information, you can enroll online and begin using Internet Banking immediately. If you do not have all the information or use the enrollment form, a letter will be sent to you including your User ID, PIN and Internet Banking Agreement and Disclosure Statement. If you apply in person, you should be able to use Internet Banking the same day.

Q: What accounts can I access with Internet Banking?
A: Checking, Savings and Money Market, Certificates of Deposit, Loans, IRAs and ODPs

Q: What will I be able to do with Internet Banking?
A: View account balances, account history or statements, transfer funds between eligible accounts, view and print images of checks and deposits that have cleared your account, activate or cancel debit cards, download transactions and request stop payments. There are also optional services available such as Mobile Banking, Bill Pay and Remote Deposit.

Q: How current is the information displayed on Internet Banking?
A: The balance and transactions display the current bank information.

Q: Will there be times when I will not be able to access my account?
A: The system is available 7 days a week, 24 hours a day, and has an extremely high "up time" percentage. Unfortunately, some down time is necessary to keep our system constantly improving, reliable and safe. Down times are usually scheduled during low usage periods of the day. A list of scheduled down times can be found at www.jacksoncountybank.com/internet-banking-support.

Q: Are there limits on the number of transfers I can make?
A: The Internet Banking system does not limit the number of transfers you can make. However, Federal Regulations limit the number of withdrawals and transfers on certain types of savings and money market accounts. If you are unsure about the restrictions on your accounts, please call us at 715-284-5341 or use the **Contact** feature on the web site to contact us securely.

SECURITY

Q: Is Internet Banking Safe?
A: We and our service providers have established security procedures and have procedures in place to prevent unauthorized access to accounts and transactions. The system uses up-to-date encryption methods and software. However, there is no assurance that this type of activity will be completely secure, or that access to Internet Banking will be free from delays, interruptions, malfunctions, or other inconveniences generally associated with this electronic medium. We are not responsible for any electronic viruses, spyware, phishing attempts or other malicious Internet or computer related activity that you may encounter. We encourage our customers to obtain software and/or hardware to combat this activity including anti-virus, anti-spyware, firewall, anti-spam and privacy software for example. Users should also keep all software and devices current and regularly update the software and use malware scans for detection.

Q: What is encryption, and how does it make everything more secure?
A: Encryption is rewriting something in code which can then be decoded later with the right key. The effectiveness of encryption is in the number of bits. The higher the number of bits, the better the encryption is. In our pursuit to maintain security on our Internet Banking product at the strongest available level, the encryption standard for Internet Banking is 128-bit. This means all users will be required to use a browser with the 128-bit standard.

Q: How do I know if I'm viewing a secure Web page?
A: All the most common browsers have a padlock in either the location/address bar or in the status bar. A locked padlock indicates a secured page.

Q: What else assures the security of my banking information?
A:

- Your accounts are identified by nicknames rather than account numbers in the account listing area.
- Internet Banking utilizes encryption protection for your banking information.
- Log-in sessions have a time-out limit. If you do not respond when prompted, your session is disconnected. This assures that sessions are not left open and unattended.
- Your password must be between 8-15 characters with a required alpha, numeric and special character. This complexity generates greater security for you. You will also be prompted to change this password periodically for added security.
- Accounts are locked after three invalid login attempts.
- High level firewall and Intrusion Detection Systems monitor the Internet Banking System 24/7/365.
- Unusual activity is monitored to protect your accounts.
- Challenge questions are used to authenticate you during higher risk activity.
- At the bottom of the *Account Listing* you can track when your Internet Banking account was last accessed.

For more information on security and identity theft, please visit our website.

USING INTERNET BANKING

Q: Once I sign up, what happens?
A: Once you receive your Internet Banking user name and password and log in for the first time, you will need to change your password.

Q: I share my accounts with someone. Do we both need a user name and password?
A: Yes, we advise setting up individual user names and passwords because each account you own may be owned differently. Also, passwords must be changed periodically and when sharing a password, this could cause problems. Remember—by giving someone your user name and password you will be authorizing access to your accounts, and you are liable for the transactions made using Internet Banking.

Q: Can I personalize my User ID to something easier for me to remember?
A: Yes, you may change your User ID to something easier for you to remember. To change your User ID, log in to Internet Banking and click on OPTIONS. This will bring you to the Personal category under OPTIONS. Here you can add a *Personal ID* that is easy for you to remember. You can then use this ID in place of your Internet Banking ID number when logging in.

Q: Can I tell my Personal ID and password to someone else?
A: Because your Personal ID and password are used to access your accounts, you should treat them as you would any other sensitive or personal data and keep it confidential. Do not use this password for other applications, such as email. Change your password frequently using the OPTIONS tab in Internet Banking.

Q: Can I use Internet Banking on my smart phone?
A: You may use Internet Banking on your smart phone, HOWEVER we recommend you use our Mobile APP or Web Mobile for the best functionality on a mobile device. To sign up for Web Mobile log into Internet Banking and go to the options tab. For instructions on downloading our free app go to https://www.jacksoncountybank.com/mobilebanking/ .

Q: What can I do with my accounts?
A:

- Transfer funds from checking or savings accounts to checking or savings accounts.
- Transfer funds from a line of credit to checking or savings accounts.
- Make transfers to and from an Overdraft Protection Line with the corresponding checking account.
- View images and print images of checks and deposits that have cleared your account.
- View statements.
- Make payments from checking or savings accounts to loan accounts with us.
- View account information and current balance.
- View current transactions, view a date range of transactions or view previous statements.
- Download account information.
- Report a lost or stolen ATM or Debit Card.
- Activate or de-activate a Debit Card.
- Initiate a Stop Payment.

Q: How late in the day can I transfer funds?
A: Transfers made on business days before 9 P.M. will be processed on that business day. Transfers made after 9 P.M. or on weekends or holidays will be processed on the next business day. *Note: Infrequently, the system's evening processing may be running at the same time an Internet Banking user is making a transfer. If this occurs, you may not see the transfer in the transaction list until the next business day. However, if you have received a confirmation number the transfer will be made as scheduled.*

Q: Can I set up a transfer for a future date?
A: Yes! In addition to a single future transfer, you can also set up a transfer to be done on a weekly, bi-weekly, monthly, or semi-monthly basis. Be sure to note the Stop Date if you are setting a recurring transfer. You will NOT be notified of the end date of the transfer unless you set up an Event Alert. (OPTIONS – ALERTS – EDIT EVENT ALERTS – choose EXPIRING TRANSFERS and TRANSFERS EXPIRED.)

Q: How do I make a transfer?
A: Log in to Internet Banking and from the *Accounts* tab click the drop-down menu across from the account and choose *TRANSFERS*. Complete the TRANSFER FUNDS TO, AMOUNT, FREQUENCY (a one-time transfer or a recurring) and DATE. Click Submit and then Confirm. (If you transfer to or from a loan or overdraft protection account, the screen will quickly change after your account selection in order to reflect the correct transfer options.)

Q: How do I edit or delete an existing transfer?
A: On the Accounts page, choose Transfers from the drop-down menu across from your account. From the Transfers sub-menu select "Pending". This will display a selection of all currently scheduled transfers for the account indicated. From the drop-down menu to the right of the transfer, you may select View, Edit or Delete to make changes to your transfer. If a check box does not appear to the left of the transfer and/or the drop down only offers the "View" option, this transfer was not set up directly by you via Internet Banking and you must contact us to make any changes.

Q: How do I change my account nicknames?
A: The account nickname is the friendly name you gave your account because Internet Banking does not identify your account by account numbers for security purposes. To change a nickname, for example from "Vacation Savings" to "Tax Escrow", log in to Internet Banking and click on *OPTIONS - Account*. Simply type in your new nickname (pseudo name) and click submit. You can also change the display order here by dragging the account names.

Q: How can I view just certain transactions?
A: Log in to Internet Banking and select *TRANSACTIONS* from the drop-down menu to the right of the account you wish to view. If you would like to view a specific range of transactions or only certain types of transactions, choose SEARCH below the black bar at the top of the screen. Then specify which transactions you would like to display (it is not necessary to fill in all fields). Once your transactions appear you may click on any header to sort by that header.

Q: How can I view my checking account statement?
A: You may enroll in eStatements to have your statements delivered electronically to give you faster access and save paper. If you prefer that your statements are mailed, you may also access the statement information through internet banking. After logging in choose *ACCOUNTS* and then *STATEMENTS* from the drop-down menu to the right of the account you wish to view. Choose the statement you would like to display. You may choose from the following view formats.

The **PDF format** is commonly used with the Adobe Reader program. It is a nice format to use because you can click on the page number on the side bar to skip to the page you wish to view. You can also do searches for certain dollar values or words. Adobe Acrobat is required to view this format. The good news is Adobe offers Acrobat Reader as a download free of charge. Visit http://www.adobe.com.

The **HTML format** is the same format that your browser uses. Your statement will pop up in your browser window. If you consider yourself a beginner and just want to see the information, you will probably feel most comfortable using this view format.

The **Text format** is the format that allows you to save the statement so that it can be used in programs like Notepad or Microsoft Word.

Q: How can I download my account information?
A: From the Accounts page choose *DOWNLOAD* from the drop-down menu to the right of the account you wish to download. If you've bypassed the initial account listing screen you may select DOWNLOAD from the selection bar under the top header. Choose the appropriate account from the drop-down menu. Then select the *DOWNLOAD RANGE* (time period) for the transactions and the format. The following formats are available:

Microsoft® Money (.OFX)	Personal Finance (.QIF)
Spreadsheet (.CSV)	Word Processing (.TXT)

You will need to choose the format that matches the program you will be using with this data. Because there is such a variety of programs into which to download this data, we cannot support the download to your specific program. If you need general information regarding downloading account information, please call the bank for assistance (715-284-5341). Downloading your account information can be a great time saver with your accounting applications!

Q: **What are Alerts?**
A: The *Alert* function of Internet Banking is a great tool. It can alert you by email, text or when you log in to a variety of events. For instance—an incoming ACH Credit, if your balance falls below a set amount, if your loan or CD has matured, if a certain check has cleared, or you can set up personal reminder alerts. To set up an alert, log in and choose OPTIONS - Alerts.

Q: What is the At a Glance page?
A: The *At a Glance* page can be customized by you to give you a quick look at your Internet Banking information and activities. Select *Configure This Page* to customize the features you'd like to see. Check the box if you'd like to set this as your Start Page when you log in.

SUPPORT

Q: How do I contact the bank for support or information?
A: You may use the *CONTACT* button on the top header of Internet Banking to send a message securely. When the bank responds, you will receive a notification to your e-mail account on record that there is a secure message waiting for you on Internet Banking. You can then log into Internet Banking and go to the *CONTACT* area to pick up the secure message.

You may also contact a Personal Banker at 715-284-5341 for more information during normal business hours.

Q: What if I put in the wrong password?
A: Three invalid sign-on attempts will lock you out of Internet Banking. For security purposes, an e-mail will then be sent to the e-mail account on record to notify you that you have been locked out.

Q: What do I do if I forget my password or I'm locked out?
A: If you have previously set up a self-reset question and answer within Internet Banking, you may click on the link "Forget your password?" in the login section. You will then be guided through a process that will enable you to establish a new password. **Note:** It is important to complete the Password Reset Question and Password Reset Answer *before* you get locked out if you intend to use the self-reset option. To do so, log in to Internet Banking and click on Options. You may enter the information under the Personal tab.
You may also call us for help in resetting your password during regular business hours. Please call 715-284-5341 for personal assistance.

Q: Which browser can I use?
A: We recommend the most current version of supported browser for security purposes, however we support the current and prior major releases of Internet Explorer, Firefox, Safari and Chrome. You must have the 128-bit high encryption software component (which is included in the newer versions).

Q: Are there times when I will not be able to log on to Internet Banking?
A: Scheduled system maintenance down times are necessary to keep our system constantly improving, reliable and safe. Down times are usually scheduled during low usage periods, such as late night or early morning. The maintenance down times are listed on the Internet Banking Support page, and an alert message will usually be posted on the Internet Banking log in screen two days before the down time. *(Briefly, in the evening during daily bank processing—about 9 pm—the transfer function may not be utilized until the processing is completed. However, all other inquiry functions are unaffected.)*

FTC Phishing Warning

Federal Trade Commission Bureau of Consumer Protection Office of Consumer & Business Education

Phishing is when a scammer uses fraudulent emails or texts, or copycat websites to get you to share valuable personal information – such as account numbers, Social Security numbers, or your login IDs and passwords. Scammers use your information to steal your money or your identity or both.

Scammers also use phishing emails to get access to your computer or network then they install programs like ransomware that can lock you out of important files on your computer.

Phishing scammers lure their targets into a false sense of security by spoofing the familiar, trusted logos of established, legitimate companies. Or they pretend to be a friend or family member.

Phishing scammers make it seem like they need your information or someone else's, quickly – or something bad will happen. They might say your account will be frozen, you'll fail to get a tax refund, your boss will get mad, even that a family member will be hurt or you could be arrested. They tell lies to get to you to give them information.

Be cautious about opening attachments or clicking on links in emails. Even your friend or family members' accounts could be hacked. Files and links can contain malware that can weaken your computer's security.

Do your own typing. If a company or organization you know sends you a link or phone number, don't click. Use your favorite search engine to look up the website or phone number yourself. Even though a link or phone number in an email may look like the real deal, scammers can hide the true destination.

Make the call if you're not sure. Do not respond to any emails that request personal or financial information. Phishers use pressure tactics and prey on fear. If you think a company, friend or family member really does need personal information from you, pick up the phone and call them yourself using the number on their website or in your address book, not the one in the email.

Turn on two-factor authentication. For accounts that support it, two-factor authentication requires both your password and an additional piece of information to log in to your account. The second piece could be a code sent to your phone, or a random number generated by an app or a token. This protects your account even if your password is compromised.

As an extra precaution, you may want to choose more than one type of second authentication (e.g. a PIN) in case your primary method (such as a phone) is unavailable.

Back up your files to an external hard drive or cloud storage. Back up your files regularly to protect yourself against viruses or a ransomware attack.

Keep your security up to date. Use security software you trust, and make sure you set it to update automatically.

Report phishing emails and texts.

- Forward phishing emails to spam@uce.gov – and to the organization impersonated in the email. Your report is most effective when you include the full email header, but most email programs hide this information. To ensure the header is included, search the name of your email service with "full email header" into your favorite search engine.
- File a report with the Federal Trade Commission at FTC.gov/complaint.
- Visit Identitytheft.gov. Victims of phishing could become victims of identity theft; there are steps you can take to minimize your risk.
- You can also report phishing email to reportphishing@apwg.org. The Anti-Phishing Working Group – which includes ISPs, security vendors, financial institutions and law enforcement agencies – uses these reports to fight phishing.

MORE HELPFUL TIPS

- **Use anti-virus software and a firewall, and an operating system patches, and keep them up to date.** Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge.

Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for an anti-virus software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically. Many come with a firewall feature that should be enabled.

Be sure your patches on your operating system (Windows, Mac, etc.) are set to run on a regular basis. Unpatched devices are an attacker's favorite target. Also keep your browser and any other programs on your device up to date with the latest security patches..

- **Don't email personal or financial information.** Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.

- **Review credit card and bank account statements as soon as you receive them** to check for unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances. Regularly checking your account information online is a great way to quickly detect fraud.

- **Be cautious about opening any attachment or downloading any files from emails** you receive—regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security.

- **If you believe you've been scammed, file your complaint at ftc.gov**, and then visit the FTC's Identity Theft website at www.consumer.gov/idtheft. Victims of phishing can become victims of identity theft. While you can't entirely control whether you will become a victim of identity theft, you can take some steps to minimize your risk. If an identity thief is opening credit accounts in your name, these new accounts are likely to show up on your credit report. You may catch an incident early if you order a free copy of your credit report periodically from any of the three major credit bureaus. For details on ordering a free annual credit report see: www.annualcreditreport.com.

You can learn other ways to avoid email scams and deal with deal with deceptive spam at ftc.gov/spam.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them.

FEDERAL TRADE COMMISSION
ftc.gov 1-877-FTC-HELP

(11/2017)