Notify JCB immediately *if you believe an unauthorized electronic funds transaction has been made or someone has accessed your Internet Banking without your permission.*

YOUR PROTECTIONS UNDER REG E

LIABILITY OF CONSUMERS FOR UNAUTHORIZED TRANSFERS.

Customer Liability. Tell us at once if you believe your Password has been lost, stolen or otherwise becomes available to an unauthorized person. Telephoning is the best way of keeping your possible losses down. You could lose all the money in your accounts (plus your maximum overdraft line of credit). If you tell us within two business days after you learn of the loss or theft of your Password, you can lose no more than $50 if someone used your Password without your permission. If you do NOT tell us within two business days after you learn of the loss or theft of your Password, and we can prove that we could have stopped someone from using your Password without your permission if you had told us, you could lose as much as $500.

Also, if your statement shows transfers that you did not make, tell us at once. If you do not tell us within 60 days of the date we deliver a periodic statement to you, you may not get any money you lost after the 60 days if we show that we could have stopped someone from taking the money if you would have told us in time. If a good reason (such as a long trip or a hospital stay) kept you from telling us, we will extend the time periods.

Contact in Event of Unauthorized Transfer. If you believe your Password has been lost or stolen or that someone has transferred or may transfer money from your account without your permission, call 715-284-5341, or write Jackson County Bank, P.O. Box 490, Black River Falls, WI 54615.

Business Days. Our business days are Monday through Friday, except the Federal holidays on which the Bank closes. We can process an Internet Banking Internal Funds Transfer (including loan payments) on the same business day as your instructions, if we receive your instructions before our Internet Banking cut-off hour of 9:00 p.m. on a business day. If we receive your instructions after 9:00 p.m., we will process the transaction on our next business day. If you schedule an Internal Funds Transfer for a future date, we process the transaction after the close of business on that date, if that day is a business day. If the date you request for a future transfer is not a business day, we process the transaction on our next business day. If you schedule a recurring Internet Banking Internal Funds Transfer and the transfer date does not exist in a month, the transfer will be processed on the last business day of that month.

LEARN MORE

As an online user, understanding the current threats and knowing how fraudsters may steal your information is critical. Visit our website at jacksoncountybank.com for fraud and identity theft information.

You can also visit the following sites for more information regarding online safety and security.

www.ftc.gov
Federal Trade Commission

www.staysafeonline.org
National Cyber Security Alliance

www.ftc.gov/idtheft
FTC Identity Theft Site

www.antiphishing.org
Anti-Phishing Working Group

www.nacha.org/for-consumers
NACHA, The Electronic Payments Association

Disposing of Your Online Device

When disposing of your device—whether donating it, giving it to someone, reselling it, or throwing it out—be sure to wipe all the information on it. Most mobile devices now have a reset feature that wipes all the data from the device. Also remove the SIM and any flash cards from the device. The best way to ensure the data on a computer is destroyed is to remove the hard drive and physically destroy it.

QUESTIONS?

Contact us at 715-284-5341 or
Click on **Contact Us** at jacksoncountybank.com

Rev. 2/2017

Internet Banking and Mobile Banking for Consumers

STAY SAFE ONLINE

jcbank

Provided by

JACKSON COUNTY BANK

Black River Falls, Alma Center, Hixton, Merrillan, Taylor
jacksoncountybank.com 715-284-5341

MEMBER FDIC

Internet Banking and **Mobile Banking** provide you the opportunity to be on the go and keep in touch with your finances. However with their use comes additional risks. Because user awareness is a key defense against fraud and identity theft, we are providing sound security practices for your protection regarding online and mobile banking.

DEFENDING AGAINST THE RISKS

As technology becomes increasingly important in our daily lives, malicious cyber scams and attacks are accelerating in number and complexity. Keeping up with the best security practices is a challenge.

We realize that security is of great importance to you, and it has always been a priority at Jackson County Bank. That's why we have extremely high criteria to protect your banking information online, and we assess new risks so we can apply layered methods of protection.

As an online banking user, you should also use strong security practices and be alert to fraud and malware. Following are guidelines to guide you to **STAY SAFE ONLINE**.

JACKSON COUNTY BANK jcbank
Member FDIC

☐ **Update your device, software and apps.** Cyber attackers can more easily exploit your devices if you are running outdated software. Be sure to automate updates for your operating system, apps, security software, and other third-party software. Protect all devices that connect to the Internet including smart phones, tablets, gaming systems, and other web-enabled devices. If your device is old and no longer supported, consider upgrading to a new one that can run the latest version of the operating system and security updates.

☐ **Protect all of your devices with hard to guess passwords.** Unless it is protected, anyone can access all of your information if your device is lost or stolen. If your device supports encryption, use it. Set your device to auto-lock after a short period of time.

☐ **Open e-mail and messages cautiously.** E-mail attachments and links are the root of most successful cyber attacks. If it looks suspicious, even if you know the source, it's best to delete. Fraudsters often capitalize on your fear or curiosity, offer you great deals, or attempt to threaten you, to get you to click and unknowingly download malware. Similar to e-mail phishing attacks, fraudsters may also attack via text, messaging, or a phone call. For example, cyber criminals can text, message or call asking you to connect to a malicious website, download an infected app or ask you for private information, such as your bank account or card number, claiming to be someone they are not.

☐ **Protect your personal information.** Your Social Security number, credit card numbers, and bank and other account numbers can be used to steal your money or open new accounts in your name. So every time you are asked for your personal information – whether in a web form, an e-mail, a text, or a phone message – think about whether you can really trust the request. In an effort to steal your information, scammers will do everything they can to appear trustworthy.

☐ **Install only apps or programs that are needed and make sure that you download them from trusted sources.** Criminals can create apps that look real, but are actually malicious programs. Check the number of downloads and reviews, check the known website for reference to the web app, and don't install apps that request excessive permissions.

☐ **Make passwords long and strong.** Combine capital and lowercase letters with numbers and symbols to create a more secure password. Use separate passwords for every account and change these passwords frequently to help thwart cyber criminals. Do not store your passwords or other sensitive information on your device where it could be lost or stolen. If you use security questions and answers as verification, select questions and answers that someone else could not find in your wallet, on a social network, or simply guess.

☐ **Be careful when using Wi-Fi.** Public Wi-Fi or public computers (Internet cafes, hotels, restaurants, etc.) should not be used for any type of banking activities. When connecting to a public network, you are exposing your device and all of your traffic to all other users on that network. It is also very simple for a fraudster to spoof the name of a reputable hotspot. Check your device settings to be sure it will not automatically connect to Wi-Fi networks without asking you, putting your device at risk. Attackers can also take advantage of Bluetooth capabilities. Just like Wi-Fi, disable Bluetooth when you are not using it.

☐ **Use two-step verification whenever possible.** Many online services offer a second way to authenticate when logging into your account. It may be a text message verification, secret questions or PIN, for example.

☐ **Adjust security settings on your computer.** When available, set the privacy and security settings on websites or applications to the highest level of security that will function appropriately. Disable features that allow user names and passwords to be saved. Be sure to log out of your banking application, and if using an Internet Banking website or other secure site, close your browser after you log off.

☐ **If you use a wireless internet connection in your home, be sure your router is current** enough to be capable of the newest security features. Configure your router with a unique password and change the default network name (SSID). Enable the firewall on the device, and position it in a place where it is least likely to leak outside your home.

☐ **When banking and shopping online, check to be sure the site is "security enabled".** Look for a lock on the browser, or web addresses with "https" or "shttp". Even if it appears to be a secure site, it's important that you know and trust who you are doing business with.

☐ **Do not allow someone else to attach to your device.** Whether it is remotely connecting over the Internet or physically using a cable, flash drive, DVD, or other device, don't allow someone to connect unless you are certain of who and why, and that the device connecting is malware free.

☐ **Click with Caution.** Links within social networking sites, online advertising, e-mails, and text messages are often the way cyber criminals compromise a device. Think before you click.

Sign up for free scam alerts from the FTC at ftc.gov/scams. Get the latest tips and advice about scams sent right to your inbox.