

Newsletter

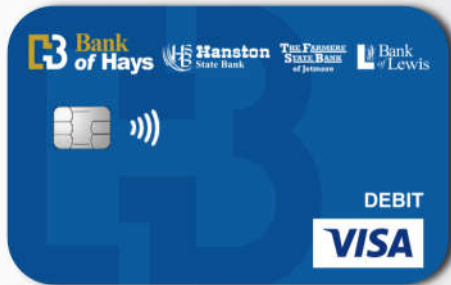
2021
Volume 25

New and exciting things coming your way...



Contactless Debit Card

Tap to pay with your Visa contactless card.



1. Look for the Contactless Symbol at checkout



2. Tap your Bank of Hays Visa contactless card on the contactless-enabled terminal



3. Once your payment is complete, you're good to go!

Your Bank of Hays Visa contactless card has the same dynamic security as a chip card, so it's also a secure way to pay!

Use your Bank of Hays Visa contactless card where you see the Contactless Symbol. 

...and Bank of Hays Mobile Wallet Pay!



You will be able to add your Bank of Hays debit card to your mobile wallet. A mobile wallet lets you easily make online or in-store purchases right from your smartphone, tablet or smartwatch. Enjoy peace of mind by making convenient and secure purchases from your mobile device.

Mobile Wallet Benefits

- Make fast, in-store purchases by holding your device to a contactless terminal
- Shop and check out without the need of entering your card information
- Enjoy enhanced security with the use of your phone's security controls

Start making purchases with just a tap of your mobile device. Learn how on your Apple Pay, Samsung Pay, or Google Pay mobile wallet.



What to Do if You're a Victim of Unemployment Fraud

If you discover that a bogus unemployment claim has been filed in your name, do the following immediately:

1. Notify your local unemployment agency. If the fraud comes to light as you apply for unemployment, the agency will already be notified. If your employer notifies you of a bogus claim, enlist your human resources department to assist with pursuing the false claim—but make sure you also notify the unemployment agency yourself.
2. Inform the IRS by filing an Identity Theft Affidavit (IRS Form 14039) [with the IRS](#) or through the Federal Trade Commission's identity theft website, [IdentityTheft.gov](#), where you can also find information on cleaning up the damage identity theft can cause.
3. If you suspect unemployment fraud is connected to email or bogus websites or social media accounts, file a report at the [FBI Internet Crime Complaint Center](#).
4. Get your free credit report right away at: [annualcreditreport.com](#) or call 1-877-322-8228
5. Call your bank and have them place an alert on your accounts.

Three Ways to Avoid COVID-19 Vaccine Scams

While vaccination details are getting worked out, here's what you can be sure of:

- You can't pay to put your name on a list to get the vaccine. **That's a scam.**
- You can't pay to get early access to the vaccine. **That's a scam.**
- Nobody legit will call about the vaccine and ask for your Social Security, bank account, or credit card number. **That's a scam.**

Ignore any vaccine offers that say different, or ask for personal or financial information.

Learn more at

[ftc.gov/coronavirus/scams](#)

[consumerresources.org/beware-coronavirus-scams](#)

10 Tips to Avoid Becoming a Victim

1. **Ignore offers or claims for early access to the COVID-19 vaccine.** If you get a call, text, email or even someone knocking on your door claiming they can get you early access to the vaccine — that's a scam.
2. **Watch out for phishing scams.** Phishing scams use fraudulent emails, texts, phone calls and websites to trick users into disclosing private account or login information. Do not click on links or open any attachments or pop-up screens from sources you are not familiar with, and NEVER give your password, account number or PIN to anyone.
3. **Rely on official sources for the most up-to-date information on COVID-19.** Visit the Centers for Disease Control and Prevention, World Health Organization and your state's health department websites to keep track of the latest developments.
4. **Remember that the safest place for your money is in the bank**—it's physically secure and it's federally insured. When you deposit your money at a bank, you get the comfort of knowing that your funds are secure and insured by the government. You don't have the same level of protection when your money is outside the banking system.
5. **Do some research before making a donation.** Be wary of any business, charity or individual requesting COVID-19-related payments or donations in cash, by wire transfer, gift card or through the mail.
6. **Keep your computers and mobile devices up to date.** Having the latest security software, web browser, and operating system are the best defenses against viruses, malware and other online threats. Turn on automatic updates so you receive the newest fixes as they become available.
7. **Recognize and avoid bogus website links.** Cybercriminals embed malicious links to download malware onto devices or route users to bogus websites. Hover over suspicious links to view the actual URL that you are being routed to. Fraudulent links are often disguised by simple changes in the URL. For example: [www.ABC-Bank.com](#) vs [ABC_Bank.com](#).
8. **Change your security settings to enable multi-factor authentication for accounts that support it.** Multi-factor authentication—or MFA—is a second step to verify who you are, like a text with a code.
9. Before you make any investments, **remember that there is a high potential for fraud right now.** You should be wary of any company claiming the ability to prevent, detect or cure coronavirus. For information on how to avoid investment fraud, visit the U.S. Securities and Exchange Commission website.
10. **Help others by reporting coronavirus scams.** Visit the FBI's Internet Crime Complaint Center at [www.ic3.gov](#) to report suspected or confirmed scams. You can also stay up-to-date on the latest scams by visiting the FTC's coronavirus page at [ftc.gov/coronavirus](#).

Bank of Hays
1000 W 27th St
Hays, KS 67601
Phone: (785) 621-2265
Fax: (785) 621-2471

Hanston State Bank
102 N Logan St
Hanston, KS 67849
Phone: (620) 623-4811
Fax: (620) 623-2727

Bank of Lewis
217 S Main St
Lewis, KS 67552
Phone: (620) 324-5794
Fax: (620) 324-5797

Farmers' State Bank of Jetmore
601 Main St
Jetmore, KS 67854
Phone: (620) 357-8324
Fax: (620) 357-6398