



October - December 2024



Volume 13, Issue 4



Small town, big life!

NEW YORK MILLS, MN

Member FDIC



Our Two Cents

In Case You Missed It! New Digital Banking Products!

In August, we launched our updated website and new mobile app! You can enjoy the same great online products with a whole new look. You can still utilize our Bill Pay system, mobile deposit, notification system and so much more! All login information will carry over into the new website and mobile app so there are no worries about creating new information for you to remember.



Previously you were not able to enroll a new login

credential via the mobile app and we are happy to announce that option is now available! Business customers should contact us to help with registration for digital banking going forward.



Be sure to download our new app! Search for FMBANK NEW YORK MILLS.



We hope all our customers enjoy the new look and if you have any questions, please don't hesitate to contact us!

Never Share Digital Wallet Information!



Using your own digital wallets (Google Wallet, Apple Wallet, etc) is a great way to securely pay for goods and services! However, recently, we have gotten reports of customers who have shared their debit card information with someone and that person has used it to put *OUR CUSTOMER'S* full debit and/or credit card information in *THE SCAMMER'S* digital wallet. Please be very cautious when giving out your card information! If you have doubts, call us!

Community Events for Fall & Winter 2024

October

October 5th: Pickletoberfest at the Continental Divide Brew Pub 6 pm - 9pm

October 8th: Turkey Bingo hosted by the New York Mills Education Foundation & meal put on by Bandwagon

October 26th: Kids Halloween Party at the New York Mills Cultural Center 12 pm - 3 pm

November

November 22nd: Annual Community Carnival from 4 pm - 7 pm at the school

November 27th: Annual Community Thanksgiving Meal at Trinity Lutheran Church

November 29th: Christmas Tree Festival Kick-Off from 4 pm - 7 pm at the City Hall Ballroom

December

December 3rd: Sleigh Rides in front of F&M State Bank

December 7th: Community Christmas Party starting at 6 PM at City Hall Ballroom

December 21st: Longest Night Music Festival at the Cultural Center





Letters from Latham

Wow, hard to believe we are already in the fall season! I find myself looking forward to the cooler nights, changing of the leaves, and my perennial hope that the Vikings will win a Super Bowl. We are very excited for all of our customers to explore our new website and digital banking. It's been a big project and we are very proud of how it all turned out. As always, if you have any questions, please don't hesitate to reach out to us!



The biggest topic in banking right now is interest rates. The Federal Reserve has begun the process of starting to cut rates, which in turn will lower interest rates on credit cards, mortgages, and most other types of loans. If you are thinking a refinance of your home may be the right decision for you, please give us a call and we would be happy to look it over with you.

Latham H. Hetland
Latham Hetland, Loan Officer
NMLS #2063221

In closing, I wish you all a happy end of 2024 and will surely see you all at the celebrations after the Twins win the World Series, the Vikings win the Super Bowl, and the Timberwolves win the NBA Championship this year!

Tech Tips: Tips to Help Protect You and Your Money

Scammers are constantly trying to steal your money and your personal information, and they use a variety of ways to try to trick you. Scammers often pretend to be from an organization you might know and trust (such as an FDIC-insured bank) and try to get your personal information. FDIC can help you verify whether a website is a fake bank website or the legitimate website of an FDIC-insured bank.

There are a number of ways scammers try to reach you, too. The term "phishing" is when scammers try to reach you by email or on a website. Similarly, "smishing" is when criminals use text messaging to reach you. The word "vishing" is when these scammers call you and try to trick you into providing personal information by sounding like a legitimate business or government official. Learn how to identify these scams and better protect yourself and your money.

Am I dealing with a legitimate, FDIC-insured bank?

Criminals create fake bank websites to mislead and entice people into transferring money or disclosing personal information. This scam is a form of "phishing." Some of these fake bank websites use the FDIC name or "Member FDIC" logo to instill a false sense of security. Sometimes it is hard to tell which websites are real, and which are fakes. Before engaging with any website for an entity that claims to be an FDIC-insured bank, it is important to make sure that the website is real.

Text messages from scammers

Scammers may use text messaging to reach you too, known as "smishing." They may pretend they are from your bank and try to get you to provide your personal information. The text message often looks like a bank security message. Note that these fraudulent messages often try to create a sense of urgency to make you provide your personal information faster and less carefully. Take your time and call your bank using a phone number that you are familiar with, for example, the number provided on your debit or credit card. Do not use a phone number provided by someone you are unfamiliar with or that you think may be a scammer. As an alternative, contact the FDIC before you provide any information when something does not seem right.

Email links

Just like text message scams, avoid clicking on links in unsolicited emails or emails from unfamiliar sources. Some links may download malware (malicious software, such as computer viruses) to your device when you click on them. This is another form of "phishing." The malware may steal your banking information, including your username, passwords, and credit or debit card numbers. Some links may lead to an illegitimate website attempting to get you to enter your personal information. These emails typically look very similar to ones sent by familiar sources like well-known retailers, banks, and other entities.

Be on the lookout for emails with typos, obvious mistakes, unusual fonts, that create a sense of urgency, or just seem off. In addition, be skeptical of email attachments described as coupons, rebates, or payment forms – they could include malware. Moreover, avoid email offers that seem "too good to be true." Also watch for fee-related scams. This type of scam is where the scammer requests you to send money or pay "FDIC insurance fees" to receive a large amount of money in return. As a reminder, the FDIC does not charge or collect fees from consumers.

No matter how the scammers try to reach you, following the tips highlighted in this article will help keep you and your money safe.

