

In This Issue:

- **Heart of Hope Awards Luncheon**
- **The History of Mardi Gras**
Mardi Gras - Fat Tuesday - March 5, 2019
- **Spoiler Alert!!**
- **Computer Security Tips for Bank Customers: A Basic Checklist**
- **Take Full Control of Your ATM/Debit Cards**
- **eBanking Support Group**

Heart of Hope Awards Luncheon

Save the Date!

The 2019 Heart of Hope event will take place on Friday, May 17, 2019 from 11:00am - 1:00pm at the Red Rock Casino Resort in Summerlin.

Tickets and sponsorships support Catholic Charities efforts in transforming lives and making a lasting impact in the lives of those most vulnerable in our community. Tickets may be purchased at CatholicCharities.com or by calling 702.387.2275

The History of Mardi Gras

Mardi Gras - Fat Tuesday - March 5, 2019

In cities around the world, and particularly in New Orleans, Mardi Gras fills the late days of winter with colorful revelry. If you've ever wondered how this annual tradition got its start, here's a look at the roots of the holiday and how it developed in the United States.

What is Mardi Gras?

Mardi Gras is French for "Fat Tuesday," which is the final day before the Christian season of Lent. Fat Tuesday is the culmination of the longer Carnival season that begins in January. It's traditionally been viewed as one last chance to party and feast on rich foods before Ash Wednesday kicks off Lent's 40 days of fasting and reflection. While Mardi Gras retains its religious significance for millions of Christians, many other people celebrate it independently of a spiritual tradition.



When did Mardi Gras begin?

Mardi Gras and the broader Carnival season date from the early days of the Christian church, but Mardi Gras historian Arthur Hardy writes on his website that the celebration may have originated in ancient pagan fertility rituals. These rituals were eventually co-opted by the church as a way to more effectively attract and retain new converts.

When did Mardi Gras come to the U.S.?

Versions of Mardi Gras and Carnival are celebrated around the world. Mardi Gras was first observed on American soil in 1699 by the French explorer Pierre Le Moyne d'Iberville. Hardy writes in the *New Orleans Advocate* that d'Iberville and his team marked the occasion at a site near the mouth of the Mississippi River in what is now Louisiana — even christening the spot Pointe du Mardi Gras.

While most people think of New Orleans when they think of Mardi Gras, the first city to mark the holiday was Mobile, Alabama. According to CNN, Mobile held a Mardi Gras celebration in 1703, the year after the city's founding.

Residents of the surrounding region, including New Orleans, put on masked balls and threw big parties to celebrate Mardi Gras in the years that followed. But in 1766, Spain took over and banned these celebrations. Masked Mardi Gras balls weren't allowed again in New Orleans until 1823, well after Louisiana had become a state.

How did Mardi Gras take root in New Orleans?

According to AL.com, Mobile held its first Mardi Gras parade in 1830, organized by the Cowbellion social club, or "krewes." By 1837, the practice had spread to New Orleans. Authorities and the press frowned upon these frequently rowdy events.

In 1857, Hardy writes, a small group of New Orleans residents formed the Comus krewe and turned Mardi Gras into a more formal and broadly acceptable event permanently associated with the city. Their club organized a Mardi Gras parade, built mythologically themed floats, dressed in masks and elaborate costumes and held a celebratory ball.

In 1875, Mardi Gras became an official Louisiana state holiday. Over the final quarter of the 19th century and the early years of the 20th century, New Orleans' celebration exploded in popularity, filling the weeks before Fat Tuesday with parades, music, balls and parties. More and more krewes

formed, contributing their own costumes and themed parade floats to the excitement. During these years, many of the most iconic Mardi Gras traditions appeared, including the annual election of Rex, the king of the carnival.

Modern Mardi Gras celebrations draw millions of people every year to the streets of New Orleans and other cities. Although the holiday's image is often one of excess and indulgence, it's also a celebration of good times, warm feelings and strengthened community ties.

Meadows Bank • 702-471-2004 • <https://www.meadowsbank.bank/>

Meadows Bank eNewsletter

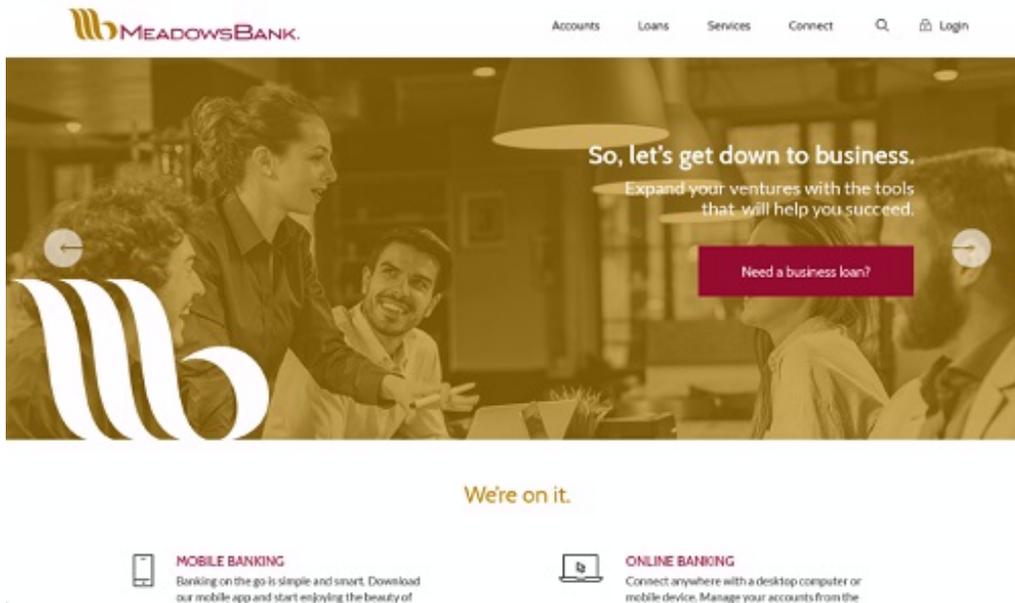
Spoiler Alert!!

We are excited to announce a new Meadows Bank website is getting ready to launch. In the upcoming weeks, you will notice a fresh, easier to use meadowbank.bank

The new website will boast a clean design with simple navigation making it easier than ever to find the information you need. It will be fully responsive with mobile devices, offering a more consistent experience whether you visit the website from your desktop, smartphone or tablet. You will still be able to get to online banking directly from the top right of the home page.

We're excited and we know you will be as well. Feel free to let us know what you think when it goes live by sending us an email at jehall@meadowbank.com.

Here is just a little preview of what the new site will look like!



New Website Homepage

Meadows Bank • 702-471-2004 • <https://www.meadowsbank.bank/>

Computer Security Tips for Bank Customers: A Basic Checklist

The following article was published by the Federal Deposit Insurance Corporation (FDIC) in the Spring 2015 issue of FDIC Consumer News. It can be accessed at <https://www.fdic.gov/consumers/consumer/news/cnspr15/computersecurity.html>

Computer Security Tips for Bank Customers: A Basic Checklist

Computer-related crimes affecting businesses or consumers are frequently in the news. While federally insured financial institutions are required to have vigorous information security programs to safeguard financial data, consumers also need to know how to protect and maintain their computer systems so they can steer clear of fraudsters. Here is a short checklist.

1. Protect your computer. Install anti-virus software that scans your computer for malicious software ("malware") that can steal login IDs, passwords and account information (including credit or debit card numbers). Also use a firewall program to guard against unauthorized access to your computer. "Anti-virus protection and firewall options vary, and some are free," said Michael Benardo, Manager of the FDIC's Cyber Fraud and Financial Crimes Section. "Choose one, install it, and then set the software to update automatically."

2. Safeguard your smartphone, tablet and similar mobile devices, especially when using them for banking or shopping. Reduce your risk of downloading "apps" (applications) that contain malware by using well-known app stores, such as those established by your phone manufacturer or cellular service provider, or from the official Web site of the bank.

Also, to ensure that you have the latest fixes to software problems affecting mobile devices, opt for automatic updates for your operating system and apps or manually download updates as soon as you receive notice that they are available. You can also purchase anti-malware software from a reputable vendor.

Do not leave your mobile device unattended. In case your device does get lost or stolen, use a password or other security feature to restrict access. You should enable the "time-out" or "auto-lock" feature on your mobile device to secure it when it's not used for a period of time. "Some phones have a remote feature that will allow you to erase all the personal information on your phone or disable it in the event that your phone is lost or stolen," said Jeff Kopchik, a Senior Policy Analyst with the FDIC.

3. Understand your Internet safety features. When you are buying something online or filling out an application that contains sensitive personal information, you can have greater confidence in a Web site that encrypts or scrambles the information as it travels to and from your computer. Look for a padlock symbol on the page and a Web address that starts with "https://." The "s" stands for "secure."

4. Be careful where and how you connect to the Internet. A public computer, such as at an Internet café or hotel business center, may not have up-to-date security software and could be infected with malware. Also, for online banking or shopping, avoid connecting your computer, tablet or smartphone to a wireless network at a public "hotspot" (such as a coffee shop, hotel or airport).

5. Be suspicious of unsolicited e-mails and text messages asking you to click on a link or download an attachment. It's easy for fraudsters to copy corporate or government logos into fake e-mails that can install malware on your computer.

"Your best bet is to ignore any unsolicited request for immediate action or personal information, no matter how genuine it looks," Benardo said. "If you decide to validate the request by contacting the party that it is supposedly from, use a phone number or e-mail address that you have used before or otherwise know to be correct. Don't rely on the one provided in the e-mail."

6. Use "strong" IDs and passwords and keep them secret. Choose combinations of upper- and lower-case letters, numbers and symbols that are hard for a hacker to guess. Don't, for example, use your birthdate or address. Also don't use the same password for different accounts because a criminal who obtains one password can log in to other accounts. Finally, make sure to change your passwords on a regular basis.

7. Take precautions on social networking sites. Criminals can go there to gather details such as someone's date or place of birth, mother's maiden name or favorite pet and use that information to figure out and reset passwords. Fraudsters also may pretend to be your "friend" to persuade you to send money or divulge personal information.

For more tips on computer and Internet security for bank customers, including how to protect yourself from data breaches, see back issues of FDIC Consumer News. Also watch the FDIC's multimedia presentation Don't Be an Online Victim

Also visit OnGuardOnline.gov for a variety of information from the federal government on how to be safe online. The site includes new videos from the Federal Trade Commission on what to do if your e-mail is hacked or malware attacks your computer.

Additional tips are published on our website - Protect Yourself

Meadows Bank • 702-471-2004 • <https://www.meadowsbank.bank/>

Take Full Control of Your ATM/Debit Cards

MyCard Rules is an easy-to-use mobile app that lets you set card controls, add restrictions and receive transaction alerts ¹ on all your Meadows Bank ATM/Debit cards.

Just download the MyCardRules app from Google Play™ or the App Store®. Then you can set a wide range of controls and alerts on all your cards. For example, you can:

- Turn your card on and off.
- Set transaction spending limits based on your preferences, including dollar amount, transaction type and merchant type.
- Get instant alerts on certain types of transactions, like when a transaction is declined.
- Set a specific region where the card can be used or restrict usage based on your mobile device's location.
- Set parental controls and monitoring.

Alerts will show up just like any other notifications you get on your mobile device.

Knowing that you've set rules, restrictions and alerts that meet your specific spending preferences adds another layer of fraud detection and prevention, and gives you added peace of mind. You have complete control of how, when, where – and WHO uses your cards.

For more information, please contact us at hereforyou@meadowsbank.com or at 702.471.2233.

¹ Message and data rates may apply. Please contact your wireless provider for more details.

eBanking Support Group

Question about Online Banking - we've got you covered! Need help with Mobile Banking or your ATM card - we are here for you!

Our eBanking Support Team can be reached at:

- hereforyou@meadowsbank.com
- 702.471.2233 (New Support Phone Number)

Using the above email and/or phone number will get you directly to the entire eBanking Support Team, so the first available team member is able to assist you. You won't have to go through the main line and get transferred, and/or reach voicemail.

