October 2024

The Messenger

120 E. FIRST/PO BOX 48, KIMBALL, SD 57355-0048
605.778.6221 WWW.MIDSTATESD.NET

CALENDAR

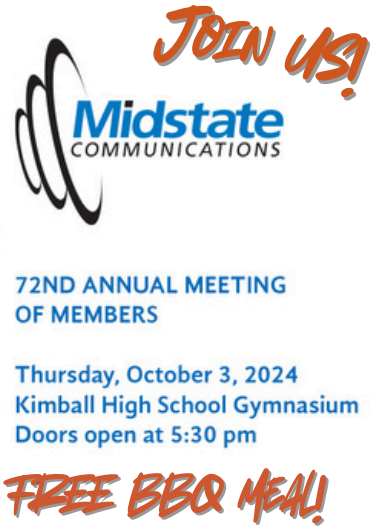
October 3
72nd Annual Meeting
Doors Open at 5:30 pm

October 5
Disconnect of all accounts with a 30 day balance.

October 14
Native American Day
Offices Closed

October 20
Bills due by 12:00 PM
Overdue notices mailed out

October 31
November bills are mailed out and due November 20th.



Attention Midstate Communications Cooperative members! You're invited to join us for the 72nd Annual Meeting on Thursday, October 3rd, 2024, at the Kimball High School. Doors open at 5:30 PM for registration and a complimentary customer appreciation meal. The short business meeting will start at 6:30 PM, followed by Bingo and exciting door prize drawings. We look forward to seeing you there!

#FallVibes

Midstate's Float Takes Top Spot!

The Midstate crew sizzled in this year's Kimball homecoming parade, frying up 1st place honors and bragging rights with our "WildKats Are Bringing Home the Bacon" float. Plant Manager Lantz Brennan cooked up the breakfast treat while CEO/GM Chad Mutziger and Cheri Eimers from Customer Service dressed up as bacon slices. If you didn't see our "bacon" float, you may have seen staff drive thru other area parades of Stickney, White Lake and Platte during the month of September tossing candy to all attendees. We enjoy being out in the area!

Top Tips to Protect Your Digital Footprint

October is National Cybersecurity Awareness Month, a great time to focus on keeping your devices and data safe. At Midstate Communications, we deliver fast, reliable internet and prioritize your security. Our best efforts are only most effective when you take necessary precautions to ensure your online security and protect your privacy, too.

We've compiled some of the best cybersecurity measures from experts worldwide to help you stay safer online. Hackers and other security breaches have compromised numerous online accounts in recent years.

Here are four essential tips for protecting your digital footprint:

Create Strong Passwords: It really is time to stop using your initials and birthday as your password. Use at least 8 characters with a mix of letters, numbers, and symbols. The longer the password the harder it is to crack. Also, stop re-using the same passwords on different accounts. Each password should be as unique as your own fingerprint is!

Use a Password Manager: Do you recall what you had for dinner last night? Me neither! No one can remember all of the passwords they need to use these days. A Password Manager is your next step toward improving your online security. You have one key to unlock your house to gain access to all your rooms, right? A password manager also uses a "master password" for you to easily gain access to all your accounts reducing the frustration of needing to remember multiple passwords for all your online accounts.

Keep Software Updated: When was the last time you restarted your computer? Can't remember? Then it has been too long! Many system updates occur when your computer or device is restarted. Ensure your devices are running the latest software to stay protected from security breaches.

Watch for Phishing Scams: Did you know your personal information is enticing to companies? Phishing is different from ordinary hacking because scammers attempt to lure you into providing your personal information directly to them. Signs of phishing scams include:

- Emails or text messages indicating "unusual activity" on your account and then asking you to click on a link and follow the instructions—do NOT click on any such link!
- Messages with a lack of any greeting, or only using portions of your email address, or using "Sir/Madam" instead of your name, or containing an incorrect spelling of your name.
- The email address domain name is misspelled or does not match the company or governmental entity it claims to be.
- Urgent time limitations to "act now" are included in the message, often provoking you to respond within one day or even a matter of hours, which attempts to make you "click" without thinking carefully about whether it is a legitimate issue.

Be cautious of suspicious emails or texts. If you have questions about an email you have received, call Midstate to talk with the IT team. We are here to answer your questions! For more Cybersecurity tips in October, follow us on Facebook.