A NEWSLETTER FROM YOUR FRIENDS AT USA COMMUNICATIONS

In Touch

SEPTEMBER 2025

Fall in Love With Fall

There's so much to love about the fall season. Spending a chilly evening around your firepit. Wearing your favorite cozy sweaters. Watching movies snuggled under a blanket. Enjoying a pumpkin spice latte (or pumpkin-flavored anything). Cheering on your team at the local football field. Whatever fall activities speak to you, we hope you make the most of them in the months ahead.

USA Communications
PO Box 389, Shellsburg, IA 52332

Office Locations:
Shellsburg: 124 Main Street
Blairstown: 312 Locust Street
319-436-2224 or 1-800-248-8007
usacomm.coop

Hours: M–F 8:00 am to 4:30 pm

Closure: September 1st for Labor Day, November 26th & 27th in observance of Thanksgiving

Find Us on Facebook
Search USA Communications

USA Communications
Connecting Your Community to the Future.

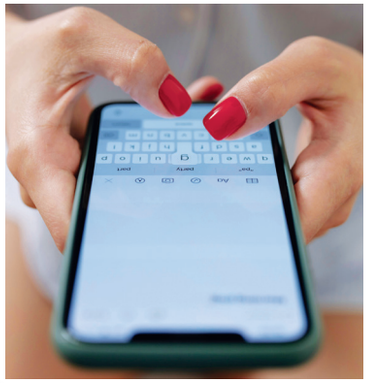
Please Watch Out for Imposter Scams

According to the FTC, imposter scams — where criminals pretend to be from a government agency or well-known company — have increased dramatically in recent years. For example, someone might call you or send an email or text to say:

- They're from Microsoft or Apple and need to inform you of a problem on your computer.
- You owe money to the IRS or another government agency.
- Your Social Security account was suspended or your Social Security number was linked to a crime.
- You just won a prize but you have to pay fees to redeem it.
- Your credit card has been charged a large amount for an Amazon.com order and you need to call "Amazon Support" if you didn't make that purchase.

If you receive messages like these, hang up the phone or ignore the email or text.

Be sure to follow USA Communications on Facebook. We regularly post about scams to help keep you from becoming a victim.



Don't BelieveThese Cybersecurity Myths

There are lots of myths about cybersecurity. Let's debunk a few common ones.

Myth: I have a strong password, so I don't need to worry.

It's great if you have a long and strong password with a blend of letters, numbers, and special characters. However, you need more than one. Every account and device should have its own password — don't use the same one in multiple places, regardless of how strong it is. If you reuse passwords, it means that if one of your accounts is hacked, all of your other accounts are at risk. It's also recommended that you enable MFA (multi-factor authentication) for every account, which doubles up your protection beyond your password. The few seconds required to enter a code sent to your phone is well worth the added security.

Myth: Password managers aren't safe because they could get hacked.

Sometimes people express concerns about storing all their passwords in one place. However, high-quality password managers are the safest way to store your passwords. These programs also ensure that you're using strong, unique passwords for each of your accounts. Because of the technology password managers use, the password manager company doesn't even know your master password. When you enable MFA on your password manager, it becomes even more secure. There have been incidents when password manager companies get hacked. However, when you use a strong master password and MFA, you can maintain your security even in these situations. This is why password managers are safer than notebooks, sticky notes, or documents saved on your computer.

Myth: Phishing emails will always be obvious. I'll know them when I see them.

This myth may have been true at one time, but that's no longer the case. Due to the widespread use of AI, both grammar and spelling in phishing emails have improved significantly in recent years, making them harder to spot. Some scam messages can appear almost identical to messages from trusted sources. What you need to look for now is a sense of urgency. Is the message unexpected? Is it trying to get you to act quickly without thinking?