The Communicator

News from your local coop to keep you connected. November 2023

Do you have family visiting for Thanksgiving? Make sure your network is prepared for the extra devices and usage! We have higher speed packages available to get you and your guests the best connection.

Make Secure Payments Online with SmartHub

Your life is busy and managing your account can sometimes feel complicated. With our SmartHub tool it won't be. Save time and money by managing your account at anytime from anywhere. Here are some of the ways SmartHub will put you in control of your account:

Billing & Payments: No more waiting for your bill to arrive in the mail! Access and pay your bill at anytime from anywhere. Save time with easy payment options to avoid late fees and service interruptions.

Alerts & Notifications: Stay informed on important account events via email or text messages.

Paperless Billing: What if you could save some time and a tree at the same time? Activate SmartHub paperless billing, an eco-friendly way to instantly access your bill.

You can download the SmartHub app for free right from the Apple App Store or Google Play Store. You can also access SmartHub from our website at www.yourlocal.coop/smarthub. If you need any assistance getting this set up, please give us a call!

Office Closed

Our office will be closed Thursday, November 23 and Friday, November 24 for Thanksgiving. If you have any service outages, please call 498-3456 to reach our on-call technician or to leave a message for the following Monday.

ProtectIQ

Keep your home network and devices safe with ProtectIQ! For only $6 month, **all devices** in your home are protected from threats, intrusions, viruses and malware. ProtectIQ has saved our customers from thousands of monthly threats!

In the past 2 months

We've protected our customers from over

2,082

Web threats, Intrusions, Viruses and Malware

ProtectIQ®

What is phishing?

Phishing is a type of social engineering attack where criminals attempt to trick people into revealing sensitive information, such as passwords, credit card numbers, or other personal information. This information can then be used to steal money, commit identity theft, or other crimes.

Scammers are after a variety of things when they phish, but they are usually after financial account details, passwords, or sensitive data. Financial account details are valuable to scammers because they can be used to steal money from people's accounts. Passwords are valuable because they can be used to access people's online accounts, such as email, social media, and banking accounts. Sensitive data, such as Social Security numbers, can be used to commit identity theft.

Scammers use a variety of methods to phish people, but they often use email, social media, and text messages. They may send emails that look like they are from legitimate companies, such as banks or credit card companies. They may also post fake ads on social media or send text messages that look like they are from legitimate businesses.

Protecting yourself from phishing methods

It is important to be aware of phishing scams and to take steps to protect yourself. Here are some tips to help you avoid phishing scams:

- Be suspicious of any email, social media post, or text message that asks for personal information.
- Do not click on links in emails or text messages unless you are sure they are legitimate.
- Do not enter personal information on websites that you do not trust.
- Use strong passwords and change them regularly.
- Be aware of the latest phishing scams and how to protect yourself from them.
- If you think you have been the victim of a phishing scam, you should immediately change your passwords and contact your bank or credit card company. You should also report the scam to the Federal Trade Commission (FTC).

What can I do to stay safe?

- **Avoid clicking suspicious links.** Phishing attacks often use deceptive links or attachments to trick you into downloading malware or revealing personal information. If a message looks suspicious or is from an unknown sender, refrain from clicking any links or opening attachments.
- **Use official websites.** Only log in to your accounts through official websites. Be cautious of redirects to unfamiliar sites.
- **Verify email addresses**. Watch out for spoofed email addresses that mimic legitimate companies. Hover over the sender's email address to confirm its authenticity when dealing with emails from businesses you trust.
- **Take advantage of Spring Grove Communication's security tools.** We offer ProtectIQ and TechShield to help protect you and all your devices online.