



A Touchstone Energy® Cooperative 

1511 14,000 Road, P.O. Box 368, Altamont, KS 67330
866-784-5500
www.twinvalleyelectric.coop

TWIN VALLEY ELECTRIC CO-OP

NEWS

TWIN VALLEY ELECTRIC COOPERATIVE, INC.

BOARD OF DIRECTORS

Bryan Coover
President

Jason Zwahlen
Vice President

Bryan Hucke
Secretary

Heath Steeby
Treasurer

J J Bebb
Director

Zach Foster
Director

Jason Martin
Director

Diane McCartney
Director

Adam Smith
Director

STAFF

Angie Erickson
CEO

OFFICE HOURS

Monday-Friday
8 a.m. to 4:30 p.m.

CONTACT US

1511 14,000 Road
P.O. Box 368
Altamont, KS 67330
866-784-5500
www.twinvalleyelectric.coop

FROM THE CEO

This Fall, Refresh Your Cybersecurity Habits



As the leaves begin to change and we settle into the routines of fall, it's a good time to take stock of a few things around the house — preparing for cooler weather, checking our heating systems and getting ready for the months ahead. It's also a good time to refresh our cybersecurity habits.

October is National Cybersecurity Awareness Month, but protecting your personal information is something that deserves attention all year long.

At Twin Valley, cybersecurity is a critical part of providing safe, reliable electric service. While much of our focus is on protecting the physical systems that operate the electric grid, we also work to protect the systems and information that help us serve

you — including online accounts, payment systems, member portals and outage communications.

Unfortunately, scammers are becoming more sophisticated, too. Artificial intelligence (AI) is making it easier for cyber criminals to create convincing emails, text messages, websites and even voice messages that can look and sound legitimate. The FBI has warned that generative AI can make fraudulent schemes more believable by eliminating many of the errors that once helped us identify a scam.

That matters when it comes to utility scams.



Angie Erickson

Continued on page 12B ►

ENERGY EFFICIENCY TIP OF THE MONTH

Don't let phantom energy haunt your electric bill this October. TVs, gaming systems, coffee makers and phone chargers continue using electricity even when they're turned off. While each device uses only a small amount, the energy waste can add up over time. Before heading out for Halloween fun, unplug devices you don't use regularly or plug them into a smart power strip that automatically cuts power when equipment is off to keep phantom energy waste in check. SOURCE: U.S. DEPARTMENT OF ENERGY



SAVE ENERGY THIS

*Fall and
Winter*

FOLLOW THESE SIMPLE TIPS TO REDUCE ENERGY USE AND KEEP YOU WARM THIS SEASON:

- ▶ Seal gaps around windows and doors with caulk or weatherstripping.
- ▶ Close curtains and blinds at night to keep the cold out.
- ▶ Open window coverings on sunny days to let the sun in.
- ▶ Clean or replace furnace filters.
- ▶ Run ceiling fans clockwise to push warm air down.
- ▶ Check insulation in your attic, attic hatch and crawl space.
- ▶ Use a smart thermostat to lower temperatures when asleep or away.
- ▶ Close the fireplace flue when not in use.
- ▶ Schedule a home energy audit to find and fix energy wasters.



SOURCE: WWW.SAFEELECTRICITY.ORG

This Fall, Refresh Your Cybersecurity Habits

Continued from page 12A ▶

A scammer may impersonate Twin Valley and claim your account is past due, your service is about to be disconnected or you need to make an immediate payment. The message might even include our logo, use professional-looking language or direct you to a website that appears legitimate. With AI helping scammers create more convincing communications, simply looking for spelling mistakes or other obvious warning signs may no longer be enough. And these scams are not a small problem.

According to the Federal Trade Commission, consumers reported losing \$3.5 billion to imposter scams in 2025, making these types of scams the most commonly reported type of fraud. Nearly one in three fraud reports involved an imposter scam.

So, what should you do if you receive an unexpected message claiming to be from Twin Valley?

If a message creates a sense of urgency or threatens immediate disconnection, take a moment to verify it. Don't click the link or call the phone number provided in the message. Instead, contact Twin Valley directly using our trusted methods. You can reach us by phone at 620-784-

5500 or by email at memberservices@twinvalleyelectric.com.

You can also take steps to protect your online accounts before a scam occurs. Start with your password. Longer is generally better than simply adding more special characters. Choose a long, unique passphrase that is difficult for others to guess, and don't reuse the same password across multiple accounts.

If the accounts you access online offer multifactor authentication (MFA), consider using it. MFA adds an extra layer of protection by requiring an additional way to verify your identity, such as a code sent to your phone or an authentication app.

Most importantly, remember that you don't have to make a payment simply because someone tells you that you do. We want you to have an opportunity to verify any unexpected request.

Twin Valley is committed to protecting the systems that help us deliver your electricity and serve our members. You can help by protecting your own account, slowing down when something seems urgent and contacting us directly when you're unsure.

For questions about your account or payment options, contact us at 620-784-5500.

OCTOBER IS CYBERSECURITY AWARENESS MONTH



Longer
passwords
= stronger
protection.



Watch
for co-op
impersonation
scams.



Think before
you click.



Use multifactor
authentication.

Protect Your Home Network During Cybersecurity Awareness Month

October is Cybersecurity Awareness Month, a good time to check the security of the technology we use every day. From phones and laptops to smart TVs, thermostats and doorbells, many household devices connect to the internet.

This connection provides convenience, but it also means your home network needs protection. Your router acts like the front door between these devices and the internet, and it's important to keep it secure.

The good news: You do not have to be a technology expert. A few simple steps can help protect your devices, accounts and your family's personal information.

START WITH YOUR ROUTER

Your router connects your phones, computers, tablets and smart devices to the internet. Taking a few minutes to review its settings can make a big difference.

CHANGE DEFAULT PASSWORDS

Change your router's default network name and password to something unique. Avoid using your name, address or phone number in your Wi-Fi network name.

Change the password used to access your router's settings. It's different than your Wi-Fi password. Use long, unique passwords, and consider a password manager to help create and store them.

USE THE SAFEST WI-FI SECURITY SETTING AVAILABLE

Your Wi-Fi security settings help protect information moving between your devices and your router and help keep people nearby from joining your network without permission.

In your router's settings or app, look for the Wi-Fi security option. Choose WPA3 if it is available. If not, choose WPA2. Avoid WEP or WPA, which are outdated and easier to break into.

If you are unsure how to find this setting, check your router app, look for instructions from your internet provider, or search the router model number with "change Wi-Fi security settings" on your internet browser to find instructions online.

UPDATE DEVICE SOFTWARE

Software updates are not just about new features.

They often fix security problems that scammers or hackers could exploit.

Turn on automatic updates when available for your router, phone, computer, tablet and smart devices. If automatic updates are not an option, check for updates regularly.

This includes devices that are easy to forget, such as smart TVs, cameras, doorbells, printers, gaming systems and thermostats. If your router or modem is outdated and no longer receives security updates, consider replacing it.

CREATE A GUEST NETWORK

Many routers allow you to set up a guest network. This gives visitors internet access without connecting them to the same network as your personal computers, phones and sensitive information.

A guest network can also be useful for smart devices, such as smart TVs, speakers, cameras and appliances, which may not have the same security features as a laptop or phone.

REVIEW CONNECTED DEVICES

Most router apps or settings pages show a list of connected devices. If you see something you do not recognize, remove or block it, then change your Wi-Fi password. Disconnect old devices you no longer use.

TURN OFF FEATURES YOU DO NOT NEED

Some router features are convenient but may add risk if they are not needed.

Consider turning off remote management, which allows router settings to be changed from outside your home network. Also, review features such as Wi-Fi Protected Setup (WPS) and turn them off if you are not using them.

A SAFER HOME NETWORK STARTS WITH SIMPLE HABITS

You do not have to fix everything at once. Start with a few basic steps: Change default passwords, update your devices, use strong Wi-Fi security, and turn on multi-factor authentication for important accounts.

Small actions can help protect your personal information, your devices and your family's online safety.

Artificial Intelligence Creates Real Problems for Scam Victims

BY CATHY CASH

Artificial intelligence sometimes doesn't seem so artificial and that could be a real problem.

Artificial intelligence can create realistic text, voices, images and websites in seconds. Those capabilities make many everyday tools more useful, but they also make it easier for scammers to impersonate family members, banks and even your electric cooperative.

Through friendly chatbots and website agents, AI monitors your selections and online behavior so it can efficiently recommend entertainment or other online goods and services for you to consume.

But be vigilant. Scammers are using this amazing invention of computer-learning software for theft and extortion.

Scammers are applying AI to mimic familiar voices and change videos and emails to appear authentic in urgent online or phone requests for credit card and bank account numbers, electronic money transfers and personal information.

Maybe you know someone who believed their adult child or grandchild was calling to say they were in legal trouble and needed a large sum of money wired immediately. That scam has made the rounds.

Then there are investment or get-rich-quick scams, where criminals bully their victims via emails, websites or calls promising a big payout if they pay up now.

Website spoofing is also on the rise. Everything looks genuine on the surface

but when consumers hit "submit" after punching in their credit card number and other personal information they are basically handing over valuable data to a cybercriminal.

"AI can help scammers produce polished, convincing messages and build fake websites that closely mimic a bank or even an electric co-op," says Carter Manucy, NRECA's senior director for cybersecurity.

Scammers can build sites and communications that resemble an electric co-op and contact members with high-pressure calls or emails demanding instant payment via gift cards, wire and even cryptocurrency or risk shutoff.

So, what should co-op members do in that situation?

Stop and make sure the contact is legitimate. Members should treat any unexpected demand for immediate payment by gift card, wire transfer or cryptocurrency as a scam and contact their co-op directly using the number on their bill.

"Call back using a number you already know, never one the caller provides. For a co-op message, use the number on your bill," Manucy says.

"Any message that pressures you to act immediately is the top red flag, no matter how real it sounds. Real family, banks and utilities let you take a breath."

But as AI makes scams harder to spot, it also equips these rip-off artists with ways to boost their output and victimize thousands of people in just a few clicks. AI allows criminals to create, personalize and distribute convincing scams at a scale that once required far more time and people.

"Criminals can generate thousands of tailored attacks cheaply, so more scams reach members' phones and inboxes, more often," Manucy says.

As a result, the loot scammers are reaping is unprecedented. Americans

reported nearly \$900 million in AI-assisted scam losses in one year, according to the FBI. "Those figures capture only complaints that were reported and identified as AI-related, so they do not show the full scope of the problem," Manucy says.

HERE ARE SOME TIPS TO HELP PROTECT YOURSELF AGAINST TODAY'S SCAMS MADE MORE SOPHISTICATED THANKS TO AI:

- ▶ Distrust urgency of a request for money or personal data.
 - ▶ Verify parties making requests through a trusted channel, such as a phone number on your bill.
 - ▶ Before you click, verify the website address; better yet, open a new browser and type in the website address after verifying its accuracy.
 - ▶ Set a family code word not shared online and ask for the code word, such as "pineapple", if you receive an emergency call. A cloned voice won't know it.
 - ▶ Protect yourself when paying for goods and services online. Reject requirements for gift cards, wire transfers or cryptocurrency as these payments are difficult (and sometimes impossible) to recover.
 - ▶ Report scams to the Federal Trade Commission at [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud).
- "AI has changed the tools scammers use, but not the trick behind them," Manucy says. "Every scam still depends on getting people to act fast, before they stop and think. Pause and verify remains the single best defense."

CATHY CASH writes on consumer and cooperative affairs for the National Rural Electric Cooperative Association, the national trade association representing more than 900 local electric cooperatives. From growing suburbs to remote farming communities, electric co-ops serve as engines of economic development for 42 million Americans across 56% of the nation's landscape.

