



Kilowatt Korner

APRIL 2024

SIGNS OF AN

ENERGY SCAM

Tenants and homeowners have long been targets for utility scams. But in today's digital world, every swipe and click increases the risk of potential scams. Identity thieves' prey upon our increasing reliance on technology. With their sharpened digital knives, they have adapted their tactics to trick unsuspecting consumers through a variety of methods. White River Electric wants to be a partner in helping members avoid scams that result in either financial loss or compromise personal information- both of which can be incredibly damaging.



Scammers often disguise themselves—either physically or digitally—as utility staff and can be friendly, charming, and seemingly harmless. These criminals will approach consumers through a variety of means—including phone calls, text messages, emails and even in-person visits. However, the digital line of attack is most common.

New capabilities disguising caller ID can make the phone number you see on caller ID appear to be from a trusted source when it originates elsewhere – often overseas. This is called “spoofing.” Spoofing makes it easier for scammers to gain access to you because their call shows up as a local (and often familiar) number and is less likely to be ignored if it comes from a business name that you recognize and trust. Similarly, scammers will create “look alike”

websites that mirror a legitimate website as an additional method to trick you into disclosing your financial data. When visiting websites, double check the web address to make sure it matches the exact address printed on your bill.



Spotting a Scam

There are several red flags you can watch for to identify a scam. Scammers often use high-pressure tactics to create a sense of urgency, like claiming your electricity or other services will be disconnected if a payment isn't made immediately. Don't cave to the pressure or allow their urgency to rattle you. Hang up on any caller demanding money and immediately call WREA, or whatever company they claim to represent, to verify the status of your account. Digital scams, like emails or text messages, often include poor grammar or spelling errors that should raise a red flag. If you receive a dodgy email or text, don't respond, and delete it immediately.

What White River Electric Will (and Won't) Do

WREA will never demand an immediate payment and threaten to disconnect your service without prior notice or written warnings. For consumers facing disconnect, a final Notice of Termination will appear as a red door knocker which outlines payment options to avoid termination of service. WREA will never call, email, or text demanding that you disclose personal data or payment information. WREA consumers must initiate payments themselves either in-person, via mail or through our secure web portal (SmartHub) or automated phone system. Most importantly, WREA will never ask consumers for their social security number.



If you're ever in doubt about whether a person claiming to represent White River Electric is authorized, we welcome a call at 970-878-5041 to confirm their identity. WREA wants to help protect our community against fraud of all types, and work with our consumers to squash out potential scams. By doing so, we can be our own first (and best) line of defense.