HOW TO SPOT UTILITY FRAUD

1 REQUESTS FOR PERSONAL INFORMATION

Scammers often call asking for your social security number, banking information, or PIN.

When UPPCO calls or emails you, we do not ask you for your personal information. **When a customer contacts UPPCO,** customer service representatives may ask you for the last four digits of your Social Security Number or a passcode you've already established with UPPCO to identify you.

2 URGENT PAYMENT METHODS

Scammers coerce their targets to make payments through pre-paid debit cards, gift cards, money transfers, bitcoin, or other websites.

UPPCO offers many ways to pay including check or money order, secure online portal, through our payment processing partner Kubra EZPay, and cash at in-person authorized local pay stations.

3 URGENT PAYMENT REQUESTS

It's common for scammers to pressure targets to make immediate payments using scare tactics like threatening immediate disconnection for non-payment.

If you are behind on your bill and subject to disconnection, UPPCO will send a notice to your mailing address and will attempt to contact you by phone before power is disconnected.

4 PREFERENTIAL POWER RESTORATION

Scammers may call customers and pitch that they can restore power during a storm or unplanned outage immediately, for a fee, or in preferential order.

UPPCO does not require payment for electric service restoration during an outage.

5 UNANNOUNCED VISITS REQUIRING ENTRY TO A HOME

Utility worker imposters may make unannounced visits coercing residents to allow them to enter the home.

UPPCO employees do not make unannounced visits that require entry to a home. Visits requiring entry to a home are pre-scheduled, pre-arranged, or when crews need to cut power to complete work on UPPCOs facilities. Additionally, UPPCO employees will have company-branded clothing and can produce a company ID.

**Unannounced visits outside a premises may be required by UPPCO employees to: restore power, perform meter work, read an outside meter, locate buried electrical lines, or trim limbs around power lines. In these instances, an UPPCO employee may notify you that power may be interrupted or ask you to take an action e.g. turning your circuit breaker main on/off. They will not seek to enter your premises or be insistent on doing so.*

6 SUSPICIOUS EMAILS (PHISHING)

Email messages from scammers include content that mimics the company logo and colors which can be deceiving. Do not click links in suspicious messages.

Always check the email address that the notice is coming from. Emails from UPPCO Customer Service will be from customerservice@uppco.com. You will not receive an email from UPPCO requiring immediate payment. All payments should be made using UPPCO's approved payment methods.

WHAT TO DO IF YOU THINK YOU'VE BEEN SCAMMED.

If you suspect you're being scammed, hang up the phone, close the email, or shut the door before taking any other action:

1. Call UPPCO Customer Service, directly, at (906) 449-2013 to confirm that the request you've received is legitimate.
2. Always type www.uppco.com directly into your web browser when paying your bill online or looking up contact information. Don't rely on search results from your search engine.
3. Report scams to your utility provider immediately and provide as much information as possible about the nature of the call, email or visit you received.