## UTILITIES ARE RAISING AWARENESS ABOUT SCAMS

By Lisa Dailey, CPA; Northfork Electric Cooperative, Inc. COO

Last year, a scammer called Cindy Evers, a Florida pet clinic operator, and demanded immediate payment on an overdue electric bill. It sounded real.

"They knew my account number and gave me a figure that I owed that's close to what I usually pay on my electric bill," Evers said. Although she knew in the back of her mind her payment wasn't late, Evers made another payment.

"I have pets under sedation and I'm taking care of animals. I think I just panicked, thinking they were going to shut my electricity off. I did what they told me to do."  $\frac{1}{2} \int_{-\infty}^{\infty} \frac{1}{2} \int_{$ 

Evers lost \$900 because the call was a scam.

The scam that duped Evers has been plaguing utility consumers across North America for several years, robbing them of millions.

Now, utilities are fighting back.

Three years ago, more than 80 utilities and energy industry organizations from across the U.S. and Canada joined forces to recognize the first-ever North American Utilities United Against Scams (UUAS) Day on November 16, 2016. Today, the consortium includes 125 US and Canadian electric, water and natural gas utilities. Each November, a week is set aside to bring attention to these crimes during Utility Scam Awareness week. UUAS aims to educate customers about scam tactics in hopes of putting an end to these types of crimes.

Utilities have increased their communication efforts, sending information directly to members and encouraging local TV stations and newspapers to warn citizens about the scam, how it works and what people should do and not do, if they are ever targeted.

Even the wariest consumers can be duped, however. The scammers are developing new tactics every day.

The "past due" scam, similar to the one Florida customer Evers experienced, goes something like this: A customer gets a call from an 800-number that looks like a valid utility company phone number. Widely available spoofing software allows crooks to display what appears to be an official number on caller IDs. The caller threatens to cut off power if the customer doesn't pay.

But here's the giveaway: The crook will demand payment via a prepaid debit card or money order. And he'll ask for it within a specified time frame—often an hour or less.

The scammer may even quote an amount that sounds like your typical monthly bill. That way, the threat has even more credibility.

Scammers might direct the customer to a specific store nearby that sells the prepaid cards and instruct the customer to put money on the card and provide the card number to the scammer.

Some scammers have even been bold enough to contact potential victims in person, coming to the member's house.

Here are some tips on how to protect yourself:

- Do not assume the name and number on your caller ID are legitimate. Caller IDs can be spoofed.
- Never share your personal information, including date of birth,
   Social Security number or banking account information.
- Never wire money to someone you don't know.
- Do not click links or call numbers in unexpected emails or texts—especially those asking for account information.
- Utilities will never require their customers to purchase prepaid debit cards or money orders to avoid an immediate disconnection.
- If you receive a call that sounds like it may be a scam, or if you
  believe the call is a scam, hang up, call the police and report
  the incident to your local utility.

Consumers who suspect they have been victims of fraud or who feel threatened during contact with one of these scammers, should contact local law enforcement authorities. Additionally, to help prevent the spread of scams, share the information you have learned with others and repost scam awareness information on social media using #stopscams.

Visit www.utilitiesunited.org for more information and tips about how consumers can protect themselves from scams.