

SCAMS: 'YOUR POWER WILL BE CUT IN 30 MINUTES'

Co-ops and other utilities wage war on scammers

November 6, 2017

Michael W. Kahn, NRECA Staff Writer

Tim Lehenbaur came this close to falling for the scam.

It was early 2016, about six months after he bought My Father's Place, a 50-seat pizza restaurant in Warner Robins, Georgia. The phone rang during the lunch rush, and it wasn't for takeout.

"They said, 'We're with Flint, and you haven't been keeping up with your electric bill. We've got some guys headed your way, and they're going to shut off your power if you don't make a payment here by phone,'" Lehenbaur recalls. "I was sweating because we were busy, and I can't have the power shut off right now. I was almost at the point of maybe I should give them a payment because they threaten you."

It's a trap designed to panic a busy restaurateur at the worst possible time.

"That's what the scammer is doing—hoping you don't know enough about it and that you'll take action that you'll regret later on," says Jimmy Autry, senior vice president of member and community relations at Flint Energies in Reynolds, Georgia.

Scams have an estimated impact of \$50 billion a year, hitting one in four households, according to the Better Business Bureau. Lehenbaur was lucky not to have added to the tally. He asked for a callback number—which the caller provided—and then reached out to the previous owner, thinking there might be an outstanding bill.

Instead, Lehenbaur got outstanding advice.

"He said, 'Tim, just so you know, there are guys that call with this scam trying to get money out of you.'"

The previous owner suggested that Lehenbaur contact the Flint Energies CEO, Bob Ray. Ray also cautioned him about the scams and urged vigilance.

Another Day, Another Victim

What happened at the pizzeria is a story Autry has heard too many times—one that plays out daily at utilities across the country.

"I was in the call center and heard a restaurant owner nearly in tears say to one of our member service representatives, 'You mean you can't refund me that money?' And she said, 'No, you never paid us. We don't have your money,'" Autry recalls. "It was just so sad to hear that. Small-business owners have a hard time—\$1,500 doesn't come easy."

In response, NRECA and Flint Energies are among more than 100 utilities and related organizations that signed on in 2016 to Utilities United Against Scams, or UUAS. Several important partners have been recruited in the fight.

The U.S. House of Representatives recognized the third Wednesday in November as Utilities United Against Scams Day, a chance to raise awareness of the bad guys and how they ply their trade. This year's event will be November 15, 2017.

It's an uphill struggle for co-ops, municipals, and investor-owned utilities, including natural gas, water, and electric. But there are hopeful signs as they battle back for consumers.

At least for Lehenbaur there was a happy ending, though it's not really over. While it was the first time the scammers called My Father's Place, it wasn't the last. They still dial the restaurant every so often, but Lehenbaur is ready.

Part of that preparedness includes making sure staffers are aware. They're instructed that if they ever get such a call, to write down the incoming phone number—which appears in the restaurant's computer system—and then immediately report it to Flint Energies. The co-op's number is on the wall.

"It's tough. We've got a lot of high school kids, and some are part time. You have a lot of new kids, and you always have to remind yourself to tell them what's going on," Lehenbaur says.

Lehenbaur only lost time, but he understands how some folks lose cash.

"I can see how people get tied into sending them some money just to keep the power on. They definitely know how to try and scare you."

'Why Do You Want That Card?'

Autry went to a CVS drugstore recently to buy a gift card for a co-op event and got a pleasant surprise.

"When you buy a gift card, the touch screen comes up and queries you about why you're getting the card, and warns you that sometimes scammers will ask you to buy these cards," he says. "They're not saying they won't sell you a card, but it's got a little warning on the screen. I thought that was amazing."

The salesperson told Autry they've been instructed to ask customers about what they have planned for the card. Not to be nosy, but to make sure no one falls for a scam.

"I was thrilled and amazed. I told the salesperson how much I appreciate it," Autry says. "I told the manager how important it was."

UUAS has worked with two of the biggest prepaid card issuers: Blackhawk Network, whose products are often found in supermarkets, and InComm, whose cards are usually found in drugstores.

"They have invested some serious effort into detecting fraudulent activity on their networks and trying to stop it at the source," says Jared Lawrence, vice president of revenue services at Duke Energy and a leader of UUAS.

Using sophisticated analytics, prepaid card companies and retailers can jointly take actions, including "sending alerts in real time to the clerks at the retail outlets to let them know that a certain purchase looks like it might be made by a victim of a scam," Lawrence says.

The alert also prompts clerks to try to stop the purchase—exactly what happened to Autry.

They've Got Your Number; We've Got Theirs

Joel Bernstein might be the only man in America who wants a subpoena.

Bernstein is vice president for regulatory and public policy at Somos. That's not a household name, but Somos plays an important behind-the-scenes role in many phone calls you make. Somos manages more than 41 million toll-free numbers in the United States and Canada as the Federal Communication Commission's (FCC) appointed toll-free neutral administrator.

Anyone wanting a toll-free number goes to what's known as a Responsible Organization, or RespOrg, which is authorized to search for and reserve toll-free numbers in the Somos system. There are hundreds of RespOrgs, including big names like Verizon and AT&T.

"The RespOrg is critically important," Bernstein says, because the RespOrg knows who the end user is. And when you dial an 800 number, it's the RespOrg that routes the call to a local number where it's answered—the co-op office, for example.

So why does Bernstein want to be subpoenaed?

"I've got a treasure trove of information. As soon as the FCC sends me a subpoena—and I've already asked them for it—I can give them 300 numbers used in fraud and the RespOrgs responsible. Here's their contact information. Here's the dates it was up and running. Go subpoena them and figure out who the next person down the line is," he says. "I guarantee you that the utility scams are almost all going to point back to a handful of people, and it's all going to be overseas."

Over the past six months, Somos has shut down between 250 and 300 numbers on behalf of utilities.

"If it's a couple of dollars here, a couple of dollars there, you can't get the FBI and the FCC interested in it," Bernstein says. "But if you're talking about a massive fraud where people are losing millions of dollars, they're going to want to know."

If a scammer tells your co-op's members to buy a prepaid card and then call a toll-free number with the payment information, Somos wants to know.

Utilities can send an email to Bernstein jbernstein@somos.com in which he says to include key information.

"One, I need the toll-free number and that you've confirmed it's an inbound toll-free number," Bernstein says. Somos can't work with any numbers that appear on caller ID because those are easily spoofed; it has to be a number that a member has been told to dial.

"I need confirmation that this is indeed defrauding your company's customers."

He only takes that information from companies, not consumers, so the co-op will want to call the number to hear how it's answered. If there's someone using the co-op name, or even playing the co-op's outgoing message, Somos wants to know.

"We'll need a contact name at the utility and contact information—a phone number or email to confirm. With those four things, we can go after the toll-free number," he says.

Bernstein does that by going into the Somos database, finding the RespOrg for that number, and telling them that a utility has reported it as a scam number.

"They often call the number," Bernstein says, checking to see how it's answered. If it's with a utility name, "they say, yes, it's fraud, and shut it down. Within 15 minutes, that number won't connect anymore. You'll get a message that 'This number cannot be completed as dialed.'"

Lawrence of UUAS praises Somos for being "extremely responsive."

And if misery loves company, your co-op can take comfort in knowing that Somos has also shut down toll-free numbers at the behest of giants including Apple and eBay.

And, Bernstein notes, Somos has a vested interest.

“For all intents and purposes, we are the voice of toll free in the U.S. And so we want to protect the integrity of toll free as a service, and keep it so that people trust it.”

Dialing for Dollars

One way Mike Morley protects his members from scams is by calling the scammers.

Midwest Energy members reported more than 50 scam attempts in 2016, so there’s no shortage of numbers to call.

“I have to assume that the number of our members that got those calls is probably five to 10 times that,” says Morley, director, corporate communications and government relations at the Hays, Kansas, co-op.

When Morley calls one of the scam numbers, he poses as a member. “I want to know exactly what our members are experiencing and what [the scammers] are asking them to do.”

Sometimes they answer claiming to be Midwest Energy; other times they pose as different utilities. They’re always polished. While they usually read from a script, he finds them “very adaptable.”

“I can make up a completely bogus account number, and they’ll say, ‘Yeah, yeah, that’s your account number.’ It’s amazing how good these folks are at their job. This is what they do every day.”

Morley likes to throw roadblocks at the scammers, telling them he thought his wife paid the bill, or he can’t get the money for another few hours, or he doesn’t know where to buy the prepaid card they want.

“They’ll tell you where to pick up the card,” he says. “They’re making up stuff like I’m making up stuff, but they’re doing it with an air of authority that makes you want to believe.”

After five or 10 minutes, Morley tells the scammer he works for Midwest Energy, at which point “they tell me exactly where to go.” But, he adds, “This is five minutes that this guy isn’t scamming one of my members.”

Midwest Energy is a member of UUAS, which Morley says is educating consumers about scammers, whom he likens to the Whac-A-Mole arcade game—knock out one only to have another pop up.

Midwest Energy has talked with local and state law enforcement, as well as the Kansas City FBI office.

“Their threshold for investigation is usually \$50,000 in losses. Well, these guys know that, and they’re smart enough. They stay under that threshold by posing as different entities to escape prosecution. Today, they’re Midwest Energy. Tomorrow, they’re a co-op in Florida,” Morley says.

Lawrence says one of the goals of UUAS is to “paint a much better picture of the magnitude of the problem, so that law enforcement sees the value in dedicating significant resources to investigating and ultimately shutting down these scammers.”

Scam Tracker

Watch a news story about utility scams, and you’re likely to see senior citizens who’ve fallen victim. But the Better Business Bureau (BBB) says that’s not an entirely accurate picture of the more than 80,000 scams it has logged since launching its Scam Tracker in November 2015.

“Overall, what we see is that it’s young people who are at the greatest risk,” says Emma Fletcher, director, scam and fraud initiatives at the BBB Institute for Marketplace Trust.

But isn't the new generation hipper and wiser?

"I think that's the problem—they think that too," Fletcher says. "They think this is something that happens to somebody else. They're savvy—certainly tech savvy—and they don't listen to the messaging."

BBB research finds susceptibility to scams is highest among those 18 to 24, before decreasing with age, though the median loss increases as people get older.

"We get a lot of reports from seniors. They're very proactive. They've gotten the message that they're at risk," Fletcher says. "Young people are walking around thinking they're the only one that's been scammed because nobody else is talking about it except seniors. So they're less likely to report."

The BBB Scam Tracker allows people across the United States and Canada to report scams and see what scams are active in their areas.

"We're just getting started," Fletcher says. "BBB is the first organization people think of to report a scam, so I think we are at a tiny fraction of the volume we will eventually see."

Fletcher says scams hit one in four households, so spreading the word is crucial. For co-ops and other utilities looking to reach their consumers—especially the younger ones—Fletcher recommends letting them hear from victims.

"The voices of real people, talking about what has happened to them," helps make the problem relatable, she says, adding that it counters the misperception that victims are uneducated. Those hearing the message realize, "If it happened to this person, who is well-spoken and seems to be someone I can relate to, then it could happen to me."

Enlist Your Co-op in the Fight

UUAS is always looking for more utilities to sign on. Why should your co-op join?

"It's free, and the level of involvement is purely voluntary," Lawrence explains. "We'd love to have as many utilities at the table, helping to shape the messages, identify trends and best practices, and basically become better as an industry."

UUAS members routinely share content for ads, social media, and other forums. The material—often created by bigger utilities like Duke Energy—is free. It's also generic, coming without any utility's name.

"It's a good way for smaller organizations that don't necessarily have the marketing budget, the communications resources, or the individual lobbying presence to get things done," says Lawrence.

Still, many utility staffers wonder how anyone could fall for a scam. Jimmy Autry offers an explanation.

"Someone in this clandestine, illegal call center makes 1,000 phone calls all day long, and 999 people say, 'You must be crazy. Go away,'" Autry says. "But one person gives them \$1,500—which happens with a lot of commercial accounts—that's a day's work."