

Contact:
ComEd Media Relations
312-394-3500

FOR IMMEDIATE RELEASE

ComEd Offers Families and Businesses Tips to Avoid COVID-19 Related Energy Scams

Scammers target vulnerable customers

CHICAGO (Sept. 17, 2020) – As the COVID-19 pandemic takes a financial toll on families and businesses across northern Illinois, scammers are increasing their efforts to take advantage of vulnerable customers who may be struggling to pay their bills.

Even before the pandemic, ComEd had experienced a 60-percent increase in reports of scams and attempted scams into its call center since 2017. More recently, imposters posing as ComEd employees are approaching individuals and businesses to attempt to steal their money, as well as personal and business information.

“During the pandemic, ComEd has received reports of scammers, posing as utility representatives, contacting customers who may be experiencing difficulty paying their bills,” said Nichole Owens, ComEd vice president of customer channels. “These imposters prey on these customers’ financial situation by falsely threatening to shut off service to obtain money or a customer’s personal, business or financial information.”

One tactic scammers use with more frequency is “spoofing” ComEd’s name and phone number. Spoofing uses technology to change the caller’s identification information so that ComEd’s name and phone number appear in the customer’s caller ID display. Another tactic involves sending emails with slight modifications to the ComEd name to make it appear it is coming from the energy company. Scammers may even demand that an individual make a direct payment with a prepaid cash card or instruct a business to deposit a payment in an alternate account.

Tips to help homeowners identify scams

ComEd will never visit or call a customer’s home or business to:

- Ask for immediate payment with a prepaid cash card or cryptocurrency such as bitcoin.
- Ask for their ComEd account number or other personal information, such as a driver’s license number, Social Security number, tax identification number or bank information.

Tips to help businesses to identify email scams

- Carefully review email messages originating from outside your business network.
- Check the person’s name and business in the email and make sure it matches the name and business in the email address. For example, some imposters will use zeros in place of the letter O or switch letters in the business name so that “corp” appears as “crop.”

- If you don't recognize the sender, call the individual or business to verify the message is legitimate. Use a phone number from your own records or an online search and not the number provided in the email.
- Confirm that the contents of the email look legitimate, especially when a request can have major effects for your company, such as transferring large amounts of money.
- Hover over website links before clicking to confirm the legitimacy of the site.

Tips to help all customers identify an actual ComEd employee

- All ComEd field employees wear a uniform with the ComEd logo, including shirt and safety vest.
- ComEd employees visibly display a company ID badge with the ComEd logo and employee's name.

Scammers rapidly change their tactics so if you are suspicious of any energy-related request or actions, stop what you are doing and call ComEd immediately at 1-800-EDISON-1 (1-800-334-7661). Businesses can call 1-877-426-6331. For more tips on identifying energy-related scams, visit [ComEd.com/ScamAlert](https://www.comed.com/ScamAlert).

###

ComEd is a unit of Chicago-based Exelon Corporation (NASDAQ: EXC), a Fortune 100 energy company with approximately 10 million electricity and natural gas customers – the largest number of customers in the U.S. ComEd powers the lives of more than 4 million customers across northern Illinois, or 70 percent of the state's population. For more information visit [ComEd.com](https://www.comed.com) and connect with the company on [Facebook](#), [Twitter](#), [Instagram](#) and [YouTube](#).