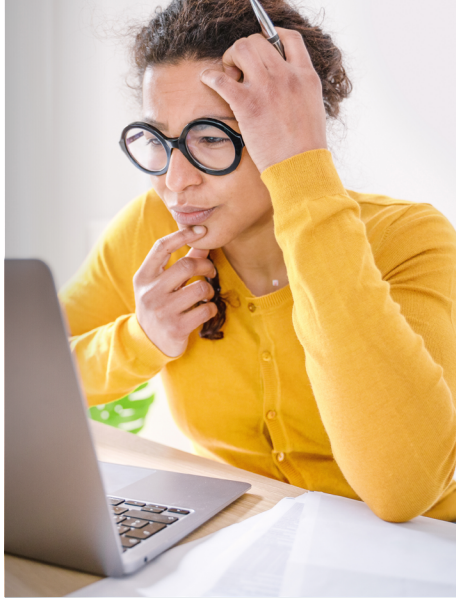
PUT A STOP TO ENERGY SCAMS

We constantly receive reports of scammers posing as ComEd employees. Whether over the phone, via email, or at your business, scammers attempt to impersonate ComEd with the intent to deceive customers into providing sensitive business information or acting on urgent requests for payment.

Actions like these should raise a red flag of a potential scam attempt. Being aware of the signs of a scam is your first line of defense.



Recognize Red Flags

It is important to remember ComEd will never call or come to your business to:

- **Sell you electricity**
- **Ask for your account number**
- **Ask you to make a direct payment with a prepaid cash card, cryptocurrency such as Bitcoin, or third-party electronic banking app such as Cash App, Zelle, QuickPay or Venmo.**
- **Ask for your personal information such as Social Security number, Tax ID, or bank information**

CONTACT YOUR ComEd LCS ACCOUNT REPRESENTATIVE

for help

ComEd.com/LCS

Identify ComEd Employees

ComEd field employees can be identified by:

- **Company ID badge**
- **ComEd clothing**
- **Safety vest**

ComEd employees may come onsite for maintenance services or requested outages. For managed customers, those visits are scheduled in advance. Call your ComEd Large Customer Services Account Representative if you are suspicious of someone on your company's property. A legitimate ComEd employee is happy to wait while the call is made.

Please be aware of potential threats via web and email:

Scammer's tactics are constantly evolving. One common tactic is "spoofing", where the scammers can alter the caller ID and use a number that appears to be a ComEd phone number. They are even taking advantage of technology to create fake websites and email addresses that mimic legitimate organizations like ComEd, this practice is known as "phishing."

- **Carefully review messages originating from outside your organization's network.**
- **Check the name of the sender and business in the email and make sure it matches the name and business in the email address. Tip: Look for misspellings and zeros in place of the letter O.**
- **Do you recognize the sender? Don't hesitate to make a phone call to verify a message is being sent from a trusted source. Tip: Confirm the phone number in the email to one on the official company website.**
- **Confirm the contents of the email look legitimate especially when a request can have financial impacts, such as transferring money. Tip: Don't click on unfamiliar links.**

If you or anyone at your business believes they have fallen victim to an energy-related scam or fraudulent attempt, please immediately call ComEd at **800-EDISON1**. For more information call your Large Customer Services Account Representative or visit **ComEd.com/LCS**.

ComEd®
An Exelon Company

powering lives