

General Tips to Avoid Impostor Utility Scams

PROTECT PERSONAL INFORMATION

Never provide or confirm personal information (Social Security number, date of birth) or financial information (banking account information, debit or credit card information) to anyone initiating contact with you, whether by phone, in-person, or email, claiming to be a utility company representative. If your utility leaves you a message or contacts you by phone, it will typically ask to speak to the person whose name is listed on the account, and if you call your utility, it may ask for some personal information to confirm your identity for your protection. Never give out information or provide any payment type to any callers or unexpected individual(s) appearing at your home or business claiming to represent your utility. Your utility will have your relevant personal and account information.

TAKE YOUR TIME

Do not be rushed. If someone calls, appears, or emails saying you have to pay your bill immediately to avoid disconnection, tell them you would like to verify that they are a legitimate utility company representative by calling a verified number for the utility company. Beware if a caller or in-person representative exhibits impatience, annoyance, or anger when you question their authority. Notice if their emotion intensifies when you ask to speak with their manager, request their phone number, or offer to call back later. While a scammer will discourage

you from hanging up and calling the number on your utility bill, a real utility representative will encourage you to do so for your own peace of mind.

ALWAYS ASK QUESTIONS

Ask the person calling you or visiting you in person to provide you with your account number, your last payment amount, date of payment, and his/her employee identification number. If he/she is a legitimate utility representative, this information will be readily accessible. If not, hang up or shut the door, and call your utility. Before you provide any information or purchase any product from someone appearing at your home or business, independently confirm the authenticity of the representative's business by researching it online—verify the website and contact information and search for customer reviews and company policies.

REPORT THE SCAM TO YOUR UTILITY

Know that your questions may scare the scammer off. If not, document what the scammer told you, including the name they provided you, the date and time you spoke with them, their caller ID number, their employee identification number, the method and amount of payment they requested, any phone number they requested you call to pay your bill, and any other details that might aid in a possible criminal investigation. If you purchased

a prepaid card and provided the card's number to the scammer for payment, record the prepaid card number as well. Call your utility immediately to inform them of the scam, and give this information to your utility when you call. If you want to check on your account, call your utility's phone number provided on your monthly bill, or on their website, or log into your account on the website.

PAY YOUR UTILITY ONLY

Never make a utility bill payment to anyone calling you on the phone, coming to your door (unless that is a verified bill payment method used by your utility company), texting you, or emailing you. Always call your utility company, at the number provided on your bill or on the utility's website, if you have a question about payment or billing information. Know your utility bill payment options—online, by phone, automatic bank draft, mail, or in person. Never wire money or give the number from a prepaid card to someone you do not know. Once you do, you cannot get your money back. Be suspicious if the caller is requiring the use of a specific payment option, like a prepaid card, as utilities never ask or require a customer to purchase a prepaid card to avoid disconnection.

STAY UPDATED ON SCAMS

Review guides like this, local news reports and websites, utility and trade association websites (including www.UtilitiesUnited.org), local law enforcement websites, state attorneys general websites, federal government websites, consumer information websites, and research incoming phone numbers you do not recognize. Scammers are constantly updating their tactics, and you will need to stay educated on new types of scams and tips to avoid them. Pass on information about impostor electric, water, and natural gas scams to people you know.