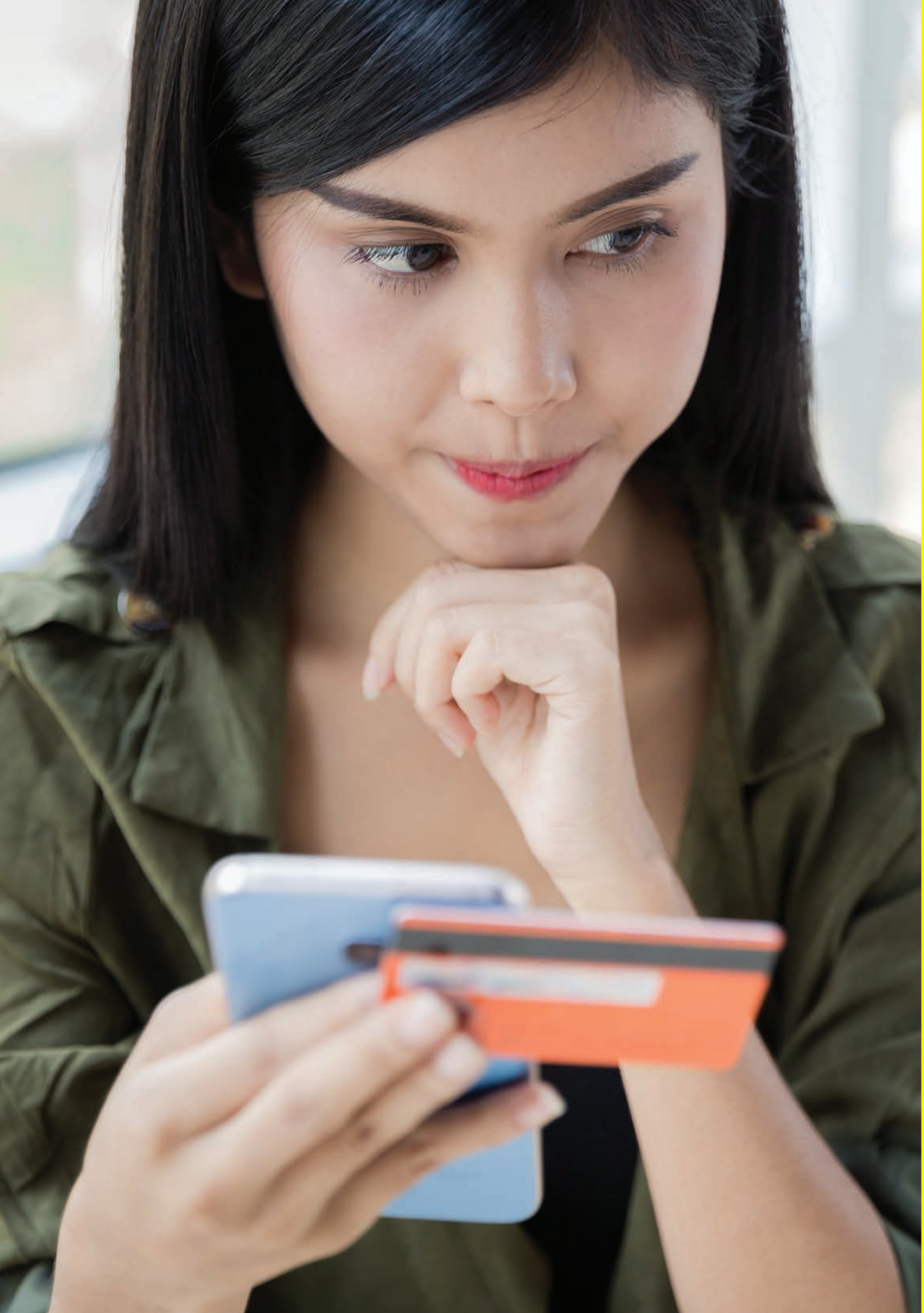
UTILITIES UNITED
AGAINST SCAMS

Consumer's Guide to Impostor Utility Scams

AUTHORED BY
Sheri Givens
Givens Energy

NOVEMBER 2017



About This Guide

The intent of this educational guide is to provide key information to consumers and community leaders on: (1) the types of impostor utility scams that are occurring across the country (phone, in-person, and internet); (2) tips to avoid scams that individuals can use and share with their communities; and (3) names and contact information for the entities and organizations that may be called upon in case someone becomes a victim of an impostor scam.

It is the hope of the author and Utilities United Against Scams (UUAS) that community leaders will: (1) use and present this information at in-person presentations at local clubs or events, workplaces, churches, neighborhoods, schools, and other venues; (2) share the information through print media, social media channels, and educational campaigns; (3) offer the guide to other local groups as a resource to help prevent utility customers from becoming scam victims; and (4) distribute the consumer scam alerts located at the back of this guide in community centers, workplaces, and other public spaces. Community leaders are encouraged to photocopy the consumer scam alerts for use in presentations and posting in public spaces, without prior permission, for noncommercial use.

Scammer tactics change daily. It is intended that ongoing updates will be developed that describe new scam types and provide tips for avoiding them. These updates may be provided by utilities, trade associations, and other similar entities through their social media platforms and websites. Toolkits, community presentation templates, additional handouts, and other related educational materials may also be forthcoming.

This guide is the result of the author's research on general utility impostor scams and the author's work with UUAS, a consortium of more than 100 North American electric, water, and natural gas utilities, and their respective trade associations, working together to educate utility customers and help put an end to scams. The opinions expressed in this guide represent the author's views alone. The author would like to express her appreciation to UUAS and the utility trade associations for their support. »

Authored by
Sheri Givens, President, Givens Energy; Executive Director, Utilities United Against Scams; and Former Texas Utility Consumer Advocate

Thanks to
This guide was enhanced by the reviews of the following organizations and individual whose input is greatly appreciated: AARP; Conference of Western Attorneys General; James Bradford Ramsay, General Counsel, Policy Shop Supervisor, National Association of Regulatory Utility Commissioners; National Association of State Utility Consumer Advocates; Office of Nevada Attorney General Bureau of Consumer Protection; and Utilities United Against Scams.

Funded by
Funding for this guide was provided by the American Gas Association, American Public Power Association, Edison Electric Institute, National Association of Water Companies, and National Rural Electric Cooperative Association.

Copyright

ATTRIBUTION NOTICE AND DISCLAIMER

This work was prepared by Sheri Givens, Givens Energy, for the Edison Electric Institute (EEI). When used as a reference, attribution to EEI is requested. EEI, any member of EEI, and any person acting on its behalf (a) does not make any warranty, express or implied, with respect to the accuracy, completeness or usefulness of the information, advice or recommendations contained in this work, and (b) does not assume and expressly disclaims any liability with respect to the use of, or for damages resulting from the use of any information, advice or recommendations contained in this work.

The views and opinions expressed in this work do not necessarily reflect those of EEI or any member of EEI. This material and its production, reproduction and distribution by EEI do not imply endorsement of the material.

PUBLISHED BY

Edison Electric Institute
701 Pennsylvania Avenue, N.W.
Washington, D.C. 20004-2696
Phone: 202-508-5000
Web site: www.eei.org

Table of Contents

1 **ABOUT THIS GUIDE**

5 **INTRODUCTION**

7 **SCAM TYPES**

8 Phone

10 In-Person

12 Internet

15 **TIPS TO AVOID SCAMS**

15 General

17 Phone: Hang up on Calls from Crooks

18 In-Person: Shut the Door on Scammers

18 Internet: Delete Suspicious Emails

21 **NEXT STEPS & UPDATES**

22 **CONSUMER SCAM ALERTS**

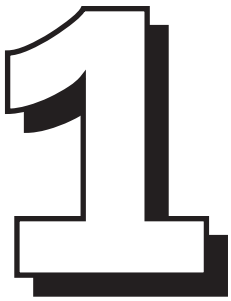
Top 10 Impostor Utility Scams

General Tips to Avoid Impostor Utility Scams

Tips to Avoid the Most Common Impostor Utility Scams

Reporting Impostor Utility Scams

Kathy, an Ohio restaurant owner, was called by someone claiming to be from her electric company and threatening to cut off her power within 45 minutes if she did not pay the more than $1,000 she allegedly owed. It was lunch-time, her eatery was full of customers, and loss of electricity would have been financially harmful for her busi-ness. She did not consider herself easily duped, but the caller was very convincing. As requested, she went to a local drug-store, purchased the requested prepaid cards to pay her bill, called the number she had been given, and unknowingly handed over her hard-earned money to a scammer.



Introduction

Congratulations on taking your first step in helping yourself and others avoid becoming a victim of an impostor posing as your electric, water, or natural gas utility. This guide may be used as your first line of defense and shared with others in your community to make them aware of crafty criminal tactics targeting their pocketbooks, property, and personal information. The information provided here can also help inform others who might not have knowledge of or access to such materials, especially the elderly, non-English speaking communities, or other vulnerable populations who might be more susceptible to criminal schemes.

What scams are out there? What tactics are scammers using to steal your money, your property, or your identity? What should you do if you think you might be or have been the target of a scam? Who should you call to report a scam? These are the questions this guide hopes to answer.

Do an internet search of "utility scam" and you will likely run across the stories of victims paying hundreds or thousands of dollars to scammers to avoid fictitious electric, water, or natural gas service shutoff, or to purchase unnecessary products or services. Scammers are clever, persuasive, and insistent. They are often professional criminals who are very skilled at finding the right angle to hook their victims. They call or arrive when people are busy or distracted, and the last thing the victims want is to have their electric, water, or natural gas service shut off or malfunction as they are working to meet their family or customer needs.

Utility companies around the nation are taking steps to help educate their customers about scams, sending alerts and messages through traditional channels, like websites, bill inserts, radio, television, and newspapers, as well as social media, like Facebook, LinkedIn, Instagram, and Twitter. Many are posting information online to help educate customers about how to recognize and respond to scams, and working with federal and state law enforcement, government agencies, regulators, legislators, advocates, businesses, and media to assist in raising awareness.

It should come as no surprise that utilities, with a core mission to serve their customers, would support a consumer scam awareness guide. Utility companies have taken on the responsibility of educating the customers they serve daily and cannot tolerate impostors posing as employees, given the level of trust necessary between customers and their utilities in providing essential public services. Utility companies are in the best position to advance customer awareness about fraudulent tactics that can put their customers' finances, identities, homes, and businesses at risk.

Use this guide as a tool to protect yourself, your family, your neighbors, and your community. Follow your utilities in their campaign against scammers through their individual websites, social media (#stopscams), and the electric, water, and natural gas utility companies' collaborative campaign, Utilities United Against Scams (www.UtilitiesUnited.org), which offers insights on scam trends, provides updates on new scam practices, and helps educate and protect all electric, water, and natural gas customers. »

Scam Types

North American utility customers are reporting millions of dollars lost annually to scams. A 2017 report published by the Better Business Bureau (BBB), *BBB Scam Tracker Annual Risk Report: A New Paradigm for Understanding Scam Risk*, found an average of about one scam report is received every 15 minutes, the top means of consumer contact by scammers is by phone, and the median financial loss to consumers is $274. Of the 30 different types of scams tracked and categorized, utility scam victims were found to have a median financial loss of $500, with the top payment method being prepaid cards and the top method of contact being by phone. BBB has found that people are more susceptible to utility scams than they are to Internal Revenue Service scams.

Scammers who pretend to be electric, water, and natural gas utility employees exploit the trust customers place in their utilities. They also rely upon aggressive tactics and the confusion created by surprise. These scammers are very cunning, will often apply pressure if you start to ask questions, and always speak with a sense of urgency, ensuring customers do not have time to think about or verify their claims.

Scammers typically use three tactics (phone, in-person, and internet) to target utility customers; however, there are more than 10 types of known scams, with new scams emerging almost daily, and scammers might use one, two, or all three tactics on customers for certain types of scams. »

> *"It is important for consumer education to boost a potential scam victim's confidence and ability to protect oneself, giving them tools empowering them to fight and avoid becoming victims of scam."*
>
> **—Better Business Bureau**

Phone

Hang Up on Calls From Crooks
Scammers are creative, tenacious, and willing to invest their time for the potential payout. They might call hundreds of phone numbers to get one hit, netting them hundreds or even thousands of dollars. Growing access to personal information through the internet gives scammers additional tools and insights to use against unsuspecting utility customers.

New capabilities for spoofing, or disguising, caller identification (ID) can make the phone number you see on your caller ID appear to be your utility company's. Spoofing makes it easier for scammers to deceive you, and makes it more difficult for you to immediately verify the call. Because of the trust we place in our caller ID, spoofing can cause even the most alert and savvy consumers to fall victim.

Following are several types of current scams targeting electric, water, and natural gas customers' phones nationwide:

- **Disconnection Deception**
  Scammers call threatening disconnection of your utility service, demanding immediate payment by prepaid cards purchased at a local retail store (or credit card, debit card, bank draft, wiring money, etc.), and insisting you call them back with the card information to make payment. They often use caller ID spoofing, and their call-back numbers may even include recorded replicas of utility company greetings. If you give them your card numbers or other payment, the scammer removes the cash value, and your money is gone. This may also be done in person or via email.

  The truth is, your utility will send you one or more disconnection notices in the mail before disconnecting or shutting off your utility service, and they will offer several bill payment options without specifying the type of payment you need to make.

- **Equipment or Repair Bogus Fee**
  Scammers call demanding a separate payment to replace or install a utility-related device or meter.

  If a utility needs to upgrade or replace a piece of equipment, it will contact you ahead of time as a courtesy. If there is a charge related to work on equipment you might own, it will typically be included in your monthly bill as the utility does not collect a separate payment for equipment or installation.

- **Overpayment Trick**
  Scammers call claiming you have overpaid your utility bill, and you need to provide personal bank account information or a credit card number to facilitate a refund. This is a scam.

  In reality, your utility will apply any overpayments you have made to your utility account, allowing the credit balance to cover any future charges. Alternatively, utility refunds of overpayments may be made by mailing a check to the customer's address on file.

- **Bill Payment or Credit Con**
  Scammers may provide you with a phony bank, Federal Reserve, secret account, or Social Security trust account routing number for you to use to pay your utility bills or to receive a credit for your utility bills. They may also offer you a promise

of federal assistance on your utility bills, claiming you are eligible for a reduced rate due to a certain federal program. In exchange for personal information, like your Social Security number, you may get what you think is a legitimate payment account number, but it is really just a way for the scammer to obtain your personal information, which can then be used for identity theft. Also, if the routing number is entered during an online transaction, it may appear that your bill is paid or credit has been applied as it often takes a day or more for a banking transaction to be rejected; however, no funds are actually paid to the utility or applied to the account, and the account balance remains due. You may also be charged a returned payment fee by your utility for attempting to use an unauthorized account for payment.

- **Power Restoration Rip Off**

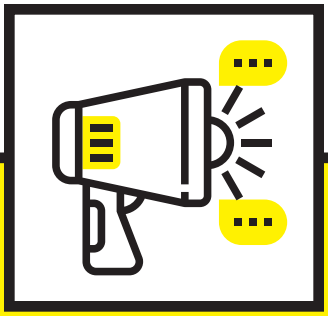
  Scammers call offering to restore power quickly or in a preferential order for immediate payment typically in the aftermath of hurricanes and other severe storms causing widespread power outages. An individual claiming to be a utility company employee might request upfront payment or a "reconnection fee" in return for restoring your service.

  Utilities do not require payment to restore electricity, water, or natural gas service after a natural disaster or other related outage, though some utilities will accept in-person payment via check or phone payment after a disconnection for non-payment. If repairs to customer-owned equipment are necessary before service can be restored, the utility's representatives will generally advise you to have the work done by a licensed contractor. If a charge is ever applicable, you will be billed through your utility account.

- **Smishing Scam**

  Smishing, short for SMS phishing, is a relatively new scam that attempts to trick mobile phone users into giving scammers personal information, which can be used for identity theft, via a text or SMS message. Scammers like smishing, as consumers tend to be more inclined to trust text messages.

  Utility companies typically do not text you unless you have signed up for a specific notification service offered by your utility.



SCAM ALERT
Duke Energy

Scammers have targeted many small businesses in this utility's multi-state service territory. They tend to call restaurants and bars during peak hours, like lunch or happy hour, threatening disconnection if the bills are not paid immediately. They have also called physician and veterinarian offices during busy office hours, and savvy business owners have fallen victim to the crooks' aggressive assertions, paying as much as $1,000 to avoid the alleged disconnection.

In-Person

Shut the Door on Scammers

Your personal safety, and that of your family members and employees, is likely your top priority. It is also important to your electric, water, and natural gas company. When someone comes to the door of your home or your business, think before you allow them to enter or engage with you. There have been numerous reports by utility customers of in-person scammers falsely stating they were with the utility company and needing access to the residence for equipment inspection, testing, treatment, or other equally plausible reasons. These scammers might have been attempting to gain access to the customer's dwelling for an immediate or future burglary. Other scammers might ask you in-person questions to gather your personal information for identity theft, or they may insist on your need to purchase a costly device to ensure the continued safety of your electric service, water quality, or natural gas service.

Scammers on your doorstep may wear "uniforms" emblazoned with your utility company's logo. These uniforms may be homemade, or even stolen, and could include a fluorescent vest, hardhat, clipboard, or walkie-talkie, all easily purchased online for around $50. The scammers may sport official-looking badges which can be printed from any computer. They may even go so far as having magnetic signage on their vehicle displaying the semblance of your utility's logo. Unless you are expecting a utility-related visit, keep your door locked and call your utility to confirm the identity of the visitor.

Most of the time, utility company employees visit your home or business in response to a service request. If no one scheduled an appointment, you should call your utility (at the number on your bill or the company's website, not a number given to you by the person at your door) before allowing anyone inside your home or business. Sometimes a utility employee may need to enter your home, business, or outdoor area. Typical examples of situations potentially requiring utility worker entry to your dwelling include natural gas-related issues, appliance checks, or internal meter reading for your monthly billing period or in response to a request you initiated.

There are other times utility companies may ask for access to your home *not* in response to a request you made; however, typically, this request is made by the utility in advance of their worker showing up at your home or business. This could occur if there has been an electrical or natural gas outage in your neighborhood, and indoor access is needed to relight the pilot lights of your gas appliances or perform a gas leak test. Regulations might require water sampling ensuring the utility's water system meets and exceeds quality standards, checking cross connections, or inspecting backflow.

Some situations may require a utility employee to enter your yard, such as restoring power associated with an electric outage in your neighborhood requiring their work on poles or metal pad-mounted cabinets, changing or restoring an outside meter, locating or digging for buried utility lines or pipes, or trimming trees away from electric lines that run through your property. Always ask for credentials or photo identification, and call your utility if you have any questions.

Following are several types of known utility impostor scammers knocking on electric, water, and natural gas customers' doors nationwide:

- **Contractor Con**
  Scammers posing as utility workers or contractors affiliated with your utility may knock on your door claiming to be employed or hired by the utility company to reset, repair, replace, or inspect your utility meter or other utility-related device. These scammers may also claim that there is a monetary charge for the service, and if you do not pay, they will return to remove your meter later.

  If a utility employee or authorized contractor needs access to your home, an appointment will be scheduled in advance, and proper identification will be provided for your review.

- **Home Improvement Huckster**
  Scammers posing as utility workers may appear unannounced at your front door offering a free energy audit, efficiency inspection, water quality or pressure testing, or some other service. These unsolicited intruders may be pitching unnecessary expensive products or attempting to steal items from you.

  Unless your utility company has notified you in advance, or you initiated a request for such a service, do not let them into your home or business.

- **Leak Lie**
  Scammers posing as utility workers may knock on your door claiming that there is a major gas or water leak in the area and that they need to come inside to check the pipes or lines. They may try to collect your personal information for later identity theft, or while one scammer distracts you, a second scammer might enter and remove valuables from your home.

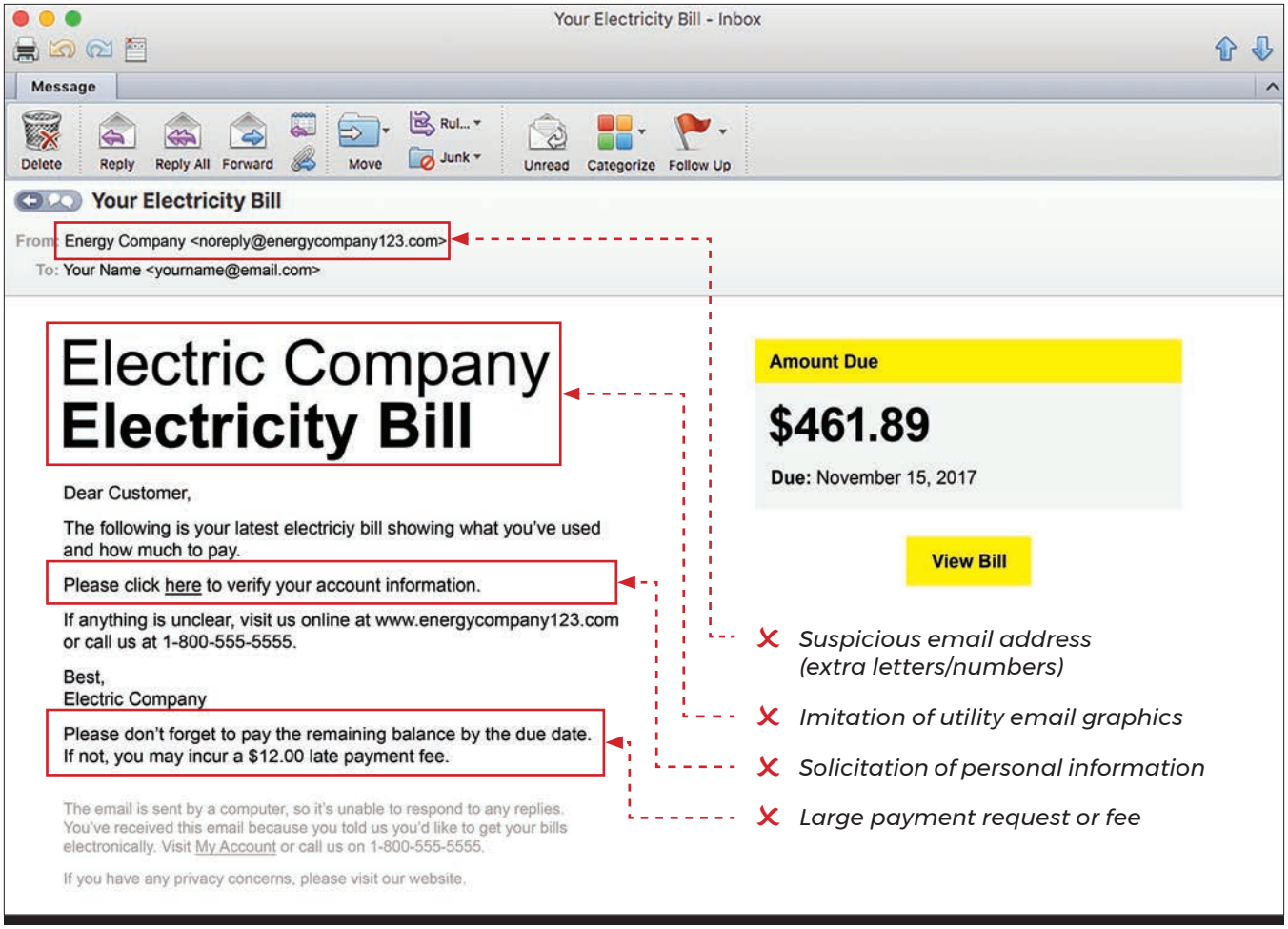
  A utility company will typically phone you in advance to set an appointment for such a service, or if it is an emergency, the company will have its workers provide you photo identification for you to call the company and verify their employment.

Internet

Delete Suspicious Emails

Many utility companies use email to communicate with their customers about their accounts, inform them about available programs, and provide newsletter updates; however, utilities never ask their customers for Social Security numbers, driver's license numbers, passwords, or financial information by email. Scammers often mimic legitimate utility company correspondence to trick you into opening an email, clicking a link, making a payment, or giving away your personal information.

Scammers posing as utility companies often utilize phishing, the fraudulent practice of sending emails to steal your money or obtain your personal information. Some scammers send spam emails disguised as legitimate utility emails with spoofed utility email addresses, logos, trademarks, website links, and wording to add to the deception.



Scammers also use malware, short for malicious software, specifically designed to gain access to or damage your computer without your knowledge. There are various types of malware including spyware (for stealing sensitive information), ransomware (for extorting money), and keyloggers (for surveilling your keystrokes to obtain personal information). If you click on attachments or hyperlinks in emails from unknown senders, including scammers posing as your utility company, you may inadvertently download malware to your computer. New types of malware are created daily due to the lure of money that can be made by scammers committing internet crimes. Always keep your computer antivirus products up-to-date.

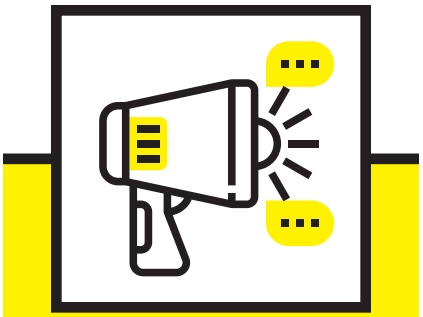
Following are several types of suspicious emails being sent to electric, water, and natural gas customers nationwide:

- **Bogus Bills**
  Scammers send suspicious emails that appear to be a bill sent by your utility company, potentially featuring your utility's logo and color scheme. The email address may be slightly or very noticeably different from the one your utility company uses to send information and updates to you.

  Utility companies typically send bills by mail, unless you have opted to receive your bill by email.

- **Employment Ruse**
  Scammers post spoofed utility employment listings on job-search websites and contact potential job applicants with employment offers in an attempt to trick them into divulging personal information. Scammers may also send checks to the victims to make purchases, which are deposited by the victim and later returned for insufficient funds.

  Utility companies typically post their job openings on their own websites.



SCAM ALERT
FirstEnergy Corp.

Jobseekers reported a scam where criminals were mimicking elements of legitimate job postings. Victims reported that the compensation listed on the fake posting was often much higher than market average. After the candidate applied for the job, an online chat interview was set up. Later, the scammer offered the candidate the job, provided them with a fraudulent check for purchase of home office equipment, then either directed them to purchase the equipment, on the scammer's designated website, providing the scammer with the victim's credit card information, or asked the victim to withdraw the funds from the scammer's deposited check, and deposit the money at another particular bank. The scammers' checks were rejected by the scam victims' banks.

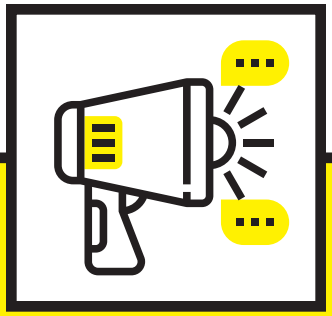
3

Tips to Avoid Scams

So far, you have learned about known, current scam tactics; however, scammers are clever and constantly adapting to find new ways to steal your money, belongings, and personal information. With that in mind, below is a list of ways for you and your community to play your part and avoid becoming victims of scams:

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. »



SCAM ALERT
American Water

In a multi-state scam, criminals called customers claiming the U.S. President was providing credits or applying payments to utility bills and requested the utility's customers provide their Social Security numbers to apply for the program. The customers were then given a phony bank routing number to pay their utility bills or to receive a credit on their utility bills. If the routing number was entered during an online transaction, it appeared that the customer's bill had been paid or the credit had been applied, but no government funds were actually applied to the customer's account, and the account balance remained due. The scammers also emailed, texted, and used social media to reach customers.

- **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.

- **Utilities Mail Disconnection Notices**
  Customers with delinquent accounts receive advance disconnection notification included with their regular monthly bill—never a single notification shortly before disconnection. Remember, your utility company will *not* notify you by phone, email, in person, or text message as your first and only notification about a potential disconnection or shutoff—it will mail you such notice—at least one, if not several times, before terminating service. Scammers might claim that you have been sent previous bills—do not fall for it. If you get a cancellation notification (especially by phone), hang up and verify it by calling your utility. Know that utilities sometimes do call customers whose bills are in arrears, or have not yet been paid, in order to remind them that a payment is due; however, a legitimate utility representative will explain to a customer how a payment can be made using the utility's established payment options—they will not demand payment over the phone or at a particular physical location. If you want to verify a utility company's phone call is legitimate, ask the representative to confirm your account information only your utility and you would know, including the date of your last payment, the amount of your last payment, and your account number.

- **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 their 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 them. If you want to check on your account, call your utility's phone number provided on your monthly bill, or on its 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.

Phone

Hang Up on Calls From Crooks

- Hang up if you receive a call requesting immediate payment of a utility bill to avoid immediate disconnection or shutoff, and always call your utility company directly at the phone number printed on your regular bill or on the company's website.

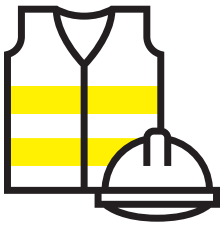
- Never be fooled because your caller ID makes the call look like it came from your utility company. It is easy to imitate a utility company's phone number. Call your utility directly to confirm your account status.

- Never use the call-back phone number provided by an unknown caller to verify billing or account information. It is easy for a scammer to imitate a utility's call-back number and voice recorded greeting and menu messages. Call your utility directly to verify your account.

- Never provide any payment (money wiring, prepaid, credit, or debit card) or personal information (Social Security number, date of birth) to a caller you do not know. If you want to check on your payment status for your account, call your utility.

- Know how to access your monthly bill easily, or call your utility company's customer service number to verify your account. You may wish to access your utility account information online through the utility's website or customer portal, keep a hard copy, take a photo of it with your phone, or another practical method that works best for you.

- Do not reply to text messages from people you do not know, do not click on links you receive on your phone unless you know the person they are coming from, and, if you receive a message from a friend, consider verifying they meant to send you the link before clicking on it.
- Never install apps from text messages, and if you have any doubt about a text message, exercise caution and do not open it.
- Several cellular service providers are now offering free scam blocking, and several smartphone apps are available for download in the Apple or Android stores. Do online research for reviews from other users and experts before committing or downloading.



In-Person

Shut the Door on Scammers

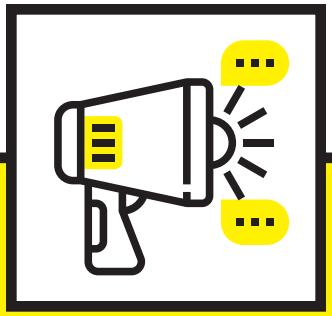
- If you feel you are in personal danger, call 911. If you can safely get a good description of the individual(s), write it down and provide the information to police responding to the area.
- Be suspicious of anyone who arrives at your home or business without an appointment asking for immediate payment or access to your dwelling to check your electrical wiring, water pipes, natural gas pipes, or appliances unless you have scheduled an appointment or reported a problem.
- Do not let unknown individuals into your home and always ask for proper identification. If you have any questions regarding such individuals, utility services, solicitation, or potential fraud, contact your utility company at its customer service number on your monthly bill or the utility's website.

Internet

Delete Deceptive Emails

- If you receive an email that appears to be from your utility company that you are unsure about, delete it. Do not click on links, open attachments, download pictures, forward it, or respond to it. Always call your utility to report suspected email and internet scams.
- Never be fooled by an email that looks like it came from your utility company requesting personal or financial information. It is easy for scammers to imitate a utility company's logo, email address, bill, and even create convincing, phony websites.
- Scam emails may come from a suspicious email address. When you move your mouse over the email address, any links, URLs, or web addresses in an email, you should see the same address or URL. If the address or URL is different from the address displayed, then the message is probably fraudulent or malicious.

- Be careful providing information online. If you are asked or directed to make payment via a website, check to make sure the website is secure. A secure website starts with "https://"—remember the "s" is for secure. In general, "http:" websites are vulnerable to attack.
- If you think you have been a victim of an internet scam and made a payment, call your financial institution immediately to let them know. Also call your utility to report the scam, disconnect your computer from the internet, and run an anti-virus scan.
- Remember the best protection against phishing and malware is being careful about what email attachments you open, keeping software updated and maintained, and installing a quality antivirus program.
- Take notice if you receive an email communication at a time of the month that is outside of your ordinary billing period. Note the email address your utility uses if you have opted to receive electronic bill notifications. Ensure the link in the notification goes to your actual account login page. If it goes to another website, the email is fraudulent. Delete it.
- Verify the authenticity of any unsolicited utility job-related emails or online utility employment listings by visiting the utility's online career board, reviewing its job posting page, or contacting the utility's human resources department. Utilities generally accept job applications through their website, email, or mail.
- If you are asked to interview for a utility job via online chat, stop communicating with the individual immediately, and report the scam to the utility.
- Do not deposit any checks received from online employment scammers. If you have deposited a check, notify your financial institution right away, and tell them that you may be a victim of an employment scam.
- Do not click on any links or attachments in any email unless you have verified the sender. If you do, you may be directed to a scam website designed to steal your personal information, or you might install malicious software onto your computer without ever knowing it.



SCAM ALERT
Xcel Energy

Scammers were reported going door-to-door offering inspection services and asking for entry into homes. The targeted homeowners denied them access and suspected the scammers either wanted the homeowners to purchase unnecessary products or services or planned to distract the homeowner while an accomplice stole valuables from the home.

Next Steps & Updates

In mid-2016, **Utilities United Against Scams** (UUAS) began as a consortium of electric, water, and natural gas utility companies, along with their respective trade associations, in the U.S. and Canada. To date, it has steadily grown to more than 100 members. Like this guide, UUAS aims to educate customers about scam tactics in hopes of ultimately putting an end to these types of crimes. UUAS is a first-of-its-kind, all-utility collaborative with a mission to combat utility scams by providing a forum for utility companies and associations to share data and best practices and to work together to implement initiatives to inform and protect customers.

In November 2016, the U.S. House of Representatives adopted a resolution designating the third Wednesday of November as "Utility Scam Awareness Day." The inaugural day was November 16, 2016, with the second annual day falling on November 15, 2017. The goal is to encourage utilities to use the day to raise awareness and knowledge among the industry, law enforcement, and the public regarding the threats posed, the techniques and tools used by scammers, and how to avoid them.

Helping to ensure that consumers have the information they need to avoid scams is an important and ongoing effort. Please help this initiative. Share the information provided in this guide and circulated by utilities, federal and state agencies, law enforcement, legislators, regulators, advocates, and other organizations. Encourage those in your community who believe they have been a victim of fraud to call their utility and relate the details of the scam.

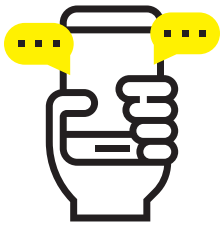
With your help, we can **#stopscams**.

"UUAS's mission is to combat utility scams by providing a forum for utility companies and associations to share data and best practices and to work together to implement initiatives to inform and protect customers."

Consumer Scam Alerts

The following alerts are provided for informational purposes. Community leaders are encouraged to photocopy and distribute these alerts for informational, noncommercial use.

Top 10 Impostor Utility Scams



HANG UP ON PHONE SCAMS

- **Disconnection Deception**
  Scammers call threatening disconnection of your utility service, demanding immediate payment by prepaid cards purchased at a local retail store (or credit card, debit card, bank draft, wiring money, etc.), and insisting you call them back with the card information to make payment. Your utility will send you one or more disconnection notices in the mail before disconnecting or shutting off your utility service, and they will offer several bill payment options without specifying the type of payment you need to make.

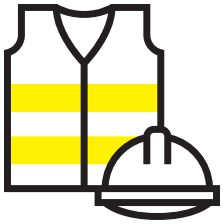
- **Bill Payment or Credit Con**
  Scammers may provide you with a phony account routing number for you to use to pay your utility bills, receive a credit, or obtain federal assistance. In exchange for personal information that can be used for identity theft, you may get a payment account number. If the number is entered during an online transaction, it may appear that your bill is paid, but no funds are actually paid to the utility, the account balance remains due, and you may be charged a returned payment fee by your utility.

- **Equipment or Repair Bogus Fee**
  Scammers call demanding a separate payment to replace or install a utility-related device or meter. If a utility needs to upgrade or replace a piece of equipment, it will contact you ahead of time as a courtesy. If there is a charge related to work on equipment you might own, it will typically be included in your monthly bill as the utility does not collect a separate payment for equipment or installation.

- **Overpayment Trick**
  Scammers call claiming you have overpaid your utility bill, and you need to provide personal bank account information or a credit card number to facilitate a refund. Your utility may apply any overpayments you have made to your utility account, allowing the credit balance to cover any future charges, or refund any overpayment by mailing a check.

- **Power Restoration Rip Off**
  Scammers call offering to restore power quickly or in a preferential order for immediate payment or an upfront "reconnection fee," typically in the aftermath of hurricanes and other severe storms causing widespread power outages. Utilities do not require payment to restore electricity, water, or natural gas service after a natural disaster or other related outage, though some utilities will accept in-person payment via check or phone payment after a disconnection for non-payment.

- **Smishing Scam**
  Smishing, short for SMS phishing, is a relatively new scam that attempts to trick mobile phone users into giving scammers personal information, which can be used for identity theft, via a text or SMS message. Scammers like smishing, as consumers tend to be more inclined to trust text messages. Utility companies typically do not text you unless you have signed up for a specific notification service offered by your utility.



SHUT THE DOOR ON IMPOSTOR IN-PERSON SCAMS

- **Contractor Con**
  Scammers posing as utility workers or contractors affiliated with your utility may knock on your door claiming to be employed or hired by the utility company to reset, repair, replace, or inspect your utility meter or other utility-related device. If a utility employee or authorized contractor needs access to your home, an appointment will be scheduled in advance, and proper identification will be provided for your review.

- **Home Improvement Huckster**
  Scammers posing as utility workers may appear unannounced at your front door offering a free energy audit, efficiency inspection, water quality or pressure testing, or some other service. These unsolicited intruders may be pitching unnecessary expensive products or attempting to steal items from you. Unless your utility company has notified you in advance, or you initiated a request for such a service, do not let them into your home or business.

- **Leak Lie**
  Scammers posing as utility workers may knock on your door claiming that there is a major gas or water leak in the area and that they need to come inside to check the pipes or lines. They may try to collect your personal information for later identity theft, or distract you to remove valuables from your home. A utility company will typically call you in advance to set an appointment for such a service.

DELETE SUSPICIOUS EMAIL SCAMS

- **Bogus Bills**
  Scammers send suspicious emails that appear to be a bill sent by your utility company, potentially featuring your utility's logo and color scheme. Do not click on any links or attachments in any email unless you have verified the sender. You may be directed to a scam website designed to steal your personal information, or you might install malicious software onto your computer without ever knowing it. Utility companies typically send bills by mail, unless you have opted to receive your bill by email.

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

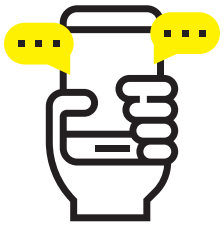
Never make a utility bill payment to anyone calling you on the phone, coming to your door (unless that is a verified bill payment method used by your utility company), texting you, or emailing you. Always call your utility company, at the number provided on your bill or on the utility's website, if you 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.

UTILITIES UNITED
AGAINST SCAMS

Tips to Avoid the Most Common Impostor Utility Scams



PHONE

- **Hang Up on Calls from Crooks**
  Hang up if you receive a call demanding immediate payment of a utility bill to avoid disconnection or shutoff. Never be fooled by a phony caller ID; never return a call to the call-back phone number provided by an unknown caller; and never provide any payment or personal information to a caller you do not know. If you have questions, call your utility company at its phone number on your monthly bill or the utility's website.
- **Keep Cell Phones Safe**
  Do not reply to text messages or click on links you receive from people you do not know, and if you receive a message from a friend, consider verifying they meant to send you the link before clicking on it. Never install apps from text messages, and if you have any doubt about a text message, exercise caution and do not open it. Several cellular service providers are now offering free scam blocking, and several smartphone apps are available for download.

IN-PERSON

- **Shut the Door on Scammers**
  Be suspicious of anyone who arrives at your home or business without an appointment demanding immediate payment, offering utility products or services, or requesting access to your dwelling to check your electrical wiring, water pipes, natural gas pipes, appliances, or other utility-related issues. Do not let unknown individuals into your home. If you have any questions, call your utility company.
- **Always Ask for Proper Identification**
  If you feel you are in personal danger, call 911. Always ask to see a company photo ID, and if you have doubts about a person at your door claiming to be from your utility, call your utility company to verify their information and work to be done before allowing them into your home or business.

INTERNET

- **Delete Suspicious Emails**
  If you receive an email that appears to be from your utility company that you are unsure about, delete it. Do not click on links, open attachments, download pictures, forward it, or respond to it. Be careful in providing information online. If you have questions about such emails, call your utility company.

- **Ensure Website Security**
  A secure website starts with "https://"—remember the "s" is for secure. In general, "http:" websites are vulnerable to attack. Remember the best protection against phishing and malware is being careful about what email attachments you open, keeping software updated and maintained, and installing a quality antivirus program. If you have any questions, call your utility company.

Reporting Impostor Utility Scams

Below is a list of suggested companies, agencies, and organizations you may wish to reach out to you if you think you have been contacted by a scammer or have been a victim of a scam:

YOUR UTILITY

Your utility can answer any questions you might have about your bill or account. Also, your utility may be working with law enforcement and other partners investigating criminals and assisting in shutting down scams. You should be able to find your utility's phone number on your monthly bill, on your utility's website, or through your phone's directory assistance.

Entity	Website/Phone Number	Purpose
Local and State		
Local Law Enforcement	▪ www.usacops.com ▪ 311 or 411 (non-emergency) ▪ 911 (emergency)	If you feel you are in immediate danger, call 911. If you want to report a crime or suspected crime, contact your local law enforcement.
State Attorney General Office	▪ **National Association of Attorneys General** – www.naag.org	Your state attorney general likely has a consumer protection division that accepts consumer complaints and inquiries about fraud.
State Consumer Protection Agency & State Utility Consumer Advocate	▪ **State Consumer Protection Agency** – www.usa.gov/state-consumer ▪ **National Association of State Utility Consumer Advocates** – www.nasuca.org	Your state may have an agency that takes and investigates consumer complaints. Many states have agencies or divisions of agencies dedicated to assisting utility consumers.
State Utility Commission	▪ **National Association of Regulatory Utility Commissioners** – www.naruc.org	All states have an entity with oversight authority over electric, water, and natural gas companies, and most have consumer protection authority.

Entity	Website/Phone Number	Purpose
Federal		
Federal Bureau of Investigation (FBI), Internet Crime Complaint Center (IC3), or Local Office	▪ www.ic3.gov/complaint ▪ www.fbi.gov	IC3 collects information from consumers who believe they have been the victim of an internet crime. The FBI asks consumers to contact their local FBI office to submit a tip electronically.
U.S. Computer Emergency Readiness Team (US-CERT)	▪ www.us-cert.gov/report-phishing ▪ phishing-report@us-cert.gov	US-CERT allows you to report phishing messages and website locations.
U.S. Postal Inspection Service (USPS)	▪ www.postalinspectors.uspis.gov ▪ www.deliveringtrust.com ▪ 800-372-8347	USPS allows you to report mail fraud and also provides information about how to protect yourself from mail fraud.
Social Security Administration (SSA)	▪ www.ssa.gov ▪ 800-269-0271	If you believe someone is using your Social Security number, contact the SSA fraud hotline.
Federal Trade Commission (FTC)	▪ www.consumerfinance.gov/complaint ▪ 855-411-CFPB (855-411-2372)	If you have been a victim of a scam and you are having trouble getting a response from your financial institution, you may wish to call the FTC.
Federal Communications Commission (FCC), Consumer Complaint Center	▪ www.consumercomplaints.fcc.gov ▪ 888-CALL-FCC (888-225-5322)	By filing a consumer complaint with the FCC and telling your story, you contribute to federal enforcement and consumer protection efforts on a national scale and help them identify trends.

Entity	Website/Phone Number	Purpose
Other Assistance		
Credit Reporting Agencies (CRAs)	▪ **Equifax** – www.equifax.com – 800-525-6285 ▪ **Experian** – www.experian.com – 888-397-3742 ▪ **TransUnion** – www.transunion.com – 800-680-7289	If you think you have been a victim of identity theft, you may wish to contact the CRAs, obtain a copy of your credit report, and ask that an alert be placed on your credit record requiring that you be contacted before credit is extended using your name/Social Security number.
Better Business Bureau (BBB), Scam Tracker	▪ www.bbb.org/scamtracker/us	If you have experienced a scam, you can tell BBB about it, help them investigate the fraud, and warn others by reporting what you know. The free interactive tool, Scam Tracker, offers a map showing where scams are being reported.
AARP Fraud Watch Network (FWN)	▪ www.aarp.org/money/scams-fraud/fraud-watch-network ▪ 877-908-3360	The FWN provides you with access to information about identity theft and the latest scams, lets you to sign up for free Watchdog Alerts to stay up to date on scammer tactics, and allows you to share your story and receive assistance from its call center.

Entity	Website/Phone Number	Purpose
Payment Providers		
Prepaid Card Companies & Wire Transfer Companies	▪ **Green Dot** – www.secure.greendot.com/customersupport/report-fraud – 866-795-7597 ▪ **MoneyPak** – www.moneypak.com/security – www.attheregister.com/moneypak/profile/refund/request ▪ **Reloadit** – www.reloadit.com/ProtectYourMoney – 888-633-9434 ▪ **Vanilla** – www.myvanillacard.com/faq.html – 855-686-9513 ▪ **iTunes Gift Cards** – www.support.apple.com/itunes-gift-card-scams – 800-275-2273 ▪ **Western Union** – www.westernunion.com/us/en/send-money/app/report-fraud – 800-448-1492 (Fraud Hotline) ▪ **MoneyGram** – www.corporate.moneygram.com/compliance/fraud-prevention/report-fraud – 800-926-9400	Using untraceable prepaid cards or wiring money to a scammer makes it nearly impossible to get back. Once you share the number on the card, the money is gone. In some rare cases, fraud victims may be able to call a customer service number immediately to stop a payment from being deposited to a card, preventing a scammer from profiting off the potential victim.

UTILITIES UNITED
AGAINST SCAMS

givens energy
consulting. education. advocacy.

www.UtilitiesUnited.org | @UtilitiesUnited | @U_U_A_S