

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.