# AVOIDING UTILITY SCAMS

## WHAT TO LOOK FOR AND HOW TO PROTECT YOURSELF

# ABOUT UTILITY SCAMS

Utility scams occur when thieves pose as your local utility company to steal personal information and empty bank accounts. These scams can happen over the phone, by text message, from in-person visits, or through email. Scammers use the trust that utilities have created by delivering reliable services in order to defraud people. They often take advantage of confusion and use scare tactics to place people in an uncomfortable position, with the elderly and non-English speakers as prime targets. It's important to learn the signs of utility scams to protect yourself and the ability of your utility workers do their jobs. This guide will help you recognize utility scams for what they are and learn how to keep yourself safe. If you think you might be the target of a scam, call the phone number on your utility bill to ask about the situation. If you are in danger, call 911. Never provide any personal or bank information if you are unsure whom you are speaking with.



# SIGNS IT'S A SCAM

Pay attention to these signs of a utility scam when dealing with supposed utility workers:

- Calls from unofficial phone numbers or calls demanding immediate action. A utility will always be fine with your saying you will call them right back from the number on your bill.
- Unexpected emails or emails requesting information.
- Unscheduled visits.
- No company badge or identification.
- Workers who seem rushed or insist that something be done immediately.
- Requests for unusual payment methods, like prepaid cards or bitcoin or other cryptocurrencies.

In addition, utility shutoffs do not happen immediately. Your utility provider will notify you in advance of a future shutoff, not show up at your door demanding payment. One of utility scammers' most common tools is the threat of a shutoff, but that process takes several steps. You can always call the number on your bill to verify the status of your account.


# PHONE SCAMS

Phone calls are the most common way scammers attempt to gain information, demand money, or sign you up for fraudulent programs. Never provide information or agree to anything about your bill when you are talking to someone who has called you. Always return the call using the number on your utility bill or the utility website. Scammers change their tactics often, so staying alert is often the best defense. Here are some tactics used by phone scammers:

- **Demanding money.** Using the threat of a shutoff to scare you, scammers demand payment of a bill using unusual methods like a wire transfer or prepaid credit card.
- **Extracting information.** Scammers may try to get elements of your account, such as an address or account number, from you, but the real utility service already has this information on file.
- **Refund scams.** A trick popular with scammers is claiming that your bill has been overpaid and they want to give you a refund but need your personal information in order to send you money. Your utility service will credit any extra payment to your account automatically.
- **Power restoration.** When a power outage occurs, some scammers take advantage by claiming to be able to restore your service faster if you make a payment. This is never the case, as utility services don't make preferential decisions.
- **Federal assistance programs.** The Low Income Home Energy Assistance Program (LIHEAP) is an important government program that helps low-income customers with their utility bills. In the past, utility scammers have called people demanding sensitive information to see if they qualify. You can sign up for the program through your state or local government or an authorized intake center—do not provide information to someone calling your home about the program. If you need help finding your local Low-Income Energy Office, call the National Energy Assistance Referral (NEAR) toll-free at 1-866-674-6327 or TTY 1-866-367-6228 for energy assistance referral. Or, email NEAR at energyassistance@ncat.org.

Scammers request payment immediately, and they're often insistent and encourage you to pay using a prepaid credit card. If the caller will not tell you what company they work for, take that as a sign you are being scammed. Hang up and call your utility company using only the number listed on your bill to verify what the supposed worker said.

With more people becoming aware of phone scams, criminals have turned to texting to gain personal information. If you receive a text from someone claiming to be your utility provider, do not send any information. Most utility services will text you only if you have signed up for texts under a specific notification plan.

Scammers may also request personal information to

- update your account file,
- qualify you for federal assistance programs, or
- give you a refund.

Call your utility company to verify any request for information, and never give out financial or personal information when taking a call.

# IN-PERSON SCAMS

Utility scammers go to great lengths to look the part for in-person scams. They may even be wearing clothing with the logo of your utility provider or holding official-looking documents. But if you are not expecting an in-person visit to your home from your provider, do not allow them to enter. Immediately contact your utility service to check if the person is authorized by the provider. In-person utility scammers tell a variety of stories to try to enter your home or property.

These include the following:

- **Equipment readings/replacement.** The scammer may ask to come inside to "fix" a meter or gather a reading and tell you that there is a fee for this service. But all repair work should be scheduled in advance with your provider and should not come as a surprise.
- **Home improvement offers.** Scammers may offer you free inspections or audits for your home, which may sound like a good deal. But their "findings" may result in your having to purchase an expensive and unnecessary item, or they may be exploring your home to plan for a future break-in.
- **Gas/water leaks.** Scammers may approach your home and claim there is a major leak in the area and they need to come in and check to see if it is affecting your home. You should verify with your provider whether there is a leak. In emergency situations you may be contacted by your provider in advance of any employees appearing in the neighborhood.

Again, scammers' goal is often to steal your valuables immediately or gain information that will help them with future burglaries. Call your utility before allowing any unscheduled entry.

Scammers may ask for personal information, including social security numbers, credit card information, and answers to personal questions, in order to commit identity theft. Do not provide any of this information to unscheduled visitors.

They may have things with them that look official. Here are some examples:

- Clipboards
- Utility badges
- A hard hat
- Magnetic vehicle stickers
- A handheld radio

It is easy for scammers to acquire such things, so always verify with your utility company, using the number on your bill, before answering questions or granting entry to your home.

# INTERNET SCAMS

Scammers can send fake bills or shutoff notices through email. These emails may look official and may even have your utility company's address on them. Submit payments only through the utility's website, by using the provided billing address, or by calling the official number on your utility bill. Never pay through a provided link in the email, as this could lead to the installation of phishing software that makes your personal information vulnerable to attack. Avoid submitting personal information on utility web forms that aren't at your utility company's official website.

Often, scammers' emails are very similar to your utility company's emails but have small mistakes in them that can help you determine they are fakes. Here are some things to look for if you have any questions about an email:

- **Watch for errors.** Emails from scammers often contain spelling mistakes (your name or the company name may be wrong) and odd formatting (oversized words, incomplete images). These are signs of a fake account.
- **Check the address.** The email address that the scammer's email comes from may be close to the one your utility uses, but it will not exactly match the email address provided on your bill.
- **Don't click or open.** Scam emails often urge customers to click on links or open attachments, but these elements are a great way for scammers to install tracking software on your computer. Do not interact with any email you feel is suspicious.
- **Ignore demands.** As with phone scams, email scammers may demand immediate payment or threaten shutoffs via email. They may urge you NOT to call your provider and to click on a link instead. You should delete any email that asks for large payments and contact your utility provider.

Following good internet and email practices can keep you safe from scammers. If there is any doubt, hit delete. Call your utility company about any suspicious emails before providing any information and never respond to the emails. Your service provider may provide you with an address where you can forward potential scam emails for investigation by authorities.

Another internet scam that utilities have seen recently involves scammers impersonating utility employees on job-posting websites. They offer work-from-home jobs and then request that the victim deposit fraudulent checks in their personal account and use the money to write checks to the scammers. Research any job inquiries that arrive unsolicited and confirm that the person actually works for the utility. If they don't want to meet for an in-person interview at the utility's office, it's a sign that it's a scam.

# PROTECT YOURSELF

Now that you know about the various utility scams, here's how you can protect yourself, your loved ones, and your neighbors from falling victim to criminals.

## DON'T RUSH INTO ACTION

No matter how insistent a caller or visitor is, utility companies do not make immediate decisions on the status of your account over the phone or in person. Take the time to call the proper number on your bill and verify your account status.

## ASK THE RIGHT QUESTIONS

Ask for the following when greeting a utility worker on the phone or in person:

- Your account number
- Your last payment amount and date
- Their employee identification number

If they don't have this information, don't speak with them, and call your utility.

## PROTECT YOUR INFORMATION

Never provide personal information other than your name during a home visit or while taking a phone call from your utility company. The company has the rest of your information. Provide information only when calling the number on your bill when it is requested for identification purposes.

## CUT OFF COMMUNICATION

If you suspect the utility worker is lying at any time during a phone call or home visit or through email, stop communicating immediately. Utility workers are trained to be polite and helpful during customer interactions, so if the person you are speaking with becomes demanding or threatens you in way, act!

- Hang up the phone
- Shut and lock your door
- Stop responding via email

Immediately call your service provider and let them know you were the target of a scam attempt.

## VERIFY WITH YOUR UTILITY

Double-check using an official utility number before giving information or money to a worker. Workers who try and prevent you from ending a call or calling to verify with the company during an interaction are almost always scammers. Call the number on your official bill and ask about potential charges.

## MAKE ONLY OFFICIAL PAYMENTS

Protect yourself by submitting utility payments through official channels. Use your account on the utility website, make payments with the phone number on your bill, or send a check through the mail to the address on the bill.

## NEVER PAY USING ANY OF THESE:

- Prepaid credit cards
- Wire transfers
- Bank transfers
- Cash

# WHAT TO DO AFTER A SCAM

## IF YOU ARE IN IMMEDIATE DANGER:

Talk with local law enforcement.

- Dial 911 for help if you believe you are in immediate danger. For example, if a fake worker is in your home or trying to break in, call for help right away.
- Call 311 to report in-person scammers to local police to help protect your neighborhood.

## IF YOU GAVE OUT FINANCIAL INFORMATION:

Talk with your financial institution right away. Report the fraud to your institution immediately and seek advice to protect yourself. The following are some recommendations that your financial institution might make:

- Cancel credit cards if you provided your card information to the scammer.
- Stop bank payments if you revealed your account number.
- Cancel checks in order to stop one or more mailed checks from being cashed.

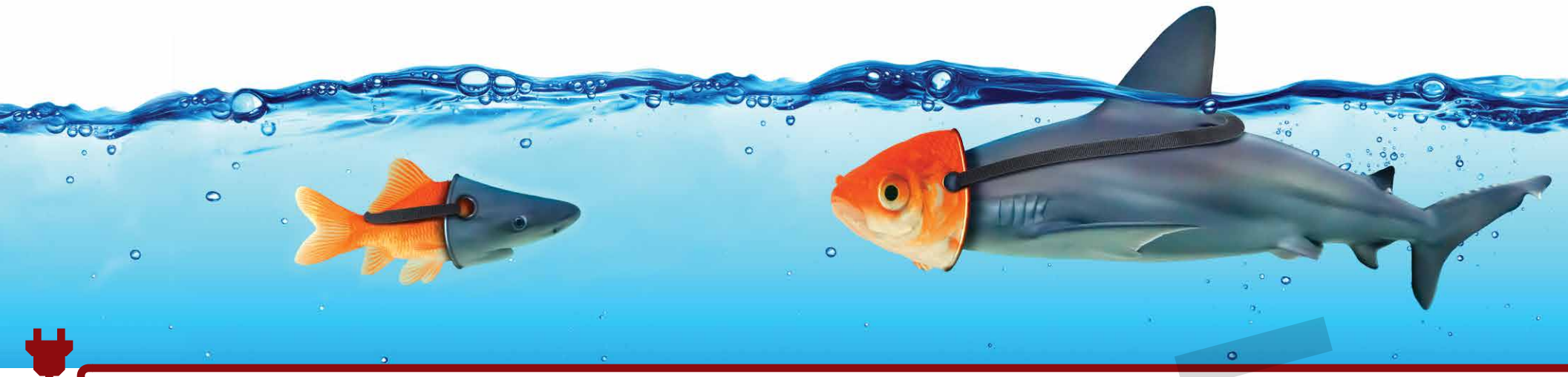
## CALL YOUR UTILITY COMPANY

Talk with your utility company using the number on your bill to report the scam or verify the charge. Sharing the information gives providers across the country the chance to alert customers to the newest tactics criminals attempt to employ to steal personal or financial information.

## SUBMIT OFFICIAL SCAM REPORTS

File official reports to help agencies track and stop scammers.

- Report the scam to the Better Business Bureau. (www.bbb.org/scamtracker/us)
- File an FCC complaint. (www.consumercomplaints.fcc.gov or 855-411-2372)
- Report an internet scam to US-CERT (www.us-cert.gov/report-phishing) and IC3 (www.ic3.gov/complaint)
- Submit a report of social security number fraud (www.ssa.gov)



# RESOURCES

Get access to helpful resources for dealing with utility scams.

## ATTORNEY GENERAL'S OFFICE
(Report to your state's consumer protection division.)
www.naag.org

## CONSUMER PROTECTION AGENCY
(Submit fraud complaints for investigation.)
www.usa.gov/state-consumer

## FEDERAL TRADE COMMISSION
(Contact the FTC when financial institutions don't respond to reports of fraud.)
www.consumerfinance.gov/complaint
855-411-2372

## INTERNET SCAMS
U.S. Computer Emergency Readiness Team (US-CERT)
(Report fraudulent emails here.)
www.us-cert.gov/report-phishing
Internet Crime Complaint Center (IC3)
(Report internet crimes here.)
www.ic3.gov/complaint

## BETTER BUSINESS BUREAU
(Report utility fraud to warn others here.)
www.bbb.org/scamtracker/us

## CREDIT BUREAUS
(Monitor your credit reports and get alerts here.)

Equifax
www.equifax.com
800-525-6285

Experian
www.experian.com
888-397-3742

TransUnion
www.transunion.com
800-680-7289

# REFERENCES


**UTILITIES UNITED AGAINST SCAMS**
https://www.utilitiesunited.org

**FEDERAL TRADE COMMISSION**
**EMPOWER YOURSELF AGAINST UTILITY SCAMS**
www.consumer.ftc.gov/blog/2018/09/empower-yourself-against-utility-scams

**AARP - UTILITY SCAMS**
www.aarp.org/money/scams-fraud/info-2019/utility.html