CyberGuardLab

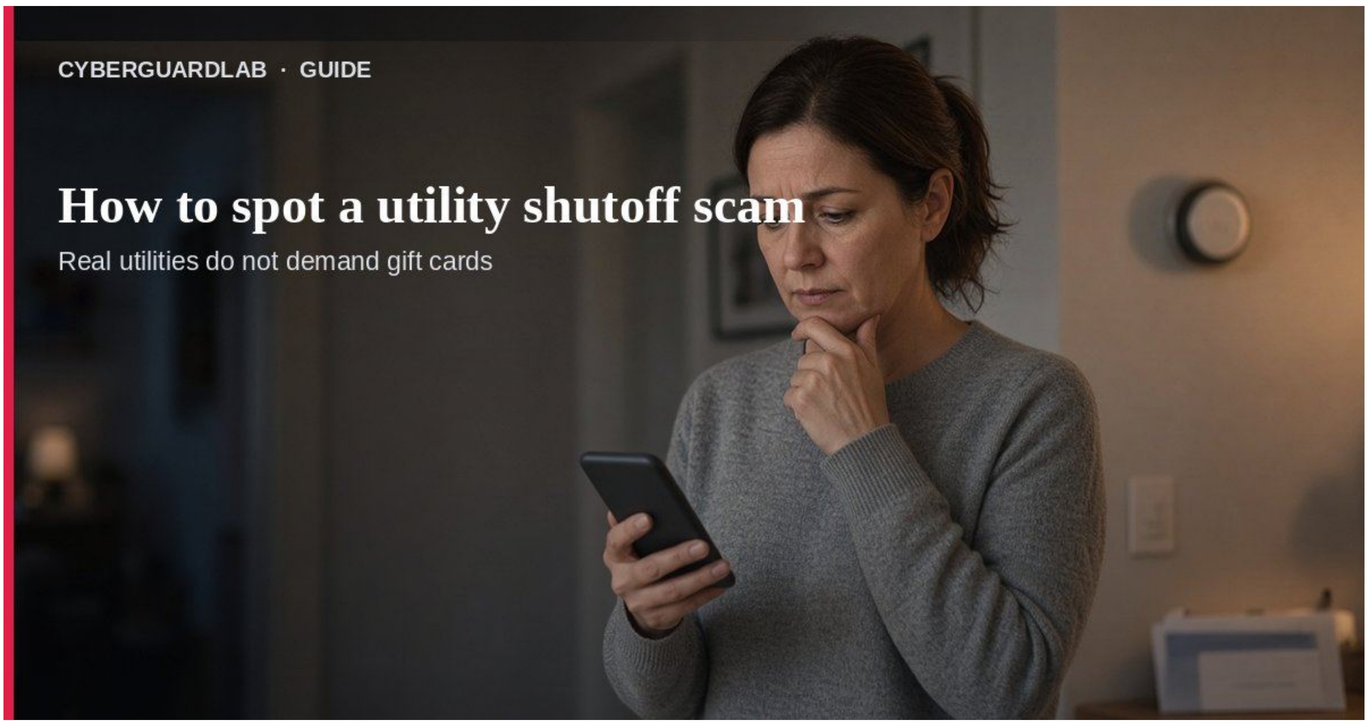
Household antivirus, explained

cyberguardlab.com

How to spot a utility shutoff scam

https://cyberguardlab.com/blog/utility-shutoff-scam

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.



A utility shutoff scam is when someone pretends to be your electric, gas, water, or other utility company and threatens to cut service today unless you pay immediately-usually by wire, crypto, payment app, or gift cards. Per FTC guidance, unexpected calls, texts, emails, or door visits that demand same-day shutoff payment on the spot are a scam. Real utilities do not run that playbook. This guide is about utility shutoff pressure, not gift card payment scams in general, spam texts broadly, or phishing email basics. You do not need antivirus to pause and call the number on your own bill.

1. How utility shutoff scams usually work

From FTC utility-impersonation guidance:

* Sudden threat - "We will shut off power/gas/water in one hour unless you pay now."
* Any channel - Phone, text, email, or someone at the door with a fake badge or clipboard.
* Irreversible payment demand - Gift cards, wire transfer, cryptocurrency, or payment-app sends-not the methods your bill lists.
* Spoofed identity - Caller ID or email may look like your real utility.
* Account "confirmation" - They ask for your account number, SSN, or banking details "to keep service on."

2. What real utilities generally will not do

* Demand same-day shutoff payment on the spot with no prior paper trail you already know about.
* Require gift cards, crypto, wires, or payment apps for past-due balances.
* Force you to use only the number or link they just gave you instead of the contact info on your bill or your utility's official site.
* Send a stranger to collect cash at the door as the only way to avoid shutoff.

If you truly are past due, your utility's legitimate notices and payment options will still match the company you already do business with-not a panic script from a stranger.

3. What to do when you get the shutoff threat

* Do not pay on the spot - Especially not with gift cards, wire, crypto, or payment apps.
* Hang up / close the message / end the door conversation - Polite exit is enough.
* Contact the utility using the number on YOUR bill or the official site you type yourself-not the caller's number or a link in the text.
* Ask whether any shutoff is actually scheduled - Many households learn there is no pending disconnect.
* Warn household members - These scripts often hit older relatives and people who answer every call.

4. If you already paid or shared account details

* Contact your bank, card issuer, or payment provider immediately and explain you paid a suspected scammer.

* Follow FTC recovery steps for the payment method you used (What to do if you were scammed).
* Tell your real utility that someone may have your account information.
* Report at ReportFraud.ftc.gov.
* Also report to your utility's fraud team and your state attorney general consumer office when applicable.

FAQ

How do I spot a utility shutoff scam?

Unexpected shutoff-in-an-hour pressure plus demand for gift cards / wire / crypto / payment apps is the FTC red-flag combo. Real utilities do not demand that kind of same-day spot payment.

The text said my power is going out-should I click the "pay now" link?

No. Use the phone number or website printed on a recent bill. Treat surprise spam texts and phishing-style links as hostile until proven otherwise.

What if I'm actually behind on a bill?

Still pay only through your utility's official channels. A stranger's panic deadline does not replace your bill's payment instructions.

Is this a tech-support or antivirus problem?

Usually no-it is payment and impersonation pressure. See tech support phone scams only if they also try to take remote control of a computer.

Where do I report it?

ReportFraud.ftc.gov, your utility, and your state AG. Step-by-step FTC reporting: how to report a scam to the FTC.

If you still want a paid suite

Stopping a utility shutoff scam does not require paid antivirus. Microsoft Defender is a valid buy-nothing choice for many Windows households. What actually helps is calling the number on your bill and refusing irreversible payments. If the household later wants multi-device paid protection, use only these on-site paid links: TotalAV (paid link), Norton (paid link), Bitdefender (paid link), McAfee (paid link), Avast (paid link).

Sources

* Scammers Pretend to Be Your Utility Company (FTC)
* What to Do If You Were Scammed (FTC)
* ReportFraud.ftc.gov (FTC)

Also read

* How to spot a gift card scam
* How to stop spam text messages
* How to spot a phishing email
* How to spot a tech support scam phone call
* How to report a scam to the FTC
* How to spot a grandparent emergency money scam