



PUBLIC

THREAT INTELLIGENCE SNAPSHOT · UTILITIES

Utility Impersonation Threats

The most common utility scam lure Doppel confirmed is a phone number: fake customer-service lines planted where customers search for help, so the victim makes the call.

VERTICAL

Utilities (electric,
gas, water)

**REPORTING
WINDOW**

01APR2026 to
15OCT2026

ISSUED

15OCT2026

PREPARED BY

Josh Bartolomie
Doppel SECR

01 EXECUTIVE SUMMARY

Utility impersonation often starts with the customer reaching out. Fake customer-service phone numbers were the single largest lure theme in Doppel's confirmed utility impersonation data. Scammers post "pay your bill by phone" and "customer service number" pages on free hosting platforms, public forums, site builders, number directories, and document-sharing sites, then wait for a customer searching for help to dial. Only about 2% of those fake-number pages sat on a domain carrying the utility's name, and the same unofficial numbers recur across channels, some advertised as the payment line for several unrelated companies at once.

Bill payment, account login, outage, and energy-assistance themes follow behind fake support numbers. A parallel fraud economy offers editable fake utility bills, likely for proof-of-address fraud, while documents on public document-sharing sites, many of which appear to be real customer bills, made up roughly one in three confirmed URLs. In October, one operator registered lookalike domains for two different utilities 11 minutes apart as the heating season began.

The posture is **phone-number-driven, off-domain, and multi-channel**. About 31% of confirmed impersonation sat off web pages entirely, on Facebook, LinkedIn, YouTube, Facebook ads, mobile apps, marketplaces, and phone numbers. Shutoff threats and gift-card demands arrive by phone and text.

LEADING LURE

**FAKE
SUPPORT
NUMBERS**

Utility scammers plant fake support numbers where customers look for help, and the victim places the call.

The official number on a customer's bill is the strongest defense, and every fake number on a search result, forum post, free-hosted page, or social profile competes with it. Protection has to reach where customers search, well beyond lookalike domains.

TOP LURE

Fake support numbers Largest confirmed lure theme

NON-WEBSITE CHANNELS

31% Social, ads, apps, marketplaces, phone

OPERATOR SPEED

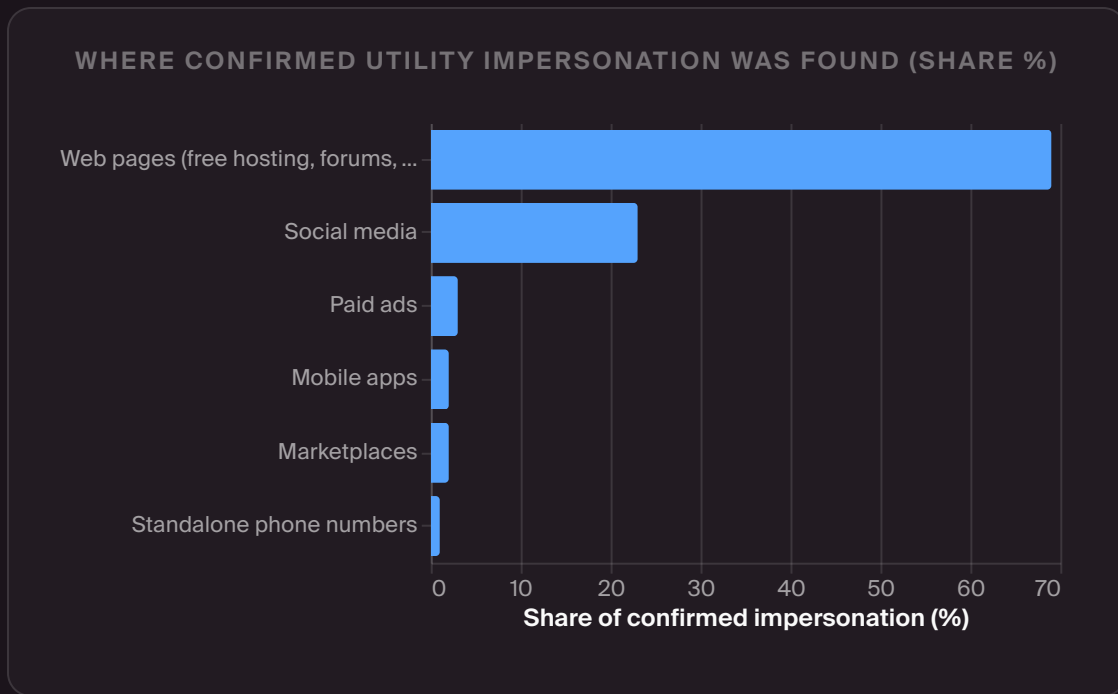
11 min Between lookalikes for two utilities

MEDIAN LOSS

\$400 Utility scams, 2025 (BBB)

02 TOP SOURCES OF ACTIVITY

Web pages carried most confirmed utility impersonation, and almost a third of it lived elsewhere. The web-page share covers far more than lookalike domains: pages on site builders such as Google Sites, templated pages on free hosting platforms such as Tencent EdgeOne, Cloudflare Pages, and Vercel, posts and profile pages planted on public forums and job boards, and documents on public document-sharing sites. Water utilities face the same search-led pattern: a large city water department warned that a lookalike bill-pay site appeared in regular search results when customers tried to pay ([city water department alert](#)), and one fake support number Doppel tracked was also posted as the pay-by-phone line for a city water utility.



Each item is counted once, by where it was found. A fake support number posted on a web page counts as a web page, which is why the standalone phone-number share is small even though fake support numbers are the leading lure.

On social media, Facebook carried 43% of confirmed social activity, LinkedIn 36%, and YouTube 10%, followed by Instagram, X, Telegram, TikTok, and WhatsApp. Facebook pages posed as the utility, some linking to forms that harvest customer data. Nearly all confirmed LinkedIn activity was fake profiles claiming to work for a utility, a persona that could lend credibility to a recruiting or support approach. Paid ads ran almost entirely on Facebook, from pages styled as energy news outlets, solar installers, electricians, and heating and cooling companies. Marketplace listings sold editable utility bill templates, and app activity was unofficial download mirrors plus a sideloaded "outage" app.

Shutoff threats and demands for gift cards, cryptocurrency, or payment apps rarely appear on a web page; they arrive as phone calls, texts, and in-person visits, the tactics [Utilities United Against Scams](#) lists first. One large West Coast utility reports a newer variant that pairs a shutoff call with a barcode or QR code sent by text or email for the customer to pay at a store. Its customers lost more than \$211,000 by July 2026, an average of \$969 per victim against \$590 in 2025 ([KTVU](#)). The web infrastructure in this report can supply what those calls need: the fake numbers customers dial, the lookalike portals that collect account details, and the documents that make a caller sound informed.

03 LURE THEMES

Fake support numbers led every other lure theme. Relative frequency is indexed to the most common theme (fake support numbers = 100), and one page can carry several themes.

RANK	LURE THEME	RELATIVE FREQUENCY	WHAT IT LOOKS LIKE
1	Fake customer-service phone numbers	100	"Pay your bill by phone" and "customer service number" pages listing an unofficial line
2	Bill payment and past-due	74	Lookalike "pay my bill" and guest-pay portals, free-hosted payment pages
3	Account login	57	Working login forms imitating the utility's customer portal
4	Outage and storm	29	Fake outage maps, outage-report pages, and a sideloaded outage app
5	Energy assistance	28	Pages and forms trading on bill-assistance and hardship programs
6	Solar, EV, and efficiency offers	10	Utility-branded solar and efficiency pitches, often via social ads
7	Refunds, rebates, and credits	6	Rebate and bill-credit offers

Refund and rebate lures were rare in Doppel's confirmed utility data, while utilities are warning about them on social media: one Canadian utility has flagged AI-generated Facebook ads showing fake bills and promising bill credits ([fraud alert](#)). The reward pitch relies on the same urgency as a shutoff threat, so the same verification step defeats it.

Two further categories enable fraud without being lures:

- **Editable fake bill templates** appeared nearly as often as fake support numbers, offered as Word and PDF documents on template shops and on unrelated websites, including what appear to be compromised small-business sites. A convincing utility bill is a standard proof-of-

address document, so these templates most likely support identity and account-opening fraud elsewhere.

- **Documents on public document-sharing sites** made up roughly one in three confirmed URLs. Many appear to be real customer bills showing names, service addresses, and account numbers, which is a data-exposure risk and gives a scammer the details that make a shutoff call believable.

04 WHAT A DOMAINS-ONLY VIEW MISSES

ACROSS DOPPEL TELEMETRY, ALL INDUSTRIES

About **three in four impersonation campaigns (74%)** had no domain component at all, and **61% of the campaigns that did touch a domain also ran on other surfaces.**

The utility data shows the same pattern. Only about 2% of confirmed fake-number pages sat on a domain carrying the utility's name or a typo of it; the rest lived on free hosting page farms, forum posts and profile pages, site builders, number directories, document-sharing sites, and phone and messaging accounts. The number itself travels from one surface to the next. Watching lookalike registrations catches the October portals; it does not catch the fake support number on a public forum, the "pay by phone" page on a site builder, or the Telegram account pointing to a WhatsApp line.

05 HOW THE INFRASTRUCTURE WORKS

SEO page farms on free hosting. In June and July 2026, dozens of templated pages appeared across dozens of throwaway subdomains on a free hosting platform, with titles such as "contact number," "outage map by zip code," "energy assistance," and "bill pay log in" for a specific utility and service area. The pages exist to rank in search for the exact phrases a customer types when looking for help.

One operator, two utilities. On 11OCT2026, two lookalike domains impersonating two different utilities in different regions were registered 11 minutes apart through the same registrar and resolved to the same IP address. Both paired the utility's name with "energy power." Within three days, what appears to be the same operator registered further "energy power" and "electric power"

domains through the same registrar on adjacent hosting, one carrying a working login form imitating a utility's bill-pay and account portal. The timing coincides with the start of the heating season.

Aged typosquats and number directories. Older typo domains, some registered more than a decade ago, sit parked and monetized, while fake "customer care number" directory sites on shared hosting list unofficial numbers for more than one utility.

06 MULTI-CHANNEL CASE STUDY

A fake support number operation against a large US electric and gas utility. Doppel investigated confirmed impersonation of the utility on more than a dozen platforms in the window, tied together by a "pay your bill by phone" lure built on fake support numbers.

1. **The bait.** Doppel observed site-builder pages, titled along the lines of "pay my bill by phone," listing an unofficial toll-free number, which also appeared in a post planted on a public community forum. A second number appeared on an unrelated website and on document-sharing pages describing how to "pay without logging in." A third ran through forum threads and a cluster of public profile pages, repeated throughout each page as the way to pay.
2. **The reach and the harm.** Doppel found one of these numbers posted on a single public forum as the bill-pay line for at least nine other US utilities, the signature of a fake-number operation serving many brands at once. One customer reported calling the third number in September 2026 and paying what they believed was their utility bill.
3. **The pivot.** Doppel traced one free-hosted page to a further unofficial phone number tied to the same lure.
4. **The messaging channel.** A Telegram account presenting itself as the utility, which has no Telegram presence, was tied to an international WhatsApp number.
5. **The portal.** In October, the cross-utility operator registered lookalike domains for this utility, staged to resemble its outage-report and bill-pay functions.

Around the core lure, the same utility saw impersonating Facebook pages, fake employee profiles on LinkedIn, branded Facebook ads, unofficial app mirrors, and customer bills exposed on document-sharing sites. No single surface held the whole operation: a customer could meet it through a search result, a forum post, a social profile, or a messaging app, and every path ended at a number the utility does not own.

07 KEY FINDINGS AND PRIORITY ACTIONS

Utilities United Against Scams, a coalition of more than 150 US and Canadian electric, water, and natural gas utilities, tells customers to call only the number on a recent bill or the official website. Scammers compete with that number on every surface in this report.

FAKE SUPPORT NUMBERS ARE THE LEADING LURE

Fake customer-service numbers were the single largest confirmed lure theme, posted on free-hosted pages, forums, directories, and document-sharing pages, and reused across unrelated companies.

- **Impact:** A customer who searches for a payment line can reach a scammer before reaching the utility, and the scammer controls the conversation from the first ring.
- **Do:** Print the official payment and support numbers prominently on bills, the website, and the app; train call-center staff to ask anyone reporting a scam where they found the number; and send every unofficial number customers report to the brand protection team.

IMPERSONATION REACHES CUSTOMERS BEYOND WEB PAGES

About 31% of confirmed impersonation ran on Facebook, LinkedIn, YouTube, Facebook ads, apps, marketplaces, and phone numbers, and across Doppel telemetry three in four campaigns never touch a domain.

- **Impact:** A program scoped to lookalike domains leaves the social, ad, app, messaging, and phone channels where customers also meet a fake utility.
- **Do:** Publish one official list of the utility's social accounts and support channels so customers can check a profile in seconds, and confirm the brand protection program covers every surface in this report.

OPERATORS TARGET SEVERAL UTILITIES AT ONCE, TIMED TO THE SEASON

One operator registered lookalike domains for two utilities 11 minutes apart as the heating season began, then added siblings within three days, one with a working login form.

- **Impact:** A lookalike portal can be live and collecting logins within days of registration, timed to the season when bills and shutoff anxiety rise.
- **Do:** Brief customer-service and fraud teams before each heating and cooling season, and give front-line staff a fast internal path to report a suspicious site a customer mentions.

BILLS ARE BOTH A TARGET AND A COMMODITY

Editable fake bill templates appeared nearly as often as fake support numbers, and documents on public document-sharing sites, many appearing to be real customer bills, made up roughly one in three confirmed URLs.

- **Impact:** Exposed bills give scammers the account numbers and amounts that make a shutoff call believable, and templates enable proof-of-address fraud against banks and other businesses.
- **Do:** Tell customers never to post a bill online, and route reports of exposed customer documents to the privacy team to assess whether notification is needed.

SHUTOFF THREATS ARRIVE BY PHONE AND TEXT, AND LOSSES ARE HIGH

Shutoff threats and gift-card, crypto, and payment-app demands reach customers by call and text. The median reported utility scam loss was \$400 in 2025, more than four times the \$93 median across all scam types ([BBB](#)).

- **Impact:** The web infrastructure in this report can supply the numbers and personal details that make those calls convincing.
- **Do:** State plainly how the utility does and does not collect payment, and repeat it on bills, in the app, and at the start of each heating and cooling season.

08 WHAT TO TELL CUSTOMERS

For Utility Scam Awareness Day messaging, the [UUAS "Slow Down, Verify, Stop the Scam"](#) framework maps directly onto the tactics in this report.

STEP	CONSUMER MESSAGE	SCAM IT DEFEATS
Slow Down	Utilities reach out more than once and offer help before disconnecting a past-due account. Hang up on any call that creates panic, and ignore any surprise refund, rebate, or bill credit that needs action right now.	Shutoff threats, refund and rebate lures
Verify	Get the utility's phone number from a recent bill or by typing the utility's official web address. Do not trust a number from a search result, a forum post, a social media page, or a text message, even one that looks official.	Fake customer-service numbers, lookalike login pages, fake support accounts on Telegram and WhatsApp
Verify	Legitimate utilities never demand payment by gift card, cryptocurrency, prepaid debit card, or a third-party payment app. A barcode or QR code sent by text after a threatening call is a known scam pattern.	Gift-card, crypto, and barcode payment scams
Stop the Scam	Do not engage. Hang up, close the page, or delete the message, then report it to the utility, local law enforcement, and the FTC.	Every variant
Stop the Scam	Never post a utility bill online. Bills carry the account number and address scammers use to sound legitimate.	Exposed bills that make scam calls convincing

Findings are based on Doppel telemetry across a global customer base, with strongest coverage in North America. Utility figures reflect confirmed impersonation of electric, gas, and water utility brands, predominantly electric and gas, observed 01APR2026 to 15OCT2026.



Our mission is to protect the world from social engineering attacks every day. Our AI-native defense anticipates deception and eliminates threats.

1B+ INDICATORS ANALYZED DAILY

300+ TRUSTED CUSTOMERS

doppel.com

Prepared by Doppel SECR - Social Engineering Counterintelligence & Research