CyberGuardLab

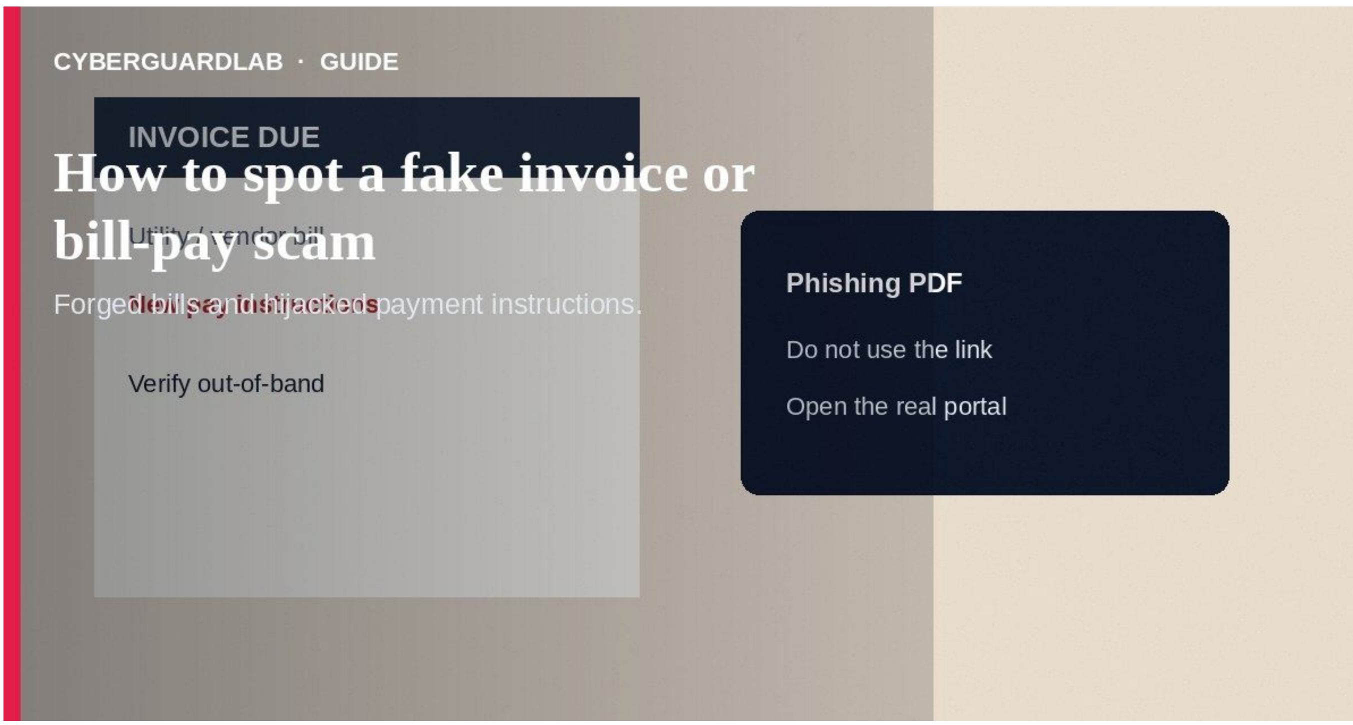
Household antivirus, explained

cyberguardlab.com

How to spot a fake invoice or bill-pay scam

https://cyberguardlab.com/blog/fake-invoice-bill-pay-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 fake invoice or bill-pay scam sends a forged bill, utility notice, subscription renewal, or vendor invoice and pushes you to pay through a bad link or new payment instructions. Do not pay surprise invoices until you verify them through a known phone number or official account portal. Do not use gift cards or wires to "avoid shutoff."

This guide is about forged bills and hijacked pay instructions-not IRS wage-garnishment calls or DMV renewal texts. It overlaps with phishing emails and fake check overpayment. No software purchase required.

1. How fake invoice and bill-pay scripts work

* Look-alike bill - Email, text, portal message, or PDF says "Invoice due," "Utility past due," or "Subscription renew." Branding looks close to a real vendor (FTC phishing guidance).
* Payment redirect - Links lead to phishing pages that harvest passwords or card numbers, or the invoice only changes the bank account or payee so your next payment goes to thieves.
* Vendor bank-detail update - Businesses see email-only ACH or wire instruction changes. Households see fake cable, power, HOA, medical, or school bills.
* Shutoff urgency - Same-day threats and legal language push people to pay before verifying (FTC how to avoid a scam).
* Gift-card or crypto settlement - A "billing desk" demands retail cards or crypto instead of normal remittance methods.

2. Red flags before you pay

Cue	Likely legitimate	Likely scam
Expected bill	Matches a service you use and a normal billing cycle	First contact about a bill you do not recognize
Payment channel	Official app or site you open yourself, or remittance details you already verified	New link in email or SMS; sudden new wiring or deposit account
Amount and tone	Consistent with past bills	Odd amount plus same-day shutoff or legal threats
Contact for changes	Bank detail changes confirmed out-of-band with a known number	Email-only bank account updates
Sender identity	Exact domain and portal login you already use	Look-alike domains, free email, or a "billing desk" you never used
Payment types	Card, ACH, or check to the known payee	Gift cards, crypto, or wire to a person's name

3. Safer habits (buy-nothing)

* Do not click invoice links. Open your bookmarked utility, bank, or vendor site and check balances there.
* Call the company using the number on a past statement or the official site-not the number on the suspicious invoice.

* Confirm vendor bank-detail changes by phone with a known contact.
* Inspect domains carefully; small spelling changes matter.
* Never pay a bill with gift cards.
* Keep a short list of real billers and how you normally pay so surprise invoices are easier to spot.

4. If you already paid

* Contact your bank or card issuer immediately to report fraud and ask about recalls or chargebacks.
* Change passwords if you typed them on a linked page. Enable multifactor authentication.
* Save the invoice, headers, and payment proof.
* Report at ReportFraud.ftc.gov. Use IdentityTheft.gov if personal data was taken.
* Notify the real vendor so they know your account may show as unpaid for the wrong reason.
* If you opened attachments, remove unknown software and review email forwarding rules (FTC guidance if you were scammed).

FAQ

My utility emailed a past-due PDF. How do I verify?

Ignore the PDF link. Sign in at the official site you already use or call the number on a previous statement you trust.

A longtime vendor sent new wiring instructions by email only. Safe?

Treat email-only bank changes as high risk. Confirm by phone or a known portal before paying.

Is a fake invoice the same as a phishing email?

Fake invoices are often a type of phishing or social-engineering payment fraud. The goal may be credentials, card data, or a misdirected payment. See how to spot a phishing email.

They said pay with gift cards to restore service. Ever legitimate?

No reputable utility or major vendor asks households to settle bills with gift cards.

How is this different from a PayPal goods scam?

PayPal goods scams center on marketplace purchases and claims. Fake invoice scams target routine bills and vendor pay instructions. See PayPal goods and services scams.

Do I need paid antivirus to avoid a fake invoice scam?

No. Verifying bills out-of-band and refusing surprise links are enough. Buy-nothing is valid.

If you still want a paid suite

Avoiding a fake invoice or bill-pay scam does not require paid antivirus. Careful bill habits are a valid buy-nothing stack. If you want multi-device paid protection later, use only these on-site paid links: TotalAV (paid link), Norton (paid link), Bitdefender (paid link), McAfee (paid link), Avast (paid link).

Sources

* How To Recognize and Avoid Phishing Scams (FTC)
* How To Avoid a Scam (FTC)
* Spotting fraud and scams (CFPB)
* ReportFraud.ftc.gov

Also read

* How to spot a phishing email
* How to spot a utility shutoff scam
* How to spot a PayPal goods and services scam
* How to spot a fake check scam
* How to report a scam to the FTC